

IBM Security Verify Governance
10.0

*Oracle Database Adapter Installation
and Configuration Guide*



Contents

- Figures..... V**
- Tables..... vii**
- Chapter 1. Overview..... 1**
 - Features of the adapter.....1
 - Architecture of the adapter.....1
 - Supported configurations..... 2
- Chapter 2. Planning..... 5**
 - Roadmap..... 5
 - Prerequisites..... 6
 - Software downloads..... 8
 - Installation worksheet..... 9
- Chapter 3. Installing in the virtual appliance..... 11**
- Chapter 4. Installing..... 13**
 - Installing the dispatcher.....13
 - Installing the adapter binaries or connector.....14
 - Restarting the adapter service..... 15
 - Importing the adapter profile.....16
 - Importing attribute mapping file.....18
 - Adding a connector.....19
 - Enabling connectors.....21
 - Reviewing and setting channel modes for each new connector.....22
 - Attribute Mapping.....24
 - Creating adapter user account.....26
 - Service/Target form details.....29
 - Installing the ILMT tags.....32
 - Verifying that the adapter is working correctly.....33
- Chapter 5. Upgrading..... 35**
 - Upgrading the dispatcher..... 35
 - Upgrading adapter profile.....35
- Chapter 6. Configuring..... 37**
 - Customizing the adapter profile..... 37
 - Editing adapter profiles on the UNIX or Linux operating system..... 39
 - Configuring the Dispatcher properties.....40
 - Customize table space quota sizes.....40
 - Enabling auditing on an Oracle resource.....42
 - Configuring OCI for Transparent Application Failover.....43
 - Installing the JDBC OCI driver.....44
 - Configuring the OCI connection.....45
 - Modifying the Oracle Database Adapter service form for OCI.....48
 - Configuring Network Data Encryption and Integrity for Thin JDBC Clients.....50**
 - Secure Sockets Layer (SSL) communication.....51
 - JDBC driver location for SSL.....52

Configuring the SSL connection.....	53
Password management for account restoration.....	57
Verifying that the adapter is working correctly.....	58
Usage instructions for Oracle 12c support.....	59
Chapter 7. Troubleshooting.....	61
Techniques for troubleshooting problems.....	61
Error messages and problem solving.....	63
Chapter 8. Uninstalling.....	65
Uninstalling the adapter.....	65
Uninstalling the adapter stored procedures from the Oracle Database.....	65
Deleting the adapter profile.....	66
Chapter 9. Reference.....	67
Adapter attributes and object classes.....	67
Adapter attributes by operations.....	68
System Login Add.....	68
System Login Change.....	69
System Login Delete.....	69
System Login Suspend.....	69
System Login Restore.....	69
Test.....	69
Reconciliation.....	70
Special attributes.....	70
Index.....	71

Figures

- 1. The architecture of the Oracle Database Adapter..... 2
- 2. Example of a single server configuration..... 3
- 3. Example of multiple server configuration..... 3
- 4. SSL communication overview..... 51

Tables

- 1. Prerequisites to install the adapter.....7
- 2. Required information to install the adapter.....9
- 3. Adapter package contents..... 11
- 4. Prerequisites for enabling a connector..... 21
- 5. Required privileges and their descriptions..... 26
- 6. Ports.....29
- 7. Warning and error messages 63
- 8. Attributes, object identifiers, descriptions, and corresponding column/table name on the Oracle database..... 67
- 9. Add request attributes for Oracle..... 68
- 10. Change request attributes for Oracle..... 69
- 11. Delete request attributes for Oracle..... 69
- 12. Suspend request attributes for Oracle..... 69
- 13. Restore request attributes for Oracle..... 69
- 14. Test attributes..... 69
- 15. Reconciliation request attributes for Oracle..... 70

Chapter 1. Overview

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

Note: The Oracle Database Adapter does not manage the Oracle System privileges. The following Oracle System privileges are available on the account form on IBM Security Verify Governance. However, these privileges are managed only on Trusted Oracle, the multi-level secure version of Oracle:

- WRITEDOWN DBLOW
- READUP DBHIGH
- WRITEUP DBHIGH
- WRITEDOWN
- READUP
- WRITEUP

Related concepts

Architecture of the adapter

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

Supported configurations

The adapter supports both single and multiple server configurations.

Architecture of the adapter

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

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.

Figure 1 on page 2 describes the components that work together to complete the user account management tasks in a Security Directory Integrator environment.

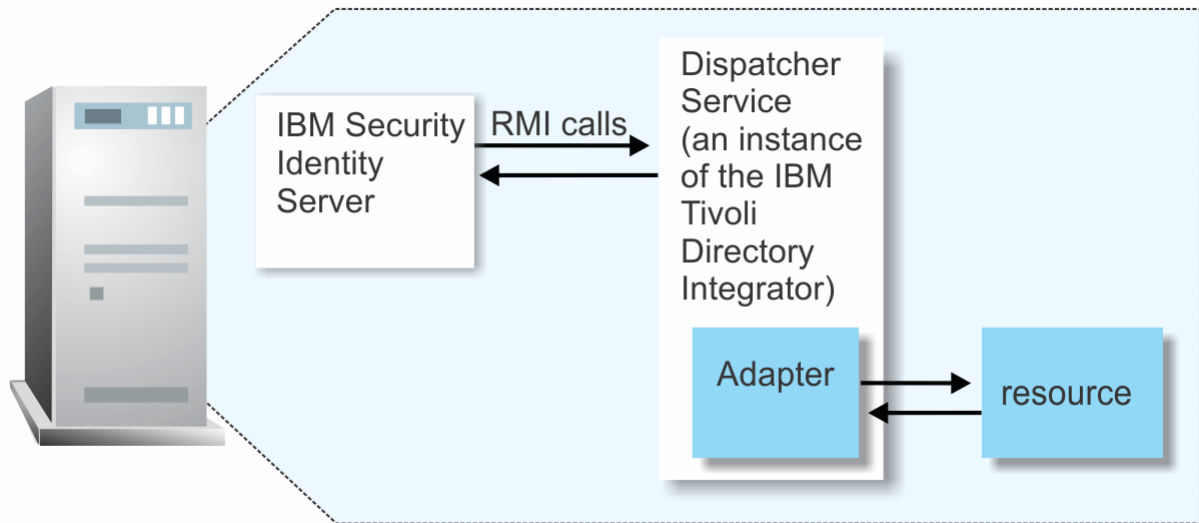


Figure 1. The architecture of the Oracle Database Adapter

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.

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 Oracle Database Adapter on one server to establish communication with an Oracle database. The Oracle database is installed on a different server as described [Figure 2 on page 3](#).

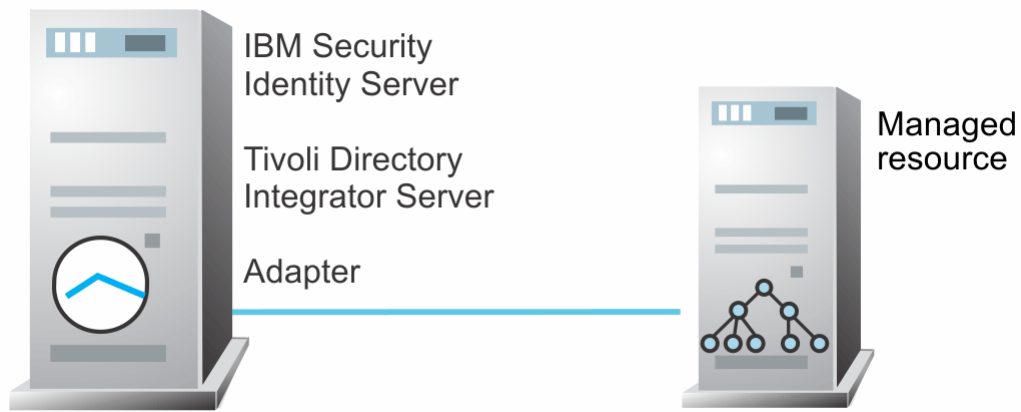


Figure 2. Example of a single server configuration

Multiple server configuration

In multiple server configuration, the Identity server, the Security Directory Integrator server, the Oracle Database Adapter, and the Oracle database are installed on different servers. Install the Security Directory Integrator server and the Oracle Database Adapter on the same server as described [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

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 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.

[Table 1 on page 7](#) identifies the software and operating system prerequisites for the adapter installation.

Ensure that you install the adapter on the same workstation as the IBM Security Directory Integrator server.

Table 1. Prerequisites to install the adapter

Prerequisite	Description
Directory Integrator	<ul style="list-style-type: none"> • IBM Security Directory Integrator 7.2 + FP6 + 7.2.0-ISS-SDI-LA0019 <p>Note:</p> <ul style="list-style-type: none"> • 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	<p>The following servers are supported:</p> <ul style="list-style-type: none"> • IBM Security Verify Governance Identity Manager v10.0 • IBM Security Verify Governance v10.0 • IBM Security Identity Manager v7.0.x • IBM Security Identity Manager v6.0.x • IBM Security Privileged Identity Manager v2.x • IBM Security Identity Governance and Intelligence v5.2.x
Oracle Database	<p>A system that runs the Oracle database with one of following versions:</p> <ul style="list-style-type: none"> • Oracle 11g (11.1.0.x) • Oracle 11gR2 (11.2.0.x) • Oracle 12c (non-container database) • Oracle 12c (Container database) • Oracle 12c R2(Container database) • Oracle 12c R2(non-container database) • Oracle 19c (non-container database) • Oracle 19c (Container database) <p>Note: The adapter supports the Oracle versions that are described in the Oracle Lifetime Support document: http://www.oracle.com/us/support/library/lifetime-support-technology-069183.pdf.</p>

<i>Table 1. Prerequisites to install the adapter (continued)</i>	
Prerequisite	Description
Oracle Thin JDBC Driver	JDBC 10.2.0.1.0 Driver Note: The driver file names are <ul style="list-style-type: none"> • <code>ojdbc5.jar</code> for Security Directory Integrator 7.0 (JDK version 1.5) • <code>ojdbc6.jar</code> for Security Directory Integrator 7.2 (JDK version 1.6)
Oracle JDBC OCI Driver Note: You need this driver for Oracle Real Application Cluster (RAC) and Oracle Transparent Application Failover (TAF) architectures.	JDBC OCI 10.2.0.x Driver JDBC OCI 11.2.0.2.0 Driver
Network Connectivity	Install the adapter on a workstation that can communicate with the 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 IBM Security Verify Adapters. See the <i>Dispatcher Installation and Configuration Guide</i> .
UTC Timezone	To integrate the Oracle Database, ensure that this query is set: <pre>SELECT TZNAME FROM V\$TIMEZONE_NAMES WHERE TZNAME=' UTC '</pre>

Install the Oracle Database Adapter and the appropriate Oracle Thin JDBC drivers on the same workstation as the Security Directory Integrator.

For information about the prerequisites and supported operating systems for Security Directory Integrator, see the *IBM Security Directory Integrator 7.0: Administrator Guide*.

Related concepts

[Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance](#)
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 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
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.

<i>Table 2. Required information to install the adapter</i>		
Required information	Description	Value
IBM Security Directory Integrator Home Directory	The <i>ITDI_HOME</i> directory contains the jars/connectors subdirectory that contains adapter jars. For example, the jars/connectors subdirectory contains the jar for the UNIX adapter.	<p>If Security Directory Integrator is automatically installed with your IBM Security Verify Governance product, the default directory path for Security Directory Integrator is as follows:</p> <p>Windows:</p> <ul style="list-style-type: none"> for version 7.0: <i>drive</i>\Program Files\IBM\TDI\V7.0 for version 7.1: <i>drive</i>\Program Files\IBM\TDI\V7.1 <p>UNIX:</p> <ul style="list-style-type: none"> for version 7.0: /opt/IBM/TDI/V7.0 for version 7.1: /opt/IBM/TDI/V7.1

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 <i>Dispatcher Installation and Configuration Guide</i> .	<p>The default solution directory is located at:</p> <p>Windows:</p> <ul style="list-style-type: none"> • for version 7.0: <i>drive\Program Files\IBM\TDI\V7.0\isimsoln</i> • for version 7.1: <i>drive\Program Files\IBM\TDI\V7.1\isimsoln</i> <p>UNIX:</p> <ul style="list-style-type: none"> • for version 7.0: <i>/opt/IBM/TDI/V7.0/isimsoln</i> • for version 7.1: <i>/opt/IBM/TDI/V7.1/isimsoln</i>

Related concepts

[Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance](#)
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 virtual appliance

For Verify Governance 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](#) 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:

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	<p>An Security Directory Integrator adapter always include a JAR profile which contains:</p> <ul style="list-style-type: none">• targetProfile.json<ul style="list-style-type: none">– 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. <p>Use the Target Administration module to import the target profile.</p>

Table 3. Adapter package contents (continued)	
Files	Descriptions
Additional adapter specific files	<p>Examples of adapter specific files:</p> <ul style="list-style-type: none"> • Connector jar files • Configuration files • Script files • Properties files <p>The file names are specified in the adapter definition file along with the destination directory in the virtual appliance.</p>

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 the *Dispatcher Installation and Configuration Guide*.

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.

Creating adapter user account

You must create a user account for the adapter on the managed resource. Provide the account information when you create a service for the adapter on IBM Security Verify Governance.

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 server, add a connector so that Verify Governance 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 account attributes.

Installing the ILMT tags

This topic describes the procedures to install ILMT tag files.

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 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.

Creating adapter user account

You must create a user account for the adapter on the managed resource. Provide the account information when you create a service for the adapter on IBM Security Verify Governance.

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 server, add a connector so that Verify Governance 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 account attributes.

Installing the ILMT tags

This topic describes the procedures to install ILMT tag files.

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.

Creating adapter user account

You must create a user account for the adapter on the managed resource. Provide the account information when you create a service for the adapter on IBM Security Verify Governance.

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 server, add a connector so that Verify Governance 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 account attributes.

Installing the ILMT tags

This topic describes the procedures to install ILMT tag files.

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 server can manage.

The adapter profile definition file is used to create a target profile on the Verify Governance 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 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 18](#).
- Create a connector that uses the target profile. See [“Adding a connector” on page 19](#).

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.

[Creating adapter user account](#)

You must create a user account for the adapter on the managed resource. Provide the account information when you create a service for the adapter on IBM Security Verify Governance.

[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 server, add a connector so that Verify Governance 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 account attributes.

[Installing the ILMT tags](#)

This topic describes the procedures to install ILMT tag files.

[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 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.

Creating adapter user account

You must create a user account for the adapter on the managed resource. Provide the account information when you create a service for the adapter on IBM Security Verify Governance.

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 server, add a connector so that Verify Governance 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 account attributes.

Installing the ILMT tags

This topic describes the procedures to install ILMT tag files.

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 server, add a connector so that Verify Governance server can communicate with the managed resource.

Before you begin

Complete [Importing the adapter profile](#).

Note: If you migrated from Verify Governance 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 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 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. For more information, see [“Enabling connectors” on page 21](#).

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.

[Creating adapter user account](#)

You must create a user account for the adapter on the managed resource. Provide the account information when you create a service for the adapter on IBM Security Verify Governance.

[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 account attributes.

Installing the ILMT tags

This topic describes the procedures to install ILMT tag files.

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.	“Adding a connector” on page 19.
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 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.

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.

Creating adapter user account

You must create a user account for the adapter on the managed resource. Provide the account information when you create a service for the adapter on IBM Security Verify Governance.

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 server, add a connector so that Verify Governance 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 account attributes.

Installing the ILMT tags

This topic describes the procedures to install ILMT tag files.

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 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 V5.2.3:

1. Log in to the Verify Governance 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 21.

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.

Creating adapter user account

You must create a user account for the adapter on the managed resource. Provide the account information when you create a service for the adapter on IBM Security Verify Governance.

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 server, add a connector so that Verify Governance 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 account attributes.

Installing the ILMT tags

This topic describes the procedures to install ILMT tag files.

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 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 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 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 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 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.

Creating adapter user account

You must create a user account for the adapter on the managed resource. Provide the account information when you create a service for the adapter on IBM Security Verify Governance.

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 server, add a connector so that Verify Governance 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.

[Installing the ILMT tags](#)

This topic describes the procedures to install ILMT tag files.

[Verifying that the adapter is working correctly](#)

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

Creating adapter user account

You must create a user account for the adapter on the managed resource. Provide the account information when you create a service for the adapter on IBM Security Verify Governance.

For more information about creating a service, see [Creating an adapter service](#).

The accounts must be able to remotely connect to the Oracle Database server and must have sufficient privileges to administer the Oracle Database users. [Table 5 on page 26](#) lists the required privileges that the user account must have to administer the Oracle Database users.

Privilege	Description
CREATE USER	To create an Oracle database user.
GRANT ANY ROLE	To grant or remove roles to the Oracle database user.
SELECT ANY TABLE	To perform the reconciliation operation and retrieve the following information from the Oracle database: <ul style="list-style-type: none">• List of Users and its attributes• List of Tables• List of Roles• List of Privileges• List of Consumer groups• Oracle version
GRANT ANY PRIVILEGE	To grant or remove privileges to the Oracle database user.

Table 5. Required privileges and their descriptions (continued)

Privilege	Description
SELECT ANY DICTIONARY	<p>The SELECT ANY DICTIONARY privilege replaces the default setting of the O7_DICTIONARY_ACCESSIBILITY initialization parameter. The default value of the parameter is FALSE.</p> <p>Using this system privilege, users can access all the objects in the SYS schema, including tables that are created in that schema.</p> <p>You must grant the required privileges to the individual users based on the requirements. The SELECT ANY DICTIONARY privilege is not included in the GRANT ALL PRIVILEGES privilege. You can also grant the SELECT ANY DICTIONARY privilege through a role.</p> <p>You might use the following scenarios, depending on your requirements:</p> <ul style="list-style-type: none"> • If the O7_DICTIONARY_ACCESSIBILITY=TRUE, then the SELECT ANY TABLE privilege provides access to all SYS and non-SYS objects. • If the O7_DICTIONARY_ACCESSIBILITY=FALSE, then the SELECT ANY TABLE privilege provides access only to non-SYS objects. • If the SELECT_CATALOG_ROLE privilege is enabled, then the SELECT_CATALOG_ROLE privilege provides access to all SYS views only. • If only the SELECT ANY DICTIONARY privilege is enabled, then the SELECT ANY DICTIONARY privilege provides access to SYS schema objects only. • If both SELECT ANY TABLE and SELECT ANY DICTIONARY privileges are enabled, then the SELECT ANY TABLE and SELECT ANY DICTIONARY privileges provide access to all SYS and non-SYS objects. • The SELECT ANY DICTIONARY and SELECT_CATALOG_ROLE privileges do not affect the O7_DICTIONARY_ACCESSIBILITY settings.
SELECT ON SYS.USER\$	<p>For Oracle 12c support (non-container database), to access the date when the password was last changed or the PTIME column from the SYS.USER\$ table.</p> <p>To retrieve Last password change date, grant this privilege to the user.</p>
WM_ADMIN_ROLE or SELECT_CATALOG_ROLE	To access DBA_WM_SYS_PRIVS view.
EXECUTE permission on DBMS_LOCK and ADMINISTER_RESOURCE_MANAGER system privilege	To execute stored procedures that set the consumer group.

By default, a user is granted access on objects within the schema of the user. The ANY keyword grants access to users on all objects of that type in all schemas. For example:

- To grant a system privilege, you must either have system privileges that are granted with ADMIN OPTION or GRANT ANY PRIVILEGE.
- To grant an object privilege, one of the following conditions must be met:
 - You must be an object owner.
 - The object owner must grant you the object privileges with the GRANT OPTION.
 - The object owner must grant you the GRANT ANY OBJECT PRIVILEGE system privilege.

If you do not use the *ANY* keyword, you must either grant privileges, roles, tables, and so on, to a user account or the user account must be an object owner. When a new privilege, role, or a table is added in the schema, you must update the permissions for the user account.

To reduce security risks, do not use the *ANY* keyword to grant privileges to user accounts.

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 server, add a connector so that Verify Governance 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 account attributes.

Installing the ILMT tags

This topic describes the procedures to install ILMT tag files.

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.

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**
- **Convert Username to Uppercase**
- **AL FileSystem Path**
- **Max Connection Count**

On the Oracle 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.

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

Oracle Service Name

Specify the service name of Oracle instance to which the adapter must connect.

Is SID

By default, this option is not selected. Select this check box if the Oracle Database service name provided is an SID instead of a service name. This option affects the connection to the database. If this option is selected while the database is using a service name, then the test connection fails.

Oracle Service Host

Specify the host workstation on which the Oracle instance is running.

Oracle Service Port

Specify the TCP or TCPS port on which the Oracle service is listening. For example:

- TCP: 1521
- TCPS: 2484

Use SSL communication with Oracle

Optional: Select this check box to enable SSL communication between the Oracle adapter and the Oracle database. When selected, specify the TCPS port in **Oracle Service Port**.

Oracle Service Alias

If the **OCI communication check box** is selected, specify the net service alias that is listed in the `tnsnames.ora` file that defines the connection to the Oracle instance.

Use OCI communication with Oracle

Optional: Select this check box to enable OCI communication between the Oracle adapter and the Oracle database.

Oracle Administrator Name

Specify the name of the user who has access to the Oracle resource and can do administrative operations.

Oracle Administrator Password

Specify the password for the user.

Oracle Server Distinguished Name

Optional: Specify the distinguished name. For example, `CN=client, C=US`. This name is verified against the Oracle database server certificate.

Owner

Optional: Specify a user as a service owner.

Service Prerequisite

Specify a service that is prerequisite to this service.

Convert Username to Uppercase

Optional: Select this check box to retain the case of the user name. By default, the adapter converts the case of the user name to uppercase.

Do not Cascade on Delete

Optional: Select this check box to disable the cascade action when deleting a user. By default, the adapter uses cascade on user deletion.

JDBC Thin Client Properties File Path

Optional: Specify the properties file path of the Oracle advanced security option, to enable thin client encryption.

See [“Configuring Network Data Encryption and Integrity for Thin JDBC Clients”](#) on page 50 for more information on how to use the properties file.

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 received from Identity server. For example, you can use these file paths to load the assembly lines from these directories:

- For Windows operating system:

```
c:\Files\IBM\TDI\V7.0\profiles
```

- 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 managed resource. These fields are examples. The actual fields vary depending on the type of adapter and how the service form is configured. The adapter must be running to obtain the information. Click **Test Connection** to populate the fields.

Last status update: Date

Specifies the most recent date when the Status and information tab was updated.

Last status update: Time

Specifies the most recent time of the date when the Status and information tab was updated.

Managed resource status

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

Adapter version

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

Profile version

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

TDI version

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

Dispatcher version

Specifies the version of the Dispatcher.

Installation platform

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

Adapter account

Specifies the account that running the adapter binary file.

Adapter up time: Date

Specifies the date when the adapter started.

Adapter up time: Time

Specifies the time of the date when the adapter started.

Adapter memory usage

Specifies the memory usage for running the adapter.

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

- Verify the adapter log to ensure that the test request was successfully sent to the adapter.
- Verify the adapter configuration information.

- Verify service parameters for the adapter profile. For example, verify the work station name or the IP address of the managed resource and the port.

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.

Creating adapter user account

You must create a user account for the adapter on the managed resource. Provide the account information when you create a service for the adapter on IBM Security Verify Governance.

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 server, add a connector so that Verify Governance 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 account attributes.

Installing the ILMT tags

This topic describes the procedures to install ILMT tag files.

Verifying that the adapter is working correctly

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

Installing the ILMT tags

This topic describes the procedures to install ILMT tag files.

About this task

Ensure that the Dispatcher is installed.

Procedure

- Copy the files from **ILMT-Tags** folder to the specified location:

- Windows: <SDI-HOME>/swidtag
- Unix/Linux: <SDI-HOME>/swidtag

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.

Creating adapter user account

You must create a user account for the adapter on the managed resource. Provide the account information when you create a service for the adapter on IBM Security Verify Governance.

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 server, add a connector so that Verify Governance 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 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.

Creating adapter user account

You must create a user account for the adapter on the managed resource. Provide the account information when you create a service for the adapter on IBM Security Verify Governance.

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 server, add a connector so that Verify Governance 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 account attributes.

Installing the ILMT tags

This topic describes the procedures to install ILMT tag files.

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 adapter profile](#)

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

Upgrading 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 Oracle 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 for that adapter.

The JAR file is included in the Oracle 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`
- `erOracleAccount.xml`
- `erOracleRMIService.xml`
- `OracleAdapter.xml`
- `service.def`
- `schema.dsm1`

Procedure

1. Edit the JAR file.
 - a) Log on to the workstation where the Oracle 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. Type the name of the JAR file for your operating system. The following example applies to the Oracle Database Adapter profile.

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

The **jar** command extracts the files into the OracleAdapterProfile 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 OracleAdapterProfile.jar OracleAdapterProfile
```

UNIX

```
cd /tmp
jar -cvf OracleAdapterProfile.jar OracleAdapterProfile
```

- b) Import the JAR file into the IBM Security Verify Governance application server.
- c) Stop and start the Identity server
- d) Restart the adapter service.

Related concepts

[Configuring the Dispatcher properties](#)

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

[Customize table space quota sizes](#)

The adapter enables customizing the required quota size on the table spaces when you provision user accounts.

[Secure Sockets Layer \(SSL\) communication](#)

You can secure your environment by using Secure Sockets Layer (SSL) communication among Identity server, Security Directory Integrator, and the Oracle servers. You can configure SSL communication across the entire solution.

[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.

[Usage instructions for Oracle 12c support](#)

The Oracle DB adapter can be now used to manage Oracle 12c container database.

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.

[Enabling auditing on an Oracle resource](#)

You must enable auditing on the database so that the Oracle Database Adapter can retrieve the last access date of the user account.

[Configuring OCI for Transparent Application Failover](#)

Transparent Application Failover (TAF) is a feature of the Java Database Connectivity (JDBC) Oracle Call Interface (OCI) driver. If you configure the adapter to use TAF, then the adapter can automatically reconnect to a secondary database instance if the original database connection fails.

[Configuring Network Data Encryption and Integrity for Thin JDBC Clients](#)

Network data encryption and integrity for JDBC thin clients is a feature of Oracle Advanced security, which lets thin Java database connectivity (JDBC) clients to securely connect and communicate with the Oracle database.

[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

[Configuring the Dispatcher properties](#)

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

[Customize table space quota sizes](#)

The adapter enables customizing the required quota size on the table spaces when you provision user accounts.

[Secure Sockets Layer \(SSL\) communication](#)

You can secure your environment by using Secure Sockets Layer (SSL) communication among Identity server, Security Directory Integrator, and the Oracle servers. You can configure SSL communication across the entire solution.

[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.

[Usage instructions for Oracle 12c support](#)

The Oracle DB adapter can be now used to manage Oracle 12c container database.

Related tasks

[Customizing the adapter profile](#)

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

[Enabling auditing on an Oracle resource](#)

You must enable auditing on the database so that the Oracle Database Adapter can retrieve the last access date of the user account.

[Configuring OCI for Transparent Application Failover](#)

Transparent Application Failover (TAF) is a feature of the Java Database Connectivity (JDBC) Oracle Call Interface (OCI) driver. If you configure the adapter to use TAF, then the adapter can automatically reconnect to a secondary database instance if the original database connection fails.

[Configuring Network Data Encryption and Integrity for Thin JDBC Clients](#)

Network data encryption and Integrity for JDBC thin clients is a feature of Oracle Advanced security, which lets thin Java database connectivity (JDBC) clients to securely connect and communicate with the Oracle database.

[Verifying that the adapter is working correctly](#)

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

Configuring the Dispatcher properties

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

[Customize table space quota sizes](#)

The adapter enables customizing the required quota size on the table spaces when you provision user accounts.

[Secure Sockets Layer \(SSL\) communication](#)

You can secure your environment by using Secure Sockets Layer (SSL) communication among Identity server, Security Directory Integrator, and the Oracle servers. You can configure SSL communication across the entire solution.

[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.

[Usage instructions for Oracle 12c support](#)

The Oracle DB adapter can be now used to manage Oracle 12c container database.

Related tasks

[Customizing the adapter profile](#)

To customize the adapter profile, you must modify the Oracle 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.

[Enabling auditing on an Oracle resource](#)

You must enable auditing on the database so that the Oracle Database Adapter can retrieve the last access date of the user account.

[Configuring OCI for Transparent Application Failover](#)

Transparent Application Failover (TAF) is a feature of the Java Database Connectivity (JDBC) Oracle Call Interface (OCI) driver. If you configure the adapter to use TAF, then the adapter can automatically reconnect to a secondary database instance if the original database connection fails.

[Configuring Network Data Encryption and Integrity for Thin JDBC Clients](#)

Network data encryption and Integrity for JDBC thin clients is a feature of Oracle Advanced security, which lets thin Java database connectivity (JDBC) clients to securely connect and communicate with the Oracle database.

[Verifying that the adapter is working correctly](#)

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

Customize table space quota sizes

The adapter enables customizing the required quota size on the table spaces when you provision user accounts.

1. Open the `OracleAdapter.xml` file on IBM Security Directory Integrator.

2. Add the required values for the table space quota sizes as follows:

- a. Open **OracleSearchUserAL**.
- b. Go to **Feed Section**.
- c. Select the **conOracleGetTSQuotas** connector.
- d. Open **Before Selection**.
- e. Search for following line where 'qt' array is defined:

```
var qt = new  
Array("128K", "256K", "512K", "1M", "2M", "4M", "8M", "16M", "32M", "64M", "UNLIMITED");
```

Note: Use the following conventions for specifying the quota sizes:

K

Kilobytes

M

Megabytes

G

Gigabytes

UNLIMITED

Unlimited quota

3. Build a profile jar with updated OracleAdapter.xml file.
4. Import the newly built profile jar (OracleAdapterProfile.jar) on the Identity server.
5. Restart the Service for IBM Security Directory Integrator.

Related concepts

[Configuring the Dispatcher properties](#)

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

[Secure Sockets Layer \(SSL\) communication](#)

You can secure your environment by using Secure Sockets Layer (SSL) communication among Identity server, Security Directory Integrator, and the Oracle servers. You can configure SSL communication across the entire solution.

[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.

[Usage instructions for Oracle 12c support](#)

The Oracle DB adapter can be now used to manage Oracle 12c container database.

Related tasks

[Customizing the adapter profile](#)

To customize the adapter profile, you must modify the Oracle 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.

[Enabling auditing on an Oracle resource](#)

You must enable auditing on the database so that the Oracle Database Adapter can retrieve the last access date of the user account.

[Configuring OCI for Transparent Application Failover](#)

Transparent Application Failover (TAF) is a feature of the Java Database Connectivity (JDBC) Oracle Call Interface (OCI) driver. If you configure the adapter to use TAF, then the adapter can automatically reconnect to a secondary database instance if the original database connection fails.

[Configuring Network Data Encryption and Integrity for Thin JDBC Clients](#)

Network data encryption and Integrity for JDBC thin clients is a feature of Oracle Advanced security, which lets thin Java database connectivity (JDBC) clients to securely connect and communicate with the Oracle database.

[Verifying that the adapter is working correctly](#)

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

Enabling auditing on an Oracle resource

You must enable auditing on the database so that the Oracle Database Adapter can retrieve the last access date of the user account.

About this task

If auditing is not enabled, the Oracle Database Adapter cannot retrieve the information about when the user last accessed the account.

Procedure

1. Set the initialization parameter **audit_trail** to TRUE in the `init.ora` file.

Alternately, you can issue the following command at the SQL command-line prompt:

```
ALTER SYSTEM SET audit_trail=TRUE scope=SPFILE
```

2. Restart the database instance.
3. To turn on the auditing for user logon and logoff, log on as a user with Oracle administration authority. Issue the following command at the SQL command-line prompt:

```
AUDIT CONNECT
```

What to do next

To verify that auditing is enabled on an instance, issue the following command at the SQL command-line prompt:

```
SHOW PARAMETER AUDIT_TRAIL
```

The parameter **AUDIT_TRAIL** and its value are displayed. Any value except NONE or FALSE indicates that auditing is enabled. For more information about the parameters, see the Oracle online help.

Related concepts

[Configuring the Dispatcher properties](#)

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

[Customize table space quota sizes](#)

The adapter enables customizing the required quota size on the table spaces when you provision user accounts.

[Secure Sockets Layer \(SSL\) communication](#)

You can secure your environment by using Secure Sockets Layer (SSL) communication among Identity server, Security Directory Integrator, and the Oracle servers. You can configure SSL communication across the entire solution.

[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.

[Usage instructions for Oracle 12c support](#)

The Oracle DB adapter can be now used to manage Oracle 12c container database.

Related tasks

Customizing the adapter profile

To customize the adapter profile, you must modify the Oracle 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.

Configuring OCI for Transparent Application Failover

Transparent Application Failover (TAF) is a feature of the Java Database Connectivity (JDBC) Oracle Call Interface (OCI) driver. If you configure the adapter to use TAF, then the adapter can automatically reconnect to a secondary database instance if the original database connection fails.

Configuring Network Data Encryption and Integrity for Thin JDBC Clients

Network data encryption and integrity for JDBC thin clients is a feature of Oracle Advanced security, which lets thin Java database connectivity (JDBC) clients to securely connect and communicate with the Oracle database.

Verifying that the adapter is working correctly

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

Configuring OCI for Transparent Application Failover

Transparent Application Failover (TAF) is a feature of the Java Database Connectivity (JDBC) Oracle Call Interface (OCI) driver. If you configure the adapter to use TAF, then the adapter can automatically reconnect to a secondary database instance if the original database connection fails.

About this task

During the reconnect process, the active transactions roll back.

To configure the Oracle adapter to use OCI, you must perform the following high-level steps in this sequence.

1. Install the JDBC OCI driver. For detailed instructions, see [“Installing the JDBC OCI driver” on page 44](#).
2. Configure the OCI connection between the Oracle Database Adapter and the Oracle database, [“Configuring the OCI connection” on page 45](#).
3. [“Modifying the Oracle Database Adapter service form for OCI” on page 48](#).

Procedure

1. Install the JDBC OCI driver.
For detailed instructions, see [“Installing the JDBC OCI driver” on page 44](#).
2. Configure the OCI connection between the Oracle Database Adapter and the Oracle database
For detailed instructions, see [“Configuring the OCI connection” on page 45](#).
3. Configure the Oracle adapter service form.
For detailed instructions, see [“Modifying the Oracle Database Adapter service form for OCI” on page 48](#)

Related concepts

Configuring the Dispatcher properties

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

Customize table space quota sizes

The adapter enables customizing the required quota size on the table spaces when you provision user accounts.

Secure Sockets Layer (SSL) communication

You can secure your environment by using Secure Sockets Layer (SSL) communication among Identity server, Security Directory Integrator, and the Oracle servers. You can configure SSL communication across the entire solution.

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.

Usage instructions for Oracle 12c support

The Oracle DB adapter can be now used to manage Oracle 12c container database.

Related tasks

Customizing the adapter profile

To customize the adapter profile, you must modify the Oracle 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.

Enabling auditing on an Oracle resource

You must enable auditing on the database so that the Oracle Database Adapter can retrieve the last access date of the user account.

Configuring Network Data Encryption and Integrity for Thin JDBC Clients

Network data encryption and integrity for JDBC thin clients is a feature of Oracle Advanced security, which lets thin Java database connectivity (JDBC) clients to securely connect and communicate with the Oracle database.

Verifying that the adapter is working correctly

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

Installing the JDBC OCI driver

Transparent Application Failover (TAF) is a feature of the Java Database Connectivity (JDBC) Oracle Call Interface (OCI) driver. You must install the Oracle Database Client software on the IBM Security Directory Integrator target.

Procedure

1. Obtain the Oracle Database Client software from the **Downloads** page on the [Oracle Technology Network](#) website.

For example, you can download the `win64_11gR2_client.zip` file for the Oracle Database 11g Release 2 Client (11.2.0.1.0) for Microsoft Windows (64-bit) software.

Note: Ensure that `OCIJDBC19.dll` is copied to `c:\Program Files\IBM\TDI\V7.2\jvm\jre\bin` (Java Library).

2. Install the client software.

When you install the client software, select the installation type that installs tools for developing applications, networking services, and basic client software. For example, if you are using the Oracle Database 11gR2 Client, select the **Runtime** installation type.

Alternatively, you can select the installation type that installs the instant client software. For example, if you are using the Oracle Database 11gR2 Client, select the **InstantClient** installation type. The instant client installation requires less disk space than the runtime installation.

Note: Use the Oracle Support website to determine the Oracle client and server versions that you require. For example, to use the OCI JDBC driver for SSL communication from an 11gR2 client to a 10gR2 server requires the following minimum versions:

- Oracle Client **11gR2** (11.2.0.2.0 or higher) to connect to Oracle Server **10gR2** (10.2.0.2.0 or higher).

Related tasks

Configuring the OCI connection

You can enable OCI communication between the Oracle Database Adapter and the Oracle database. You must configure Oracle Net Services (ONS) on the Security Directory Integrator where the Oracle Client software is installed.

Modifying the Oracle Database Adapter service form for OCI

To configure OCI communication between the Oracle adapter and the Oracle database, you must modify the Oracle adapter service form.

Configuring the OCI connection

You can enable OCI communication between the Oracle Database Adapter and the Oracle database. You must configure Oracle Net Services (ONS) on the Security Directory Integrator where the Oracle Client software is installed.

About this task

To configure Oracle Net Services, you must complete the following high-level tasks.

Procedure

1. Configure the Oracle Net Services.
For detailed instructions, see [“Configuring Oracle Net Services” on page 45](#).
2. Configure the Oracle Database Adapter.
For detailed instructions, see [“Configuring the Oracle adapter” on page 47](#)

Related tasks

Installing the JDBC OCI driver

Transparent Application Failover (TAF) is a feature of the Java Database Connectivity (JDBC) Oracle Call Interface (OCI) driver. You must install the Oracle Database Client software on the IBM Security Directory Integrator target.

Modifying the Oracle Database Adapter service form for OCI

To configure OCI communication between the Oracle adapter and the Oracle database, you must modify the Oracle adapter service form.

Configuring Oracle Net Services

For Transparent Application Failover, you must configure Oracle Net Services by editing the `tnsnames.ora` and `sqlnet.ora` files on the Oracle database server.

Procedure

1. Locate the `tnsnames.ora` and `sqlnet.ora` files in the `network\admin` directory of the Oracle home directory.
Note: These files do not exist in an Instant Client installation. In this case, you must create the files. These files must be in the same directory as one another. For example, you might choose to save these files in the Instant Client directory.
2. Open the files in a text editor.
Note: To configure Transparent Application Failover, you must use a text editor rather than Oracle Net Manager to edit these files.
3. Configure the files for your environment.

Example

The information in the following files is an example of how you can configure Transparent Application Failover:

sqlnet.ora:

```
SQLNET.AUTHENTICATION_SERVICES= (NONE)
NAMES.DIRECTORY_PATH= (TNSNAMES)
```

tnsnames.ora:

```
PRODONE =
(DESCRIPTION_LIST =
  (FAILOVER = true)
  (LOAD_BALANCE = false)
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = YourFirstHost)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVER = dedicated)
      (FAILOVER_MODE =
        (BACKUP = PRODTWO)
        (TYPE = select)
        (METHOD = basic)
        (RETRIES = 20)
        (DELAY = 3)
      )
    )
  )
  (SERVICE_NAME = ORCL)
)
)
(DESCRIPTION =
  (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = TCP)(HOST = YourSecondHost)(PORT = 1521))
  )
  (CONNECT_DATA =
    (SERVICE_NAME = ORCL)
  )
)
)
)

PRODTWO =
(DESCRIPTION_LIST =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = YourSecondHost)(PORT = 1521))
    )
  )
  (CONNECT_DATA =
    (SERVICE_NAME = ORCL)
  )
)
)
)
```

Note:

- When you use Transparent Application Failover, if the connected instance fails or is shutdown, the adapter can automatically reconnect to a database. Transparent Application Failover enables the application to transparently reconnect to a specified secondary instance. This reconnection process creates a new connection that is identical to the original connection.
- In the `tnsnames.ora` file, `PRODONE` is the example net service alias that defines both Transparent Application Failover and Connect Time Failover (CTF). The first description in the `DESCRIPTION_LIST` defines Transparent Application Failover. The second description in the `DESCRIPTION_LIST` defines Connect Time Failover.
- The Transparent Application Failover description indicates that if an established connection to `YourFirstHost` fails, then the connection fails over to `YourSecondHost` via the `PRODTWO` net service alias. The Connect Time Failover description indicates that if `YourFirstHost` is down before the initial connection, then the connection fails over to `YourSecondHost`.
- The `select` type is a feature of Transparent Application Failover. Use `select` to indicate that if the first connection fails while it is processing a `SELECT` statement, then the statement runs again when a new

connection is established. The cursor moves to the correct position so the client can continue fetching rows without interruption.

Configuring the Oracle adapter

You must configure Security Directory Integrator to locate the JDBC OCI driver and Oracle Net Services.

About this task

To use OCI communication, the adapter must have access to the JDBC OCI driver and the Oracle Net Services files, `tnsnames.ora` and `sqlnet.ora`.

Note: To locate the JDBC OCI driver, you must amend the path variable to include the `ORACLE_HOME/bin` directory or the Instant Client directory. Depending on the Security Directory Integrator service, you must configure the path variable slightly differently, as described in the following steps.

Procedure

1. Determine which Security Directory Integrator service is used on your server.

There are two Security Directory Integrator services that can exist or coexist on your Security Directory Integrator target.

- The IBM Security Verify Adapter, which is called `ITDIAsService.exe`.
- The IBM Security Directory Integrator service, which is called `ibmdiservice.exe`.

2. For the **ITDIAsService** service, edit the `ImagePath` registry variable in the following location: `HKLM\SYSTEM\ControlSet001\Service\IBM Security Verify Adapter`.

Note: The value of `ImagePath` is an expandable String Value of **REG_EXPAND_SZ** Type.

- For a Database Client installation, edit the `ImagePath` variable to include `%ORACLE_HOME%\bin` as follows:

```
"C:\Program Files\IBM\TDI\V7.2\timso1\ITDIAsService.exe" ...  
-Djava.library.path="C:\Program Files\IBM\TDI\V7.2\libs;  
%ORACLE_HOME%\bin;%PATH%" ...
```

Note: Use `%ORACLE_HOME%` in the `ImagePath` variable only when `ORACLE_HOME` is defined as a System variable on Windows. Otherwise, you must explicitly include the Oracle home bin directory as follows:

```
"C:\Program Files\IBM\TDI\V7.2\timso1\ITDIAsService.exe" ...  
-Djava.library.path="C:\Program Files\IBM\TDI\V7.2\libs;  
C:\app\administrator\product\11.2.0\client_1\bin;%PATH%" ...
```

- For an Instant Client installation, edit the `ImagePath` variable to include the directory of the Instant Client files as follows:

```
"C:\Program Files\IBM\TDI\V7.2\timso1\ITDIAsService.exe" ...  
-Djava.library.path="C:\Program Files\IBM\TDI\V7.2\libs;  
C:\app\administrator\product\11.2.0\client_1;%PATH%" ...
```

3. For the **ibmdiservice** service, edit the `path` variable in the `ibmdiservice.props` properties file.

This properties file is in the following directory:

```
C:\Program Files\IBM\TDI\V7.2\timso1
```

- For a Database Client installation, edit the `path` variable to include the Oracle home bin directory as follows:

```
path=C:\Program Files\IBM\TDI\V7.2\jvm\jre\bin;C:\Program Files\IBM\TDI\V7.2\  
libs;C:\app\administrator\product\11.2.0\client_1\bin;
```

- For an Instant Client installation, set the path variable to the Oracle home directory as follows:

```
path=C:\Program Files\IBM\TDI\V7.2\jvm\jre\bin;C:\Program Files\IBM\TDI\V7.2\
libs;C:\app\administrator\product\11.2.0\client_1;
```

4. For both services, you must configure Security Directory Integrator to locate the Oracle Net Services files as follows:

- For a Database Client installation, define the *ORACLE_HOME* environment variable in the Windows registry so that Security Directory Integrator can locate the Oracle Net Services files.

Note: Alternatively, you can define the *ORACLE_HOME* as a System variable in Windows.

An example *ORACLE_HOME* environment value is:

```
ORACLE_HOME=C:\app\administrator\product\11.2.0\client_1
```

- For an Instant Client installation, you must define the *TNS_ADMIN* environment variable, which is an Oracle Client variable, to point to the location (directory) of the ONS configuration files.

An example *TNS_ADMIN* environment value is:

```
TNS_ADMIN=C:\app\administrator\product\11.2.0\client_1
```

Note: If you define *ORACLE_HOME*, the JDBC OCI driver locates the Oracle Net Services files in the `network\admin` directory of the Oracle home directory. If you define *TNS_ADMIN*, the JDBC OCI driver locates the Oracle Net Services files in the specified directory.

Modifying the Oracle Database Adapter service form for OCI

To configure OCI communication between the Oracle adapter and the Oracle database, you must modify the Oracle adapter service form.

Procedure

1. Select the **Use OCI communication with Oracle** check box.

If the **Use OCI communication with Oracle** check box is selected, the adapter uses the JDBC OCI driver to communicate with the Oracle database server. When this check box is not selected, the adapter uses the JDBC Thin driver to communicate with the Oracle database server.

2. Enter a value for the **Oracle Service Alias** field that corresponds to the net service alias listed in the `tnsnames.ora` file.

The net service alias name is on the left side of the equals (=) sign in the `tnsnames.ora` file. The example `tnsnames.ora` file in [“Configuring Oracle Net Services”](#) on page 45 uses `PRODONE` as the net service name for TAF. For this example configuration, enter `PRODONE` in the **Oracle Service Alias** field.

What to do next

If you are using the JDBC OCI driver, and you want to use SSL communication, then you must complete further configuration. The **Use SSL communication with Oracle** check box is only for the JDBC Thin driver. To enable SSL communication between the Oracle adapter and the Oracle database for the JDBC OCI driver, you must include SSL information in the Oracle Net Services files.

The information in the following files serves as an example of how you can configure Transparent Application Failover with SSL:

`sqlnet.ora`:

```
SQLNET.AUTHENTICATION_SERVICES= (TCPS)
NAMES.DIRECTORY_PATH= (TNSNAMES)

SSL_VERSION = 3.0
SSL_CLIENT_AUTHENTICATION = FALSE
SSL_SERVER_DN_MATCH = YES
```



```

WALLET_LOCATION =
  (SOURCE =
    (METHOD = FILE)
    (METHOD_DATA =
      (DIRECTORY = C:\temp\client)
    )
  )

```

tnsnames.ora:

```

PRODNESSSL =
(DESCRIPTION_LIST =
  (FAILOVER = true)
  (LOAD_BALANCE = false)
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCPS)(HOST = YourFirstHost)(PORT = 2484))
    )
    (CONNECT_DATA =
      (SERVER = dedicated)
      (FAILOVER_MODE =
        (BACKUP = PRODTWOSSL)
        (TYPE = select)
        (METHOD = basic)
        (RETRIES = 20)
        (DELAY = 3)
      )
    )
    (SERVICE_NAME = ORCL)
  )
  (SECURITY =
    (SSL_SERVER_CERT_DN = "CN=client, C=US")
  )
)
(DESCRIPTION =
  (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = TCPS)(HOST = YourSecondHost)(PORT = 2484))
  )
  (CONNECT_DATA =
    (SERVICE_NAME = ORCL)
  )
  (SECURITY =
    (SSL_SERVER_CERT_DN = "CN=client, C=US")
  )
)
)
)

PRODTWOSSL =
(DESCRIPTION_LIST =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCPS)(HOST = YourSecondHost)(PORT = 2484))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = ORCL)
    )
    (SECURITY =
      (SSL_SERVER_CERT_DN = "CN=client, C=US")
    )
  )
)
)
)

```

For more information about configuring SSL for the JDBC OCI driver, see the "Stores for Client Authentication" subsection of ["Configuring the SSL connection"](#) on page 53.

Related tasks

[Installing the JDBC OCI driver](#)

Transparent Application Failover (TAF) is a feature of the Java Database Connectivity (JDBC) Oracle Call Interface (OCI) driver. You must install the Oracle Database Client software on the IBM Security Directory Integrator target.

[Configuring the OCI connection](#)

You can enable OCI communication between the Oracle Database Adapter and the Oracle database. You must configure Oracle Net Services (ONS) on the Security Directory Integrator where the Oracle Client software is installed.

Configuring Network Data Encryption and Integrity for Thin JDBC Clients

Network data encryption and integrity for JDBC thin clients is a feature of Oracle Advanced security, which lets thin Java database connectivity (JDBC) clients to securely connect and communicate with the Oracle database.

About this task

To enable this feature, you must:

- Configure certain properties in the JDBC thin client properties file.
- Specify the file path on the service form containing these Java properties.

Procedure

1. Extract the adapter package.
2. Locate the `OraPropertiesFile` folder from the package.
3. Edit the `OraASO.properties` file.

This file contains several configuration properties. Identify the properties that match your setup and specify the values accordingly.

The following is an example content of the properties file

```
#OraASO.properties
oracle.net.encrypted_client=requested
oracle.net.encrypted_types_client=(AES256)
oracle.net.crypto_checksum_client=requested
oracle.net.crypto_checksum_types_client=SHA1
```

Note: The `OraASO.properties` file uses a standard format where the first line always contains a comment (#) or is empty. The succeeding lines define the different properties.

For more information on these properties and the possible values, see [Configuring JDBC thin clients](#).

4. Specify the properties file path for the Oracle advanced security option. See [Creating an adapter service](#).

Related concepts

[Configuring the Dispatcher properties](#)

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

[Customize table space quota sizes](#)

The adapter enables customizing the required quota size on the table spaces when you provision user accounts.

[Secure Sockets Layer \(SSL\) communication](#)

You can secure your environment by using Secure Sockets Layer (SSL) communication among Identity server, Security Directory Integrator, and the Oracle servers. You can configure SSL communication across the entire solution.

[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.

[Usage instructions for Oracle 12c support](#)

The Oracle DB adapter can be now used to manage Oracle 12c container database.

Related tasks

Customizing the adapter profile

To customize the adapter profile, you must modify the Oracle 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.

Enabling auditing on an Oracle resource

You must enable auditing on the database so that the Oracle Database Adapter can retrieve the last access date of the user account.

Configuring OCI for Transparent Application Failover

Transparent Application Failover (TAF) is a feature of the Java Database Connectivity (JDBC) Oracle Call Interface (OCI) driver. If you configure the adapter to use TAF, then the adapter can automatically reconnect to a secondary database instance if the original database connection fails.

Verifying that the adapter is working correctly

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

Secure Sockets Layer (SSL) communication

You can secure your environment by using Secure Sockets Layer (SSL) communication among Identity server, Security Directory Integrator, and the Oracle servers. You can configure SSL communication across the entire solution.

To use SSL communication between the system components, you can configure the Security Directory Integrator server as the SSL server. You can configure both the Identity server and the Oracle servers as SSL clients.

The two main communication channels that you can secure with SSL communication are depicted in Figure 1.

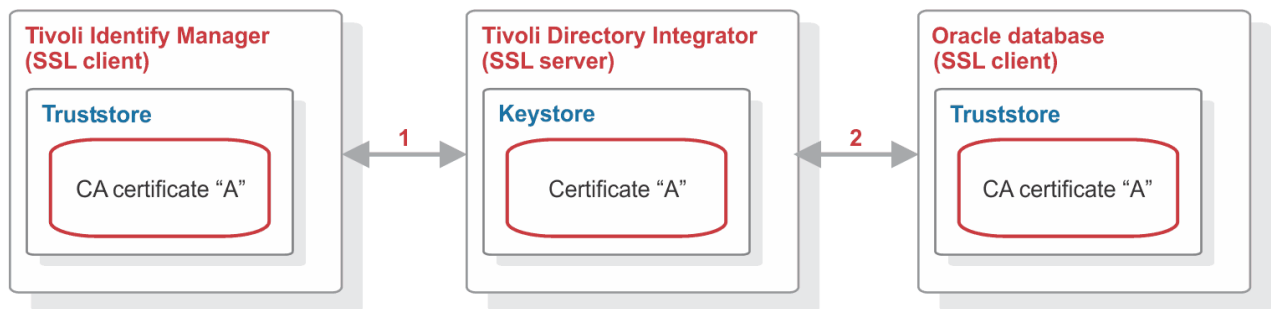


Figure 4. SSL communication overview

Each of these channels governs the communication between two main system components.

1

This channel includes communication between Identity server 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*.

2

This channel includes communication between Security Directory Integrator and the Oracle database server. To configure SSL communication for this channel, see [“Secure Sockets Layer \(SSL\) communication”](#) on page 51.

Note: Configuring SSL for each of these channels is optional. You can choose whether to configure SSL for neither, one or both channels.

Related concepts

Configuring the Dispatcher properties

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

Customize table space quota sizes

The adapter enables customizing the required quota size on the table spaces when you provision user accounts.

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.

Usage instructions for Oracle 12c support

The Oracle DB adapter can be now used to manage Oracle 12c container database.

Related tasks

Customizing the adapter profile

To customize the adapter profile, you must modify the Oracle 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.

Enabling auditing on an Oracle resource

You must enable auditing on the database so that the Oracle Database Adapter can retrieve the last access date of the user account.

Configuring OCI for Transparent Application Failover

Transparent Application Failover (TAF) is a feature of the Java Database Connectivity (JDBC) Oracle Call Interface (OCI) driver. If you configure the adapter to use TAF, then the adapter can automatically reconnect to a secondary database instance if the original database connection fails.

Configuring Network Data Encryption and Integrity for Thin JDBC Clients

Network data encryption and integrity for JDBC thin clients is a feature of Oracle Advanced security, which lets thin Java database connectivity (JDBC) clients to securely connect and communicate with the Oracle database.

Verifying that the adapter is working correctly

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

JDBC driver location for SSL

JDBC Thin driver version 10g Release 2 and above include SSL support. You can obtain the Oracle Database 10gR2, 11g, or 11gR2 driver from the following locations:

- The `ORACLE_HOME\jdbc\lib` directory of an Oracle database (client or server) installation.
- The JDBC Driver Downloads page on the [Oracle Technology Network](#) website.

Security Directory Integrator version 7.0

Use `ojdbc5.jar`, which is the driver for JDK 1.5.

Security Directory Integrator version 7.1

Use `ojdbc6.jar`, which is the driver for use with JDK 1.6.

You must copy the appropriate driver to one of the following locations on the Security Directory Integrator server:

- `TDI_HOME\jars\3rdparty\others`.
- `TDI_HOME\jvm\jre\lib\ext`.

where `TDI_HOME` is the directory where Security Directory Integrator is installed. For example, on a Windows platform, the default directory is `C:\Program Files\IBM\TDI\V7.x`.

You must also delete previous versions of the JDBC Thin driver from these two *TDI_HOME* locations. The previous versions of the driver are one or more of the following files:

- `ojdbc14.jar`
- `classes12.zip`
- `nls_charset12.zip`
- `classes111.zip`
- `nls_charset11.zip`

Note: The `.zip` files that are listed might be named as `.jar` files. For example, `classes12.jar`.

Configuring the SSL connection

To enable SSL communication between the Oracle adapter and the Oracle database, you must configure a truststore and optionally a keystore for the Dispatcher.

About this task

If the Oracle database requires SSL client authentication then you must configure a keystore.

To configure the truststore for the Dispatcher, you must import the certificate authority (CA) certificate to sign the certificate for the Oracle database.

Configuring server authentication

To configure SSL, you must first configure the server authentication by importing a CA certificate into the truststore.

Procedure

1. Run the following command to import a CA certificate into a truststore:

```
keytool -import -v -alias OACA -file CA.cer -keystore truststore.jks -storetype  
JKS -storepass "ThePwd12"
```

Note:

The location for the `truststore.jks` and the `solutions.properties` files are in the `ITDI_HOME\timsol` directory.

When you issue the **keytool** command to import the CA certificate, ensure that the truststore details match the `solution.properties` entries.

2. Set the following properties in the `solutions.properties` file:

```
## server authentication  
javax.net.ssl.trustStore=truststore.jks  
javax.net.ssl.trustStorePassword=ThePwd12  
javax.net.ssl.trustStoreType=jks
```

The store password, `ThePwd12`, is for test purposes only.

If the keystore properties are not set in the `solution.properties` file, use the same values as the truststore properties for these keystore entries:

```
## client authentication  
javax.net.ssl.keyStore=truststore.jks  
javax.net.ssl.keyStorePassword=ThePwd12  
javax.net.ssl.keyStoreType=jks
```

Configuring client authentication

If the Oracle database requires SSL client authentication, then you must configure a keystore.

About this task

To determine whether the Oracle database requires SSL client authentication, complete the following step.

Procedure

- Verify the `sqlnet.ora` file on the target Oracle database server, which is the managed resource, for the following line:

```
SSL_CLIENT_AUTHENTICATION = FALSE
```

The `FALSE` value means that the Oracle database server does NOT require SSL client authentication. The `TRUE` value means that the Oracle database server DOES require SSL client authentication.

Note: The store password `ThePwd12` is for test purposes only.

Example

For test purposes, you can use the following commands to set up a JKS type keystore:

```
cd c:\temp
mkdir clientjks

keytool -genkey -alias OADB -dname "CN=client,C=US" -storetype JKS -keystore
clientjks\client.jks -keyalg RSA -storepass "ThePwd12"

keytool -certreq -alias OADB -file clientjks\creq.cer -keystore clientjks\client.jks
-storepass "ThePwd12"

orapki cert create -wallet ./authority -request clientjks\creq.cer -cert
clientjks\signed.cer -validity 3650 -pwd=ThePwd12

keytool -import -v -alias OACA -file authority\CA.cer -keystore clientjks\client.jks
-storepass "ThePwd12"

keytool -import -v -alias OADB -file clientjks\signed.cer -keystore
clientjks\client.jks -storepass "ThePwd12"
```

These example commands assume that you created a self-signed certificate authority. See [“Configuring the Oracle database server”](#) on page 55.

What to do next

If the keystore properties are not set in the `solution.properties` file, then set the following properties accordingly:

```
## client authentication
javax.net.ssl.keyStore=client.jks
javax.net.ssl.keyStorePassword=ThePwd12
javax.net.ssl.keyStoreType=jks
```

Configuring the Oracle database server

Use Oracle tools, such as the Oracle Wallet Manager and the **orapki** command, to configure both the truststore and the keystore on the Oracle database server.

About this task

For test purposes, you can use the following commands to set up a self-signed certificate authority, truststore, and keystore:

```
cd c:\temp
mkdir authority
mkdir server
mkdir client
```

Self-signed certificate authority

```
orapki wallet create -wallet ./authority -pwd=ThePwd12

orapki wallet add -wallet ./authority -dn "CN=authority, C=US" -keysize 2048
-self_signed -validity 3650 -pwd=ThePwd12

orapki wallet export -wallet ./authority -dn "CN=authority, C=US" -cert
./authority/CA.cer -pwd=ThePwd12
```

Use the `CA.cer` file in the authority directory as the trusted certificate when you issue the **keytool** command to import a CA certificate into the Dispatcher truststore.

Stores for Server Authentication

```
orapki wallet create -wallet ./server -auto_login -pwd=ThePwd12

orapki wallet add -wallet ./server -dn "CN=server, C=US" -keysize 2048
-pwd=ThePwd12

orapki wallet export -wallet ./server -dn "CN=server, C=US" -request
./server/creq.cer -pwd=ThePwd12

orapki cert create -wallet ./authority -request ./server/creq.cer -cert
./server/signed.cer -validity 3650 -pwd=ThePwd12

orapki wallet add -wallet ./server -trusted_cert -cert ./authority/CA.cer
-pwd=ThePwd12

orapki wallet add -wallet ./server -user_cert -cert ./server/signed.cer
-pwd=ThePwd12
```

Stores for Client Authentication

```
orapki wallet create -wallet ./client -auto_login -pwd=ThePwd12

orapki wallet add -wallet ./client -dn "CN=client, C=US" -keysize 2048
-pwd=ThePwd12

orapki wallet export -wallet ./client -dn "CN=client, C=US" -request
./client/creq.cer -pwd=ThePwd12

orapki cert create -wallet ./authority -request ./client/creq.cer -cert
./client/signed.cer -validity 3650 -pwd=ThePwd12

orapki wallet add -wallet ./client -trusted_cert -cert ./authority/CA.cer
-pwd=ThePwd12

orapki wallet add -wallet ./client -user_cert -cert ./client/signed.cer
-pwd=ThePwd12
```

Oracle Network Configuration

Configure the following two files on the Oracle database server to enable SSL:

- listener.ora
- sqlnet.ora

These files are in the network\admin directory of the Oracle home directory. You can use Oracle Net Manager or a text editor to edit these files.

listener.ora:

```
SSL_VERSION = 3.0
SSL_CLIENT_AUTHENTICATION = FALSE

WALLET_LOCATION =
  (SOURCE =
    (METHOD = FILE)
    (METHOD_DATA =
      (DIRECTORY = myDir)
    )
  )

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)(HOST = myHost)(PORT = nonSSLPort))
    )
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCPS)(HOST = myHost)(PORT = sslPort))
    )
  )
```

sqlnet.ora:

```
SQLNET.AUTHENTICATION_SERVICES= (TCPS, NTS)
NAMES.DIRECTORY_PATH= (TNSNAMES)

SSL_VERSION = 3.0
SSL_CLIENT_AUTHENTICATION = FALSE

WALLET_LOCATION =
  (SOURCE =
    (METHOD = FILE)
    (METHOD_DATA =
      (DIRECTORY = myDir)
    )
  )
```

where:

myDir

The directory location of the truststore on the Oracle Database Server. For example C:\temp\server.

myHost

The server host name.

nonSSLPort

The non-SSL communication port (TCP protocol). For example, 1521.

sslPort

The SSL communication port (TCPS protocol). For example, 2484.

Modifying the Oracle Database Adapter service form for SSL

To enable SSL communication between the Oracle adapter and the Oracle database, you must configure the Oracle adapter service form.

About this task

Make the following changes to configure the Oracle Database Adapter service form.

Procedure

1. Select the **Use SSL communication with Oracle** check box.
2. Update the **Oracle Service Port** value to the TCPS port that is listed in the listener.ora file. For example, 2484.

3. (Optional) Provide a value for **Oracle Server Distinguished Name**.

If provided, the adapter verifies this value against the Oracle database server certificate.

Note:

- Start both the listener and database services as the user who created the wallet, so both services can access the wallet successfully. On Windows, change the **Log On As** account for the listener and database services from the default Local System account to wallet creator.
- The `sqlnet.ora` and the `listener.ora` files contain the wallet location. In most cases, both files contain the same wallet location, but the listener might use its own wallet.
 - Use the distinguished name of the certificate from the wallet in the `sqlnet.ora` file. The Oracle adapter verifies this name when you provide a value for the optional **Oracle Server Distinguished Name** on the service form.
 - For security, include a distinguished name in the service form to avoid the risk of a server that is faking its identity.
- For more information about configuring SSL with the Oracle driver, see the white paper "SSL with Oracle JDBC Thin Driver" on the [Oracle website](#).

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 to forego the new password requirement. You can configure the Oracle 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.dsm1` 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

Configuring the Dispatcher properties

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

Customize table space quota sizes

The adapter enables customizing the required quota size on the table spaces when you provision user accounts.

Secure Sockets Layer (SSL) communication

You can secure your environment by using Secure Sockets Layer (SSL) communication among Identity server, Security Directory Integrator, and the Oracle servers. You can configure SSL communication across the entire solution.

[Usage instructions for Oracle 12c support](#)

The Oracle DB adapter can be now used to manage Oracle 12c container database.

Related tasks

[Customizing the adapter profile](#)

To customize the adapter profile, you must modify the Oracle 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.

[Enabling auditing on an Oracle resource](#)

You must enable auditing on the database so that the Oracle Database Adapter can retrieve the last access date of the user account.

[Configuring OCI for Transparent Application Failover](#)

Transparent Application Failover (TAF) is a feature of the Java Database Connectivity (JDBC) Oracle Call Interface (OCI) driver. If you configure the adapter to use TAF, then the adapter can automatically reconnect to a secondary database instance if the original database connection fails.

[Configuring Network Data Encryption and Integrity for Thin JDBC Clients](#)

Network data encryption and integrity for JDBC thin clients is a feature of Oracle Advanced security, which lets thin Java database connectivity (JDBC) clients to securely connect and communicate with the Oracle database.

[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

[Configuring the Dispatcher properties](#)

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

[Customize table space quota sizes](#)

The adapter enables customizing the required quota size on the table spaces when you provision user accounts.

[Secure Sockets Layer \(SSL\) communication](#)

You can secure your environment by using Secure Sockets Layer (SSL) communication among Identity server, Security Directory Integrator, and the Oracle servers. You can configure SSL communication across the entire solution.

[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.

Usage instructions for Oracle 12c support

The Oracle DB adapter can be now used to manage Oracle 12c container database.

Related tasks

Customizing the adapter profile

To customize the adapter profile, you must modify the Oracle 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.

Enabling auditing on an Oracle resource

You must enable auditing on the database so that the Oracle Database Adapter can retrieve the last access date of the user account.

Configuring OCI for Transparent Application Failover

Transparent Application Failover (TAF) is a feature of the Java Database Connectivity (JDBC) Oracle Call Interface (OCI) driver. If you configure the adapter to use TAF, then the adapter can automatically reconnect to a secondary database instance if the original database connection fails.

Configuring Network Data Encryption and Integrity for Thin JDBC Clients

Network data encryption and integrity for JDBC thin clients is a feature of Oracle Advanced security, which lets thin Java database connectivity (JDBC) clients to securely connect and communicate with the Oracle database.

Usage instructions for Oracle 12c support

The Oracle DB adapter can be now used to manage Oracle 12c container database.

However, the Central Database (CDB) and each Pluggable Database (PDB) that are connected to it, must be managed separately through separate services from IBM Security Verify Governance.

Adapter user account for managing the Oracle 12c container database:

- CDB can be managed by using common users
- PDB can be managed by using local users only

Add/Modify account operation

For CDB:

- A root container service must create an account name that starts with C##. If it tries to create a user without C## in username, an error is thrown.
- When a common user is creating a common user account, the DEFAULT TABLESPACE, TEMPORARY TABLESPACE, QUOTA, and PROFILE must reference objects that exist in all containers. So, if the object does not exist in all containers, it throws an error.
- To assign/grant a privilege to common user commonly we need to provide container value as CONTAINER=ALL.

For PDB:

- A PDB container service must not create an account starting with C##. If it tries to create user with C## in username, error is thrown.

Reconciliation Operations

- For CDB: Common users are managed through CDB services.
- For PDB: Only local users are managed through PDB services.

Related concepts

Configuring the Dispatcher properties

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

Customize table space quota sizes

The adapter enables customizing the required quota size on the table spaces when you provision user accounts.

Secure Sockets Layer (SSL) communication

You can secure your environment by using Secure Sockets Layer (SSL) communication among Identity server, Security Directory Integrator, and the Oracle servers. You can configure SSL communication across the entire solution.

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 Oracle 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.

Enabling auditing on an Oracle resource

You must enable auditing on the database so that the Oracle Database Adapter can retrieve the last access date of the user account.

Configuring OCI for Transparent Application Failover

Transparent Application Failover (TAF) is a feature of the Java Database Connectivity (JDBC) Oracle Call Interface (OCI) driver. If you configure the adapter to use TAF, then the adapter can automatically reconnect to a secondary database instance if the original database connection fails.

Configuring Network Data Encryption and Integrity for Thin JDBC Clients

Network data encryption and integrity for JDBC thin clients is a feature of Oracle Advanced security, which lets thin Java database connectivity (JDBC) clients to securely connect and communicate with the Oracle database.

Verifying that the adapter is working correctly

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

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 63 contains warnings or errors which might be displayed in the user interface if the Oracle Database Adapter is installed on your system.

Message code	Warning or error message	Remedial action
CTGIMT001E	The following error occurred. Error: Either the Oracle service name is incorrect or the service is not up.	Ensure that the Oracle service name given on IBM Security Verify Governance service form is running.
CTGIMT001E	The following error occurred. Error: Either the Oracle host or port is incorrect.	Verify that the host workstation name or the port for the Oracle service is correctly specified.
CTGIMT002E	The login credential is missing or incorrect.	Verify that you provided correct login credential on service form.
CTGIMT001E	The following error occurred. Error: No suitable JDBC driver found.	Ensure that the correct version of the JDBC 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 cannot establish a connection with IBM Security Directory Integrator. To fix this problem, ensure that: <ul style="list-style-type: none"> • IBM Security Directory Integrator is running. • The URL specified on the service form for the IBM Security Directory Integrator is correct.

Table 7. Warning and error messages (continued)

Message code	Warning or error message	Remedial action
CTGIMT004E	The adapter does not have permission to add an account: <i>Account_Name</i> .	<p>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. These privileges are the minimum required for the administrator user:</p> <ul style="list-style-type: none"> • CREATE USER • ALTER USER • DROP USER • SELECT ANY TABLE • GRANT ANY ROLE • GRANT ANY PRIVILEGE • EXECUTE ANY PROCEDURE • ADMINISTER_RESOURCE_MANAGER • SELECT ANY DICTIONARY <p>Note: To use the following Stored Procedure, you must provide EXECUTE ANY PROCEDURE and ADMINISTER_RESOURCE_MANAGER privileges to the administrator user:</p> <ul style="list-style-type: none"> • dbms_resource_manager_privs.grant_switch_consumer_group • DBMS_RESOURCE_MANAGER_PRIVS.REVOKE_SWITCH_CONSUMER_GROUP • dbms_resource_manager.set_initial_consumer_group • DBMS_WM.RevokeSystemPriv
CTGIMT003E	The account already exists.	Use different name for the user to be added.
CTGIMT015E	An error occurred while deleting the <i>Account_Name</i> 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

The Oracle Database Adapter installation installs the `oracledbsql` folder on the Security Directory Integrator server. Remove the `oracledbsql` folder to uninstall the Oracle Database Adapter.

Procedure

1. Stop the adapter service.
2. Remove `oracledbsql` folder from the `ITDI_HOME\timso1` folder.

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.

Related tasks

[Uninstalling the adapter stored procedures from the Oracle Database](#)

Uninstalling the adapter stored procedures from the Oracle Database

Procedure

1. Remove the `ISIM_SET_DEF_CONGROU` stored procedure by executing the SQL command on the Oracle Database: `Drop procedure ISIM_SET_DEF_CONGROU_version`
Note: The version corresponds to the adapter version. For example: If the adapter version is 5.1.18.72, the stored procedure command is `ISIM_SET_DEF_CONGROU_5111872`
2. Remove the `ISIM_OBTAIN_LOCK` stored procedure by executing the SQL command on the Oracle Database: `Drop procedure ISIM_OBTAIN_LOCK_version`

Note: The version corresponds to the adapter version. For example: If the adapter version is 5.1.18.72, the stored procedure command is `ISIM_OBTAIN_LOCK_5111872`

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.

Related tasks

[Uninstalling the adapter](#)

The Oracle Database Adapter installation installs the `oracledbsql` folder on the Security Directory Integrator server. Remove the `oracledbsql` folder to uninstall the Oracle Database Adapter.

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 product documentation.

Related tasks

[Uninstalling the adapter](#)

The Oracle Database Adapter installation installs the `oracledbsql` folder on the Security Directory Integrator server. Remove the `oracledbsql` folder to uninstall the Oracle Database Adapter.

[Uninstalling the adapter stored procedures from the Oracle Database](#)

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. This topic is not applicable for this adapter.

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

Table 8 on page 67 is a listing of the attributes that are used by the Oracle Database Adapter. The table gives a brief description and corresponding column on the Oracle database (if applicable) for the value of the attribute.

Attribute	Description	Oracle column or table
erOraServiceName	The SID/Service Name of the Oracle instance.	NA
erOraSysPriv	The System Privilege assigned to the user.	PRIVILEGE/DBA_SYS_PRIV
erOraDefaultTableSpace	The name of the default table space.	DEFAULT_TABLESPACE/DBA_USERS
erOraTemporaryTableSpace	The name of the temporary table space.	TEMPORARY_TABLESPACE/DBA_USERS
erOraTblSpcQuota	The maximum space allowed on a table space.	MAX_BYTES/DBA_TS_QUOTA
erOraAuthenticationType	Specifies how the user is authenticated by Oracle.	PASSWORD/DBA_USERS
erOraGlobalName	An external name that identifies the user.	EXTERNAL_NAME/DBA_USERS
erOraTblspacesName	The name for the erOraTablespaces group.	TABLESPACE_NAME/DBA_TABLESPACES
erOraPrflName	The name for the erOraProfiles group.	PROFILE/DBA_PROFILES
erOraRolesName	The name for the erOraRoles group.	ROLE/DBA_ROLES
erOraRole	The database roles assigned as default roles to the account.	ROLE, DEFAULT_ROLE/DBA_ROLE_PRIV
erOraNonDefRole	The database roles assigned as non default roles (for example, password protected roles) to the account.	ROLE, DEFAULT_ROLE/DBA_ROLE_PRIV
erOraProfile	The profile name assigned to the account.	PROFILE/DBA_USERS
erOraExpirePwd	If true, set the password to expire.	ACCOUNT_STATUS/DBA_USERS
erOraProxyUsers	The proxy user for this user.	PROXY/PROXY_USERS
erOraRsrcConsumerGroup	The consumer group that a user can switch to.	GRANTED_GROUP/ DBA_RSRC_CONSUMER_GROUP_PRIVS

Table 8. Attributes, object identifiers, descriptions, and corresponding column/table name on the Oracle database (continued)

Attribute	Description	Oracle column or table
erOraServiceHost	The host workstation where the Oracle service is running.	NA
erOraServicePort	The port on which the Oracle service is listening.	NA
erOraDefRsrcConsumerGroup	The default or initial resource consumer group for a user. If this attribute is not assigned to any value, the default value, DEFAULT_CONSUMER_GROUP, is used. This attribute can have either above default value or some value from the resource consumer group list that are allowed for the user (though resource consumer group is multivalued attribute). Assigning any value outside this list will result in error on the resource. The erOraRsrcConsumerGroup and erOraDefRsrcConsumerGroup must have the same value.	INITIAL_RSRC_CONSUMER_GROUP/DBA_USERS
erOraExpiryDate	The expiry date of an Oracle account.	ACCOUNT_STATUS
erOraCreateDate	The creation date of an Oracle account.	CREATED
erOraLockDate	The lock date of an Oracle account.	LOCK_DATE
erOraAccountStatusstr	The account status of an Oracle account.	ACCOUNT_STATUS
erServiceUid	The Oracle resource administrator ID.	NA
erPassword	The password for Oracle administrator.	PASSWORD/DBA_USERS
erUid	The login name.	USERNAME/DBA_USERS
erAccountStatus	The status of the account either enabled or disabled.	ACCOUNT_STATUS/DBA_USERS
eroradonotcascadedelete	Do not Cascade on Delete.	NA
eroraasoproperties	JDBC Thin Client Properties File Path	NA

Adapter attributes by operations

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

System Login Add

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

Table 9. Add request attributes for Oracle

Required attribute	Optional attribute
erUid	All other supported attributes

System Login Change

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

<i>Table 10. Change request attributes for Oracle</i>	
Required attribute	Optional attribute
erUid	All other supported attributes

System Login Delete

A System Login Delete is a request to remove the specified user from the Oracle database.

<i>Table 11. Delete request attributes for Oracle</i>	
Required attribute	Optional attribute
erUid	None

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.

<i>Table 12. Suspend request attributes for Oracle</i>	
Required attribute	Optional attribute
erUid erAccountStatus	None

System Login Restore

A System Login Restore is a request to activate a user account that was previously suspended. After an account is restored, the user can access the system by using the same attributes as the ones before the Suspend function was called.

<i>Table 13. Restore request attributes for Oracle</i>	
Required attribute	Optional attribute
erUid erAccountStatus	None

Test

You can use attributes to test the connection.

<i>Table 14. Test attributes</i>	
Required attribute	Optional attribute
None	None

Reconciliation

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

<i>Table 15. Reconciliation request attributes for Oracle</i>	
Required attribute	Optional attribute
None	None

Special attributes

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

Index

A

- accounts
 - required privileges [26](#)
 - restoration
 - business processes [57](#)
 - password requirements [57](#)
 - service creation [26](#)
- adapter
 - customization steps [37](#)
 - features [1](#)
 - installation
 - obtaining software [14](#)
 - prerequisites [14](#)
 - profile import [14](#)
 - troubleshooting errors [61](#)
 - user account creation [14](#)
 - verifying [58](#)
 - warnings [61](#)
 - worksheet [9](#)
 - overview [1](#)
 - profile
 - upgrading [35](#)
 - supported configurations [2](#)
 - task automation [1](#)
 - uninstall [65](#)
 - upgrading [35](#)
 - user account management tasks [1](#)
- adapters
 - removing profiles [66](#)
- attributes
 - testing connection [69](#)
- auditing
 - enabling [42](#)
 - on database [42](#)
- authentication
 - CA certificate import [53](#)
 - client, configuring [54](#)
 - keystore [54](#)
 - server, configuring [53](#)

C

- client
 - authentication, configuring [54](#)
 - keystore [54](#)
- configurations
 - adapter [2](#)
 - Dispatcher properties [40](#)
 - overview [2](#)
- connection
 - OCI, configuring [45](#)
 - testing [69](#)

D

- database

- database (*continued*)
 - System Login Delete [69](#)
- definition
 - certificate authority [51](#)
 - certificates [51](#)
 - private key [51](#)
- directory integrator
 - uninstalling the adapter [65](#)
- dispatcher
 - installation [13](#)
- Dispatcher
 - configuration properties [40](#)
 - upgrading [35](#)
- download, software [8](#)

E

- error messages [63](#)

F

- first steps after installation [37](#)

I

- iKeyman utility [51](#)
- installation
 - adapter
 - software [14](#)
 - first steps following [37](#)
 - uninstall [65](#)
 - verification
 - adapter [58](#)
 - worksheet [9](#)

J

- JDBC driver, location for SSL [52](#)

K

- key management utility, iKeyman [51](#)

M

- messages
 - error [63](#)
 - warning [63](#)
- MS-DOS ASCII characters [39](#)

O

- OCI
 - configuring for the resource [43](#)
- Oracle Adapter service form

- Oracle Adapter service form (*continued*)
 - modifying [56](#)
 - OCI [48](#)
- Oracle database server
 - configuring
 - keystore [55](#)
 - Oracle tools [55](#)
 - truststore [55](#)
- Oracle Net Services
 - Instant Client installation [45](#)
 - Transparent Application Failover [45](#)
- overview, adapter [1](#)

P

- private key, definition [51](#)
- privileges
 - required [26](#)
 - user account [26](#)
- profile
 - editing on UNIX or Linux [39](#)
- properties
 - configuring the Dispatcher [40](#)
- protocol
 - SSL, overview [51](#)

R

- Reconciliation request [70](#)
- removing
 - adapter profiles [66](#)
- requests
 - Reconciliation [70](#)
 - System Login Add [68](#)
 - System Login Change [69](#)
 - System Login Delete [69](#)
 - System Login Restore [69](#)
 - System Login Suspend [69](#)

S

- server authentication, configuring [53](#)
- service
 - restart [15](#)
 - start [15](#)
 - stop [15](#)
- software
 - download [8](#)
 - website [8](#)
- SSL
 - certificate installation [51](#)
 - communication
 - keystore and truststore [53](#)
 - Oracle adapter and database [53](#)
 - connection [53](#)
 - JDBC driver [52](#)
 - overview [51](#)
- System Login Add request [68](#)
- System Login Change request [69](#)
- System Login Delete request [69](#)
- System Login Restore request [69](#)
- System Login Suspend request [69](#)

T

- TAF, configuring for the resource [43](#)
- Transparent Application Failover, configuring for the resource [43](#)
- troubleshooting
 - error messages [63](#)
 - identifying problems [61](#)
 - techniques for [61](#)
 - warning messages [63](#)
- troubleshooting and support
 - troubleshooting techniques [61](#)

U

- uninstallation [65](#)
- uninstalling, adapter from the directory integrator [65](#)
- upgrades
 - adapter [35](#)
 - adapter profile [37](#)
 - adapter profiles [35](#)
 - dispatcher [35](#)
- user account
 - Reconciliation [70](#)
 - required privileges [26](#)
 - service creation [26](#)

V

- verification
 - dispatcher installation [13](#)
 - installation [58](#)
- vi command [39](#)

W

- warning messages [63](#)

