

IBM Security Verify Identity
7.0

*Oracle eBS 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..... 8
- Chapter 3. Installing..... 11**
 - Installing the dispatcher.....11
 - Installing the adapter binaries or connector.....12
 - Restarting the adapter service..... 13
 - Importing the adapter profile..... 14
 - Attribute mapping..... 15
 - Deploying the custom subforms.....17
 - Installing the Complex Attribute Handler..... 18
 - Creating an adapter service/target.....19
 - Service/Target form details..... 22
 - Installing the adapter language package..... 25
 - Verifying that the adapter is working correctly..... 26
- Chapter 4. Upgrading.....29**
 - Upgrading the dispatcher..... 29
 - Upgrading the adapter profile..... 29
- Chapter 5. Configuring..... 31**
 - Enabling SSL communication..... 31
 - Configuring Oracle eBS database tier..... 31
 - Configuring the Security Directory Integrator for Oracle eBS database tier authentication..... 33
 - Configuring Security Directory Integrator for Oracle eBS Adapter authentication..... 33
 - Changes to the adapter service form..... 34
 - JDBC driver location for SSL..... 34
 - Customizing the adapter profile..... 35
 - Editing adapter profiles on the UNIX or LINUX operating system..... 36
 - Password management when restoring accounts..... 36
 - Verifying that the adapter is working correctly..... 37
- Chapter 6. Troubleshooting..... 39**
 - Techniques for troubleshooting problems..... 39
 - Error messages and problem solving..... 40

Chapter 7. Uninstalling.....	43
Uninstalling the dispatcher.....	43
Deleting the adapter profile.....	43
Chapter 8. Reference.....	45
Adapter attributes and object classes.....	45
Adapter attributes by operations.....	47
System Login Add.....	47
System Login Change.....	48
System Login Delete.....	48
System Login Suspend.....	49
System Login Restore.....	49
Test.....	50
Reconciliation.....	50
Index.....	53

Figures

- 1. The architecture of the Oracle eBS Adapter..... 2
- 2. Example of a single server configuration..... 3
- 3. Example of a multiple server configuration..... 3

Tables

- 1. Prerequisites to run the adapter..... 7
- 2. Required information to install the adapter.....8
- 3. Warning and error messages 41
- 4. Attributes, descriptions, constraints, and permissions..... 45
- 5. Add request attributes for Oracle..... 47
- 6. Change request attributes for Oracle..... 48
- 7. Suspend request attributes for Oracle..... 49
- 8. Restore request attributes for Oracle..... 49
- 9. Test attributes..... 50
- 10. Reconciliation request attributes for Oracle..... 50

Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server. The Oracle eBS Adapter enables communication between the Identity server and the Oracle eBS user database, also known as the FND_USER directory.

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.

Automated user account management tasks include:

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

Related concepts

Architecture of the adapter

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

Supported configurations

The adapter supports both single and multiple server configurations.

Architecture of the adapter

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

The adapter contains Security Directory Integrator AssemblyLines that serve one or more account operation. When IBM® Security Verify Identity sends the first request, the required AssemblyLine is loaded into the Security Directory Integrator. The same Assemblyline is then cached to serve subsequent operations of the same type.

You must install the following components for the adapter to function correctly:

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

You need to install the RMI 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.

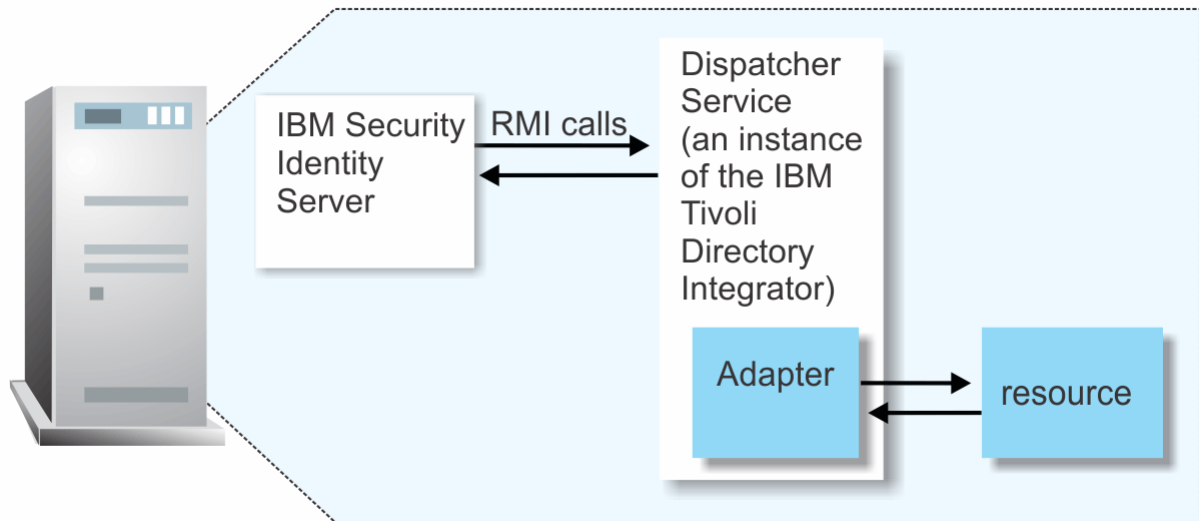


Figure 1. The architecture of the Oracle eBS Adapter

Related concepts

Features of the adapter

The adapter automates several administrative and management tasks.

Supported configurations

The adapter supports both single and multiple server configurations.

Supported configurations

The adapter supports both single and multiple server configurations.

The 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 Tivoli® Directory Integrator server, and the Oracle eBS Adapter on one server to establish communication with the Oracle eBS. The Oracle eBS is installed on a different server as described [Figure 2 on page 3](#).

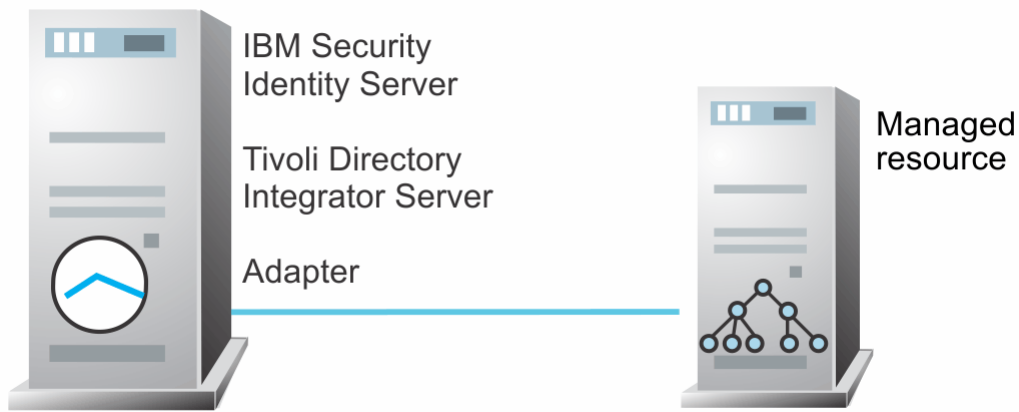


Figure 2. Example of a single server configuration

Multiple server configuration

In a multiple server configuration, install the Identity server, the Security Directory Integrator server, the Oracle eBS Adapter, and the Oracle eBS on different servers.

Install the Security Directory Integrator server and the Oracle eBS Adapter on the same server as described in [Figure 3 on page 3](#).

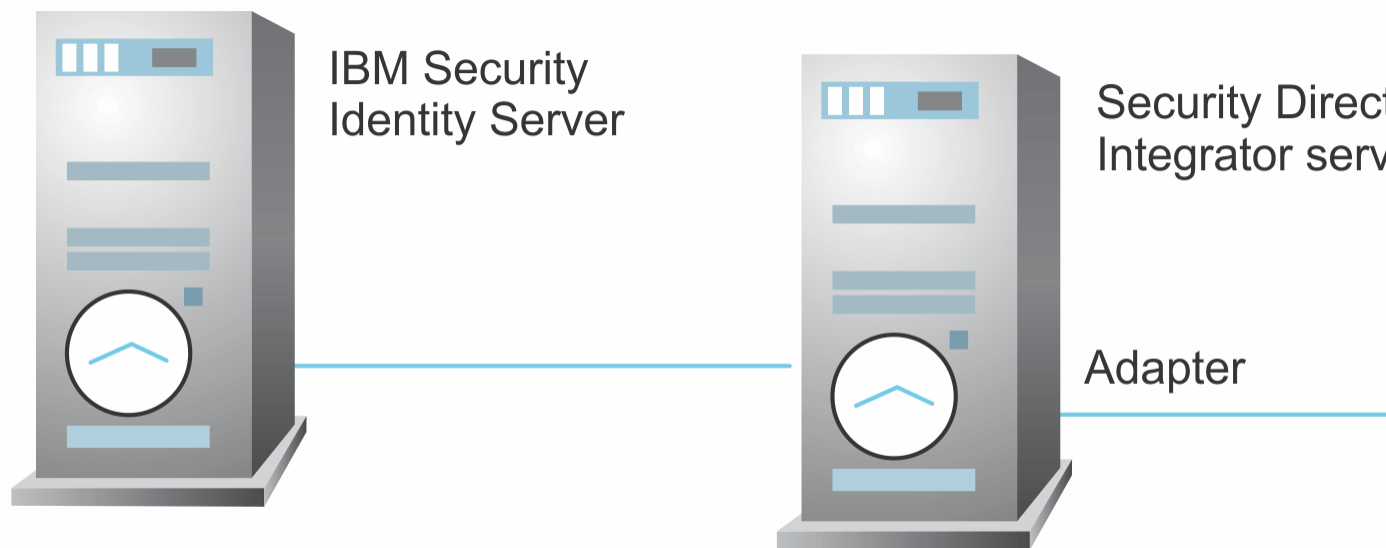


Figure 3. Example of a multiple server configuration

Related concepts

Features of the adapter

The adapter automates several administrative and management tasks.

Architecture of the adapter

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

Chapter 2. Planning

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

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

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

Pre-installation

Complete these tasks.

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

Installation

Complete these tasks.

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

Upgrade

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

Configuration

Complete these tasks.

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

Troubleshooting

See the following topics.

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

Uninstallation

Complete these tasks.

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

Reference

See the following topics.

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

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.

Note: See the release notes in the adapter package for the most current list of requirements.

Table 1. Prerequisites to run the adapter

Prerequisite	Description
Directory Integrator	<ul style="list-style-type: none"> • IBM Security Directory Integrator Version 7.1.1 + 7.1.1-TIV-TDI-FP0004 + 7.2.0-ISS-SDI-LA0008 • IBM Security Directory Integrator Version 7.2 <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"> • Identity server Version 10.0 • Identity server Version 10.0 • IBM Security Privileged Identity Manager Version 2.0 • Identity server Version 10.0
Oracle e-Business Suite	<p>A system that runs the Oracle eBS release:</p> <ul style="list-style-type: none"> • 12.0 • 12.1.1 • 12.1.3 • 12.2.4
Oracle Thin JDBC Driver	<p>All the listed JDBC driver can talk with all the supported version of Oracle except Oracle 10g r2:</p> <ul style="list-style-type: none"> • JDBC 8.1.7 Driver • JDBC 9.0.1 Driver <p>For Oracle 10g r2:</p> <ul style="list-style-type: none"> • JDBC 10.2.0.1.0 Driver
Network Connectivity	<p>The adapter must be installed on a system that can communicate with the IBM Security Verify Identity service through the TCP/IP network.</p>
System Administrator Authority	<p>To complete the adapter installation procedure, you must have system administrator authority.</p>
Security Directory Integrator adapters solution directory	<p>A Security Directory Integrator adapters solution directory is a Security Directory Integrator work directory for adapters. See the <i>Dispatcher Installation and Configuration Guide</i>.</p>

For information about the prerequisites and supported operating systems for Security Directory Integrator, see the *IBM Security Directory Integrator 7.1: Administrator Guide*.

Related concepts

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

Software downloads

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

Installation worksheet

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

Software downloads

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

Go to [IBM Passport Advantage](#).

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

Note:

You can also obtain additional adapter information from IBM Support.

Related concepts

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

Prerequisites

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

Installation worksheet

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

Installation worksheet

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

Table 2 on page 8 identifies the information that you need before installing the adapter.

Required information	Description	Value
Security Directory Integrator Home Directory	The <code>ITDI_HOME</code> directory contains the <code>jars/connectors</code> subdirectory that contains adapter JAR files. For example, the <code>jars/connectors</code> subdirectory contains the JAR files for the UNIX adapter.	Windows: <ul style="list-style-type: none">for version 7.1: <code>drive\Program Files\IBM\TDI\V7.1</code> UNIX: <ul style="list-style-type: none">for version 7.1: <code>/opt/IBM/TDI/V7.1</code>

Table 2. Required information to install the adapter (continued)

Required information	Description	Value
Adapters solution directory	For more information about the adapter solution directory, see the <i>Dispatcher Installation and Configuration Guide</i> .	<p>Windows:</p> <ul style="list-style-type: none"> for version 7.1: <code>drive\Program Files\IBM\TDI\V7.1\timsol</code> <p>UNIX:</p> <ul style="list-style-type: none"> for version 7.1: <code>/opt/IBM/TDI/V7.1/timsol</code>

Related concepts

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

[Prerequisites](#)

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

[Software downloads](#)

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

Chapter 3. Installing

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

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

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

Installing the dispatcher

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

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

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

Related concepts

Restarting the adapter service

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

Service/Target form details

Complete the service/target form fields.

Installing the adapter language package

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

Related tasks

Installing the adapter binaries or connector

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

Importing the adapter profile

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

Attribute mapping

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

Deploying the custom subforms

The Oracle eBS Adapter is supplied with custom subforms to specify the roles, responsibilities, and securing attributes associated with a user. The subforms are contained in the `0raEBSSubForms.zip` file.

Installing the Complex Attribute Handler

An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Creating an adapter service/target

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

Verifying that the adapter is working correctly

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

Installing the adapter binaries or connector

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

Before you begin

- The Dispatcher must be installed.

About this task

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

Related concepts

Installing the dispatcher

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

Restarting the adapter service

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

Service/Target form details

Complete the service/target form fields.

Installing the adapter language package

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

Related tasks

Importing the adapter profile

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

Attribute mapping

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

Deploying the custom subforms

The Oracle eBS Adapter is supplied with custom subforms to specify the roles, responsibilities, and securing attributes associated with a user. The subforms are contained in the `0raEBSSubForms.zip` file.

Installing the Complex Attribute Handler

An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Creating an adapter service/target

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

Verifying that the adapter is working correctly

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

Restarting the adapter service

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

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

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

Related concepts

Installing the dispatcher

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

Service/Target form details

Complete the service/target form fields.

Installing the adapter language package

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

Related tasks

Installing the adapter binaries or connector

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

Importing the adapter profile

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

Attribute mapping

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

Deploying the custom subforms

The Oracle eBS Adapter is supplied with custom subforms to specify the roles, responsibilities, and securing attributes associated with a user. The subforms are contained in the `OraEBSSubForms.zip` file.

Installing the Complex Attribute Handler

An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Creating an adapter service/target

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

Verifying that the adapter is working correctly

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

Importing the adapter profile

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

Before you begin

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

About this task

Service definition files are also called adapter profile files.

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

Procedure

1. Log on to the Identity server by using an account that has the authority to perform administrative tasks.
2. From the navigation tree, select **Configure System > Manage Service Types**.
The **Manage Service Types** page is displayed.
3. On the **Manage Service Types** page, click **Import**.
The **Import Service Type** page is displayed.
4. On the **Import Service Type** page, complete these steps:
 - a) In the **Service Definition File** field, type the directory location of the `<Adapter>Profile.jar` file, or click **Browse** to locate the file.
For example, if you are installing the IBM Security Verify Adapter for a Windows server that runs Active Directory, locate and import the `ADProfileJAR` file.
 - b) Click **OK** to import the file.

Results

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

What to do next

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

Related concepts

Installing the dispatcher

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

Restarting the adapter service

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

Service/Target form details

Complete the service/target form fields.

Installing the adapter language package

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

Related tasks

Installing the adapter binaries or connector

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

Attribute mapping

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

Deploying the custom subforms

The Oracle eBS Adapter is supplied with custom subforms to specify the roles, responsibilities, and securing attributes associated with a user. The subforms are contained in the `OraEBSSubForms.zip` file.

Installing the Complex Attribute Handler

An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Creating an adapter service/target

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

Verifying that the adapter is working correctly

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

Attribute mapping

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

About this task

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

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

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

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

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

Note:

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

Procedure

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

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

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

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

5. Import the updated mapping definition file through the Target Administration module. For more information, see *Attribute-to-permission mapping service* in the IBM Security Verify Governance Identity Manager product documentation.

Related concepts

Installing the dispatcher

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

Restarting the adapter service

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

Service/Target form details

Complete the service/target form fields.

Installing the adapter language package

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

Related tasks

Installing the adapter binaries or connector

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

Importing the adapter profile

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

Deploying the custom subforms

The Oracle eBS Adapter is supplied with custom subforms to specify the roles, responsibilities, and securing attributes associated with a user. The subforms are contained in the OraEBSSubForms.zip file.

Installing the Complex Attribute Handler

An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Creating an adapter service/target

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

Verifying that the adapter is working correctly

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

Deploying the custom subforms

The Oracle eBS Adapter is supplied with custom subforms to specify the roles, responsibilities, and securing attributes associated with a user. The subforms are contained in the `OraEBSSubForms.zip` file.

Before you begin

Extract the contents of the `OraEBSSubForms.zip` file to the subforms folder of the installed IBM Security Verify Identity web application.

For a self service console installation

`WAS_PROFILE_HOME/installedApps/nodeName/ITIM.ear/itim_self_service.war`

For an administrative console installation

`WAS_PROFILE_HOME/installedApps/nodeName/ITIM.ear/itim_console.war`

For Identity Service Center installation

`WAS_PROFILE_HOME/installedApps/nodeName/ITIM.ear/isim_isc_subform.war`

About this task

In a clustered environment the subform must be deployed on each WebSphere application server. If WebSphere version 6.1 is being used, the **jdkSourceLevel JSP** engine configuration parameter must be set to 15 for each web application on which the subforms are deployed.

Procedure

1. Open the `WEB-INF/ibm-web-ext.xmi` file from the configuration directory.
For example, `WAS_PROFILE_HOME/config/cells/cellName/applications/ITIM.ear/deployments/ITIM/webModuleName`. The `webModuleName` is the `itim_self_service.war` file or the `itim_console.war` file or both.
2. Add the following tag within the content of the `webappext:webAppExtension` tag:

```
<jspAttributes xmi:id="JSPAttribute_1" name="jdkSourceLevel" value="15"/>
```

Note: The integer `n` in `JSPAttribute_n` has to be unique within the file.

3. Save the file.
4. Take one of the following actions:
 - Restart the IBM Security Verify Identity application from the WebSphere Administrative Console.
 - Restart the service.

Related concepts

Installing the dispatcher

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

Restarting the adapter service

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

Service/Target form details

Complete the service/target form fields.

Installing the adapter language package

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

Related tasks

Installing the adapter binaries or connector

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

Importing the adapter profile

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

Attribute mapping

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

Installing the Complex Attribute Handler

An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Creating an adapter service/target

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

Verifying that the adapter is working correctly

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

Installing the Complex Attribute Handler

An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

About this task

The complex attribute handler enables IBM Security Verify Identity to define accesses on service groups that require additional values when assigned to an account. The access will be defined on the group name only, and the complex attribute handler will internally supply the default values that are needed for the composition value sent to the adapter.

For the Oracle eBS Adapter, Versions 6.0.10, 7.0.10 and later, you can expose an Oracle eBS responsibility as an access.

The complex attribute handler is provided as a Java class jar file that must be deployed on the IBM Security Verify Identity server. The minimum IBM Security Verify Identity version level required is IBM Security Verify Identity, Version 7.0.1 Fix Pack 1.

Procedure

1. From the top-level menu of the Appliance Dashboard, navigate to **Configure > Advanced Configuration > External Library**.
2. Select **New** to open the **Add External Library** window.
3. Browse to upload the `OraEBSHandler.jar` file.

4. Click **Save Configuration** to complete this task.
5. From **Server Control Menu**, select **Security Identity Manager Server > Restart**.

Related concepts

Installing the dispatcher

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

Restarting the adapter service

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

Service/Target form details

Complete the service/target form fields.

Installing the adapter language package

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

Related tasks

Installing the adapter binaries or connector

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

Importing the adapter profile

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

Attribute mapping

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

Deploying the custom subforms

The Oracle eBS Adapter is supplied with custom subforms to specify the roles, responsibilities, and securing attributes associated with a user. The subforms are contained in the `OraEBSSubForms.zip` file.

Creating an adapter service/target

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

Verifying that the adapter is working correctly

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

Creating an adapter service/target

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

Before you begin

Complete [“Importing the adapter profile”](#) on page 14.

About this task

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

To create or change a service, you must use the service form to provide information for the service. Service forms might vary depending on the adapter. The service name and description that you provide for

each service are displayed on the console. Therefore, it is important to provide values that make sense to your users and administrators.

Procedure

1. From the navigation tree, click **Manage Services**.
The **Select a Service** page is displayed.
2. On the **Select a Service** page, click **Create**.
The **Create a Service** wizard is displayed.
3. On the **Select the Type of Service** page, click **Search** to locate a business unit.
The **Business Unit** page is displayed.
4. On the **Business Unit** page, complete these steps:
 - a) Type information about the business unit in the **Search information** field.
 - b) Select a business type from the **Search by** list, and then click **Search**.
A list of business units that matches the search criteria is displayed.
If the table contains multiple pages, you can do the following tasks:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
 - c) In the **Business Units** table, select business unit in which you want to create the service, and then click **OK**.
The **Select the Type of Service** page is displayed, and the business unit that you specified is displayed in the **Business unit** field.
5. On the **Select the Type of Service** page, select a service type, and then click **Next**.
If the table contains multiple pages, you can do the following tasks:
 - Click the arrow to go to the next page.
 - Type the number of the page that you want to view and click **Go**.
6. On either the **Service Information** or **General Information** page, specify the appropriate values for the service instance.
The content of the **General Information** page depends on the type of service that you are creating. The creation of some services might require more steps.
7. To create a service with NTLM authentication, the administrator login is in the following format:

```
<Domain Name>\<Login Name>
```
8. For NLTM authentication, select **Authentication** mode as 'Claims-Based Authentication.
9. On the **Dispatcher Attributes** page, specify information about the dispatcher attributes, and then click **Next** or **OK**.
The **Dispatcher Attributes** page is displayed only for IBM Security Directory Integrator based services.
10. Optional: On the **Access Information** page, select the **Define an Access** check box to activate the access definition fields. Select the type of access you want to enable.
Specify the expected access information and any other optional information such as description, search terms, more information, or badges.
11. On the **Status and Information** page, view information about the adapter and managed resource, and then click **Next** or **Finish**.
The adapter must be running to obtain the information.
12. On the **Configure Policy** page, select a provisioning policy option, and then click **Next** or **Finish**.
The provisioning policy determines the ownership types available for accounts. The default provisioning policy enables only Individual ownership type accounts. Additional ownership types can be added by creating entitlements on the provisioning policy.

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

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

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

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

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

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

Results

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

Related concepts

Installing the dispatcher

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

Restarting the adapter service

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

Service/Target form details

Complete the service/target form fields.

Installing the adapter language package

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

Related tasks

Installing the adapter binaries or connector

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

Importing the adapter profile

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

Attribute mapping

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

Deploying the custom subforms

The Oracle eBS Adapter is supplied with custom subforms to specify the roles, responsibilities, and securing attributes associated with a user. The subforms are contained in the `OraEBSSubForms.zip` file.

Installing the Complex Attribute Handler

An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Verifying that the adapter is working correctly

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

Service/Target form details

Complete the service/target form fields.

The APPS account owns the Oracle eBS database and the adapter must run as the APPS user unless you have followed special configuration steps. If you use APPS, you do not require configuration changes on the managed resource.

If your security standards do not permit the use of APPS as an administrator account for the Oracle eBS Adapter, you must create a new user and grant required permissions as provided in the `nonAPPS.sql` file. The `nonAPPS.sql` file is supplied with the Oracle eBS Adapter compressed file. The adapter depends on wrapper stored procedures when an account other than APPS is used. Create the wrapper stored procedures specified in `nonAPPS.sql` file.

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**
- **Owner**
- **Service prerequisite**

On the Oracle EBS Profile tab:

Service name

Specify a name that defines the adapter service on the Identity server.

Note: Do not use forward (/) or backward slashes (\) in the service name.

Description

Optional: Specify a description that identifies the service for your environment.

Security Directory Integrator location

Specify the URL for the IBM Security Directory Integrator instance. The valid syntax for the URL is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the IBM Security Directory Integrator host and *port* is the port number for the RMI Dispatcher.

The default URL for the default SDI1 instance is `rmi://localhost:1099/ITDIDispatcher`.

Oracle EBS Service Name

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

Oracle EBS Service Host

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

Oracle EBS Service Port

Specify the port on which the Oracle eBS database service is listening.

Use SSL communication with Oracle?

Click the check box to force an SSL connection from the adapter to the Oracle eBS database.

Oracle EBS Server Distinguished Name

Optional. Specify the distinguished name that is contained in the certificate of the Oracle eBS database. If SSL communication is enabled and this field is not blank, the connection succeeds only if the distinguished names match.

Administrator Name

Specify the name of the user who has access to the Oracle eBS database and can perform administrative operations.

Password

Specify the password for the user.

Do not Reconcile Roles?

Select this check box if you do not want the list of roles to be retrieved during a reconciliation operation.

Do not Reconcile Persons?

Select this check box if you do not want the list of persons to be retrieved during a reconciliation operation.

Do not Reconcile Suppliers?

Select this check box if you do not want the list of suppliers to be retrieved during a reconciliation operation.

Do not Reconcile Customers?

Select this check box if you do not want the list of customers to be retrieved during a reconciliation operation.

Do not Reconcile Responsibilities?

Select this check box if you do not want the list of responsibilities to be retrieved during a reconciliation operation.

Do not Reconcile Securing Attributes?

Select this check box if you do not want the list of securing attributes to be retrieved during a reconciliation operation.

End Date the Responsibilities on Account Suspend

Select this check box if you want to end the responsibilities on account suspend.

Owner

Optional: Specify a user as a service owner.

Service Prerequisite

Optional: Specify a service that is prerequisite to this service.

On the Dispatcher Attributes tab:**Disable AL Caching**

Select the check box to disable the assembly line caching in the dispatcher for the service. The assembly lines for the add, modify, delete, and test operations are not cached.

AL FileSystem Path

Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines that are received from Identity server. For example, you can specify the following file path to load the assembly lines from the profiles directory of the Windows operating system: `c:\Files\IBM\TDI\V7.1\profiles` or you can specify the following file path to load the assembly lines from the profiles directory of the UNIX and Linux[®] operating systems: `system:/opt/IBM/TDI/V7.1/profiles`

Max Connection Count

Specify the maximum number of assembly lines that the dispatcher can run simultaneously for the service. For example, enter 10 when you want the dispatcher to run maximum 10 assembly lines simultaneously for the service. If you enter 0 in the **Max Connection Count** field, the dispatcher does not limit the number of assembly lines that are run simultaneously for the service.

On the Status and information tab

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

Last status update: Date

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

Last status update: Time

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

Managed resource status

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

Adapter version

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

Profile version

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

TDI version

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

Dispatcher version

Specifies the version of the Dispatcher.

Installation platform

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

Adapter account

Specifies the account that 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 conceptsInstalling the dispatcher

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

Restarting the adapter service

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

Installing the adapter language package

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

Related tasksInstalling the adapter binaries or connector

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

Importing the adapter profile

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

Attribute mapping

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

Deploying the custom subforms

The Oracle eBS Adapter is supplied with custom subforms to specify the roles, responsibilities, and securing attributes associated with a user. The subforms are contained in the `OraEBSSubForms.zip` file.

Installing the Complex Attribute Handler

An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Creating an adapter service/target

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

Verifying that the adapter is working correctly

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

Installing the adapter language package

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

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

Related concepts

Installing the dispatcher

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

Restarting the adapter service

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

Service/Target form details

Complete the service/target form fields.

Related tasks

Installing the adapter binaries or connector

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

Importing the adapter profile

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

Attribute mapping

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

Deploying the custom subforms

The Oracle eBS Adapter is supplied with custom subforms to specify the roles, responsibilities, and securing attributes associated with a user. The subforms are contained in the `OraEBSSubForms.zip` file.

Installing the Complex Attribute Handler

An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Creating an adapter service/target

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

Verifying that the adapter is working correctly

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

Verifying that the adapter is working correctly

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

Procedure

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

Related concepts

Installing the dispatcher

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

Restarting the adapter service

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

Service/Target form details

Complete the service/target form fields.

Installing the adapter language package

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

Enabling SSL communication

You must configure a truststore to enable SSL communication between the Oracle eBS Adapter and the Oracle eBS database. You can optionally configure a keystore for the dispatcher.

Password management when restoring accounts

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

Related tasks

Installing the adapter binaries or connector

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

Importing the adapter profile

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

Attribute mapping

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

Deploying the custom subforms

The Oracle eBS Adapter is supplied with custom subforms to specify the roles, responsibilities, and securing attributes associated with a user. The subforms are contained in the `OraEBSSubForms.zip` file.

Installing the Complex Attribute Handler

An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Creating an adapter service/target

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

Customizing the adapter profile

To customize the adapter profile, you must modify the Oracle eBS Adapter JAR file.

Editing adapter profiles on the UNIX or LINUX operating system

The adapter profile . jar file might contain ASCII files that are created by using the MS-DOS ASCII format.

Chapter 4. Upgrading

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

To verify the required version of these adapter components, see the adapter release notes. For the installation steps, see [Chapter 3, “Installing,” on page 11](#).

Upgrading the dispatcher

Before you upgrade the dispatcher, verify the version of the dispatcher.

- If the dispatcher version mentioned in the release notes is later than the existing version on your workstation, install the dispatcher.
- If the dispatcher version mentioned in the release notes is the same or earlier than the existing version, do not install the dispatcher.

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

Related concepts

[Upgrading the adapter profile](#)

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

Upgrading the adapter profile

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

Note: Restart the Dispatcher service after importing the profile. Restarting the Dispatcher clears the assembly lines cache and ensures that the dispatcher runs the assembly lines from the updated adapter profile.

Related concepts

[Upgrading the dispatcher](#)

Before you upgrade the dispatcher, verify the version of the dispatcher.

Chapter 5. Configuring

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

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

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

Enabling SSL communication

You must configure a truststore to enable SSL communication between the Oracle eBS Adapter and the Oracle eBS database. You can optionally configure a keystore for the dispatcher.

If the Oracle eBS database is configured to require SSL client authentication, you must configure a keystore.

To configure the truststore for the dispatcher, you must minimally import the Certification Authority (CA) certificate. This certificate is the one used to sign the certificate for the Oracle eBS database.

Note:

- All the files in the following tasks are in the solutions directory. For example: *TDI_HOME/timso1*.
- The store password *ThePwd12* in the code examples is a variable. Substitute your password for *ThePwd12*.

Related concepts

Password management when restoring accounts

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

Related tasks

Customizing the adapter profile

To customize the adapter profile, you must modify the Oracle eBS Adapter JAR file.

Editing adapter profiles on the UNIX or LINUX operating system

The adapter profile `.jar` file might contain ASCII files that are created by using the MS-DOS ASCII format.

Verifying that the adapter is working correctly

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

Configuring Oracle eBS database tier

Use the Oracle tools to configure both the truststore and the keystore on the Oracle eBS database tier.

About this task

The Oracle Wallet Manager and the **orapki** command, are used in the following steps. The following task sets up a self-signed certification authority, truststore, and keystore.

Procedure

1. Create a self-signed certificate authority.

Issue the following commands:

```
mkdir 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 CA.cer-pwd=ThePwd12
```

The CA .cer file is the trusted certificate that is used in the **keytool** command to import a CA certificate into the truststore for the dispatcher.

2. Create stores for Oracle eBS database tier authentication

Issue the following commands:

```
mkdir server

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

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

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

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

3. Configure the Oracle network.

You must configure the `listener.ora` and `sqlnet.ora` files on the Oracle eBS database tier to enable SSL. These files are typically edited with the Oracle Net Manager or with a text editor. These files are in the `ORACLE_HOME/network/admin/instance` directory of the database tier. This example does not require adapter authentication. If you want to require authentication for the Oracle eBS Adapter, set **SSL_CLIENT_AUTHENTICATION** to TRUE.

a) Edit the `listener.ora` file.

b) Locate the following lines and substitute the appropriate values for `SERVER_WALLET_LOCATION` and `HOSTNAME`.

```
SSL_CLIENT_AUTHENTICATION = FALSE
WALLET_LOCATION = (SOURCE = (METHOD = FILE) (METHOD_DATA =
(DIRECTORY = SERVER_WALLET_LOCATION)
))
LISTENER = (DESCRIPTION_LIST = (DESCRIPTION =
(ADDRESS = (PROTOCOL = TCPS) (HOST = HOSTNAME) (PORT = 2484))
))
```

Note: Port 2484 is typically used for SSL communication (TCPS protocol).

c) Edit the `sqlnet.ora` file.

d) Locate the following lines and substitute the appropriate values for highlighted values.

```
SSL_CLIENT_AUTHENTICATION = FALSE
WALLET_LOCATION = (SOURCE = (METHOD = FILE) (METHOD_DATA =
(DIRECTORY = SERVER_WALLET_LOCATION)
))
```


Configuring the Security Directory Integrator for Oracle eBS database tier authentication

You must import a CA certificate into the truststore.

Procedure

1. Import a CA certificate into the truststore.

Issue the command:

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

2. In the `solutions.properties` file, set the following properties:

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

Note: If the `javax.net.ssl.trustStore` property is already set to a truststore other than `truststore.jks`, import the CA certificate into that file instead.

3. Set the keystore properties.

If a keystore is not required and no keystore properties are set in the `solution.properties` file, use the truststore properties values for the keystore properties:

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

Configuring Security Directory Integrator for Oracle eBS Adapter authentication

If the Oracle eBS database is configured for SSL client authentication, you must configure a keystore.

Before you begin

You created a self-signed certificate authority in the Oracle eBS Adapter database tier.

Procedure

1. Create a JKS keystore.

Issue the following commands:

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

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

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

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

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

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

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

Changes to the adapter service form

To enable SSL communication between the Oracle eBS Adapter and the Oracle eBS database, you must supply information for the Oracle eBS adapter service form.

To access the service form, use the **Manage Services** utility on the IBM Security Verify Identity console. Supply following information for the fields on the service form.

Use SSL communication with Oracle?

Click this check box.

Oracle EBS Service Port

Change the value to the TCPS port. For example 2484.

Oracle EBS Server Distinguished Name

Optional. When a value is entered for this field, the entry is verified against the Oracle eBS database server certificate.

Note:

- Start the listener and database services with the same user who created the wallet, so that they are both able to access the wallet.
- The wallet location is provided in both the `sqlnet.ora` and the `listener.ora` files. Typically, both files contain the same wallet location. However, the `listener.ora` file can use its own wallet.
 - The distinguished name of the certificate pointed by the wallet in the `sqlnet.ora` file is the name to which the Oracle eBS Adapter must verify. This requirement applies only if a distinguished name is supplied on the service form.
 - Include a distinguished name in the service form as an extra measure of security. Doing so prevents another server from faking the identity.
- For information about how to configure SSL with the Oracle JDBC Thin driver, go to [the Oracle website](#). Search for the Oracle technical white paper *SSL with Oracle JDBC Thin Driver*.

JDBC driver location for SSL

You must download the JDBC Thin driver to support SSL.

Obtain the JDBC Thin driver from either:

- The `ORACLE_HOME/jdbc/lib` directory of the database tier
- The JDBC Driver Downloads page on the Oracle Technology Network (OTN) website.

Depending on your JRE, select the appropriate driver. The driver for JRE 1.5 is `ojdbc5.jar`. The driver for JRE 1.6 is `ojdbc6.jar`.

Copy the appropriate driver to the `TDI_HOME/jars/3rdparty/others` directory on the Security Directory Integrator server.

Remove previous versions of the JDBC Thin driver from the `TDI_HOME/jars/3rdparty/others` directory. For example:

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

Note: The .zip file in the list might alternatively be named as .jar files. For example `classes12.jar`.

Customizing the adapter profile

To customize the adapter profile, you must modify the Oracle eBS Adapter JAR file.

About this task

You might customize the adapter profile to change the account form or the service form. You can also change the labels on the forms with the Form Designer or `CustomLabels.properties`. Each adapter has a `CustomLabels.properties` file for that adapter.

The JAR file is included in the Oracle eBS Adapter compressed file that you downloaded from the IBM website. The JAR file and the files contained in the JAR file vary depending on your operating system.

Note: You cannot modify the schema for this adapter. Attributes cannot be added to or deleted from the schema.

The adapter JAR file includes the following files:

- Service.def
- Schema.dsml
- CustomLabels.properties
- erOracleEBSAccount.xml
- erOracleEBSRMIService.xml
- OracleEBSManagerUserAL.xml
- OracleEBSSearchUserAL.xml

To edit the JAR file, perform these steps:

Procedure

1. Log on to the workstation where the Oracle eBS Adapter is installed.
2. On the **Start** menu, click **Programs > Accessories > Command Prompt**.
3. Copy the JAR file into a temporary directory.
4. Extract the contents of the JAR file into the temporary directory by running the following command.

The following example applies to the Oracle eBS Adapter profile. Type the name of the JAR file for your operating system.

```
cd c:\temp
#jar -xvf OraEBSProfile.jar
```

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

5. Edit the file that you want to change.
6. After you edit the file, you must import the file into the Identity server for the changes to take effect. To import the file, perform these steps:
 - a) Create a JAR file with the files in the `\temp` directory by running the following commands:

```
cd c:\temp
#jar -cvf OraEBSProfile.jar OraEBSProfile
```

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

Related concepts

[Enabling SSL communication](#)

You must configure a truststore to enable SSL communication between the Oracle eBS Adapter and the Oracle eBS database. You can optionally configure a keystore for the dispatcher.

Password management when restoring accounts

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

Related tasks

Editing adapter profiles on the UNIX or LINUX operating system

The adapter profile .jar file might contain ASCII files that are created by using the MS-DOS ASCII format.

Verifying that the adapter is working correctly

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

Editing adapter profiles on the UNIX or LINUX operating system

The adapter profile .jar file might contain ASCII files that are created by using the MS-DOS ASCII format.

About this task

If you edit an MS-DOS ASCII file on the UNIX operating system, you might see a character ^M at the end of each line. These characters indicate new lines of text in MS-DOS. The characters can interfere with the running of the file on UNIX or Linux systems. You can use tools, such as **dos2unix**, to remove the ^M characters. You can also use text editors, such as the **vi** editor, to remove the characters manually.

Example

You can use the **vi** editor to remove the ^M characters. From the **vi** command mode, run the following command and press Enter:

```
:%s/^M//g
```

When you use this command, enter ^M or Ctrl-M by pressing **^v^M** or **Ctrl V Ctrl M** sequentially. The **^v** instructs the **vi** editor to use the next keystroke instead of issuing it as a command.

Related concepts

Enabling SSL communication

You must configure a truststore to enable SSL communication between the Oracle eBS Adapter and the Oracle eBS database. You can optionally configure a keystore for the dispatcher.

Password management when restoring accounts

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

Related tasks

Customizing the adapter profile

To customize the adapter profile, you must modify the Oracle eBS Adapter JAR file.

Verifying that the adapter is working correctly

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

Password management when restoring accounts

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

Certain resources reject a password when a request is made to restore an account. In this case, you can configure IBM Security Verify Identity to forego the new password requirement. You can set the Oracle eBS Adapter to require a new password when the account is restored, if your company has a business

process in place that dictates that the account restoration process must be accompanied by resetting the password.

In the `service.def` file, you can define whether a password is required as a new protocol option. When you import the adapter profile, if an option is not specified, the adapter profile importer determines the correct restoration password behavior from the `schema.dsml` file. Adapter profile components also enable remote services to find out if you discard a password that is entered by the user in a situation where multiple accounts on disparate resources are being restored. In this situation, only some of the accounts being restored might require a password. Remote services will 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">true</value>  
</property>  
<Property Name = "com.ibm.itim.remoteservices.ResourceProperties.  
PASSWORD_NOT_ALLOWED_ON_RESTORE">false</value>  
</property>
```

By adding the two options in the example above, you are ensuring that you will not be prompted for a password when an account is restored.

Related concepts

Enabling SSL communication

You must configure a truststore to enable SSL communication between the Oracle eBS Adapter and the Oracle eBS database. You can optionally configure a keystore for the dispatcher.

Related tasks

Customizing the adapter profile

To customize the adapter profile, you must modify the Oracle eBS Adapter JAR file.

Editing adapter profiles on the UNIX or LINUX operating system

The adapter profile `.jar` file might contain ASCII files that are created by using the MS-DOS ASCII format.

Verifying that the adapter is working correctly

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

Verifying that the adapter is working correctly

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

Procedure

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

Related concepts

Installing the dispatcher

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

Restarting the adapter service

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

Service/Target form details

Complete the service/target form fields.

Installing the adapter language package

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

Enabling SSL communication

You must configure a truststore to enable SSL communication between the Oracle eBS Adapter and the Oracle eBS database. You can optionally configure a keystore for the dispatcher.

Password management when restoring accounts

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

Related tasks

Installing the adapter binaries or connector

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

Importing the adapter profile

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

Attribute mapping

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

Deploying the custom subforms

The Oracle eBS Adapter is supplied with custom subforms to specify the roles, responsibilities, and securing attributes associated with a user. The subforms are contained in the `OraEBSSubForms.zip` file.

Installing the Complex Attribute Handler

An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Creating an adapter service/target

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

Customizing the adapter profile

To customize the adapter profile, you must modify the Oracle eBS Adapter JAR file.

Editing adapter profiles on the UNIX or LINUX operating system

The adapter profile `.jar` file might contain ASCII files that are created by using the MS-DOS ASCII format.

Chapter 6. Troubleshooting

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. This topic provides information and techniques for identifying and resolving problems that are related to the adapter, including troubleshooting errors that might occur during the adapter installation.

Techniques for troubleshooting problems

Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely.

Problem descriptions help you and the IBM technical-support representative find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution.

What are the symptoms of the problem?

When you start to describe a problem, the most obvious question is "What is the problem?" This question might seem straightforward; however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

- Is the problem specific to one operating system, or is it common across multiple operating systems?
- Is the current environment and configuration supported?
- Do all users have the problem?
- (For multi-site installations.) Do all sites have the problem?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration. Many problems can be traced back to incompatible levels of software that are not intended to run together or are not fully tested together.

When does the problem occur?

Develop a detailed timeline of events that lead up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you use the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:

- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

Under which conditions does the problem occur?

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:

- Does the problem always occur when the same task is being done?
- Is a certain sequence of events required for the problem to occur?
- Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might occur around the same time, the problems are not necessarily related.

Can the problem be reproduced?

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Problems that you can reproduce are often easier to debug and solve.

However, problems that you can reproduce can have a disadvantage: If the problem is of significant business impact, you do not want it to recur. If possible, re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Do multiple users or applications have the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

Related concepts

Error messages and problem solving

A warning or error message might be displayed in the user interface to provide information about the adapter or when an error occurs.

Error messages and problem solving

A warning or error message might be displayed in the user interface to provide information about the adapter or when an error occurs.

Table 3 on page 41 contains warnings or errors that might be displayed on the user interface if the adapter is installed on your workstation.

Table 3. Warning and error messages

Message ID	Warning or error message	Corrective action
CTGIMT001E	The following error occurred. Error: Either the Oracle eBS service name is incorrect or the service is not up.	Ensure that the Oracle database service name given on IBM Security Verify Identity service form is running.
CTGIMT001E	The following error occurred. Error: Either the Oracle eBS host or port is incorrect.	Verify that the host workstation name or the port for the Oracle eBS database service is correctly specified.
CTGIMT002E	The login credential is missing or incorrect.	Verify that you have 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 and that the path is included in the system CLASSPATH variable.
CTGIMT600E	An error occurred while establishing communication with the Security Directory Integrator server.	IBM Security Verify Identity cannot establish a connection with Security Directory Integrator. To fix this problem, ensure that: <ul style="list-style-type: none"> • The Security Directory Integrator is running. • The URL specified on the service form for the Security Directory Integrator is correct.

Related concepts

Techniques for troubleshooting problems

Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely.

Chapter 7. Uninstalling

To remove an adapter from the Identity server for any reason, you must remove all the components that were added during installation. Uninstalling an IBM Security Directory Integrator based adapter mainly involves removing the connector file, and the adapter profile from the Identity server. Depending on the adapter, some of these tasks might not be applicable, or there can be other tasks.

Uninstalling the dispatcher

You might need to remove the Oracle eBS Adapter.

About this task

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

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

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

Complete these steps:

Procedure

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

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

Related concepts

Deleting the adapter profile

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

Deleting the adapter profile

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

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

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

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

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

Related tasks

Uninstalling the dispatcher

You might need to remove the Oracle eBS Adapter.

Chapter 8. Reference

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

Adapter attributes and object classes

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

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

Table 4 on page 45 is a listing of the attributes that are used by the Oracle eBS Adapter. The table gives a brief description, constraints, and permissions. The permissions are:

Read

The attribute is reconciled but not modified by the adapter.

Write

The attribute is modified by the adapter but not reconciled.

Read and Write

The attribute is reconciled and can be modified by the adapter.

Attribute	Description	Constraints	Permissions
erAccountStatus	Specifies the status of the account as enabled or disabled.		Read and Write
erLastAccessDate	The users last login date and time in Oracle eBS.		Read
erOraEBSCust	Customer.		Read and Write
erOraEBSDescription	A short description for the user name.	The description is limited to a maximum of 240 characters.	Read and Write
erOraEBSLeftPwdAccess	Specifies the number of login accesses remaining (from the current day) until the password expires.	The maximum value is 9999999999999999.	Read and Write
erOraEBSPerson	Person.		Read and Write
erOraEBSPwdAccesses	Specifies the number of login accesses allowed before the password expires.	The maximum value is 9999999999999999.	Read and Write

Table 4. Attributes, descriptions, constraints, and permissions (continued)

Attribute	Description	Constraints	Permissions
erOraEBSPwdLifeSpanDays	Specifies the number of days after which the password expires	The maximum value is 9999999999999999.	Read and Write
erOraEBSResp	Specifies a directly granted responsibility formatted as Application_Name Responsibility_Name Start_Date End_Date The denotes a space character. Dates are formatted as “dd/mm/yyyy” (for example 31/12/2001) or empty to omit. For example Sales Foundation Customer Relationship Mgmt 13/01/2001.		Read and Write
erOraEBSSessionNumber	Specifies the session ID		Read
erOraEBSSupp	Specifies a supplier.		Read and Write
erOraEBSUserEndDate	Specifies the user's effective end date.		Read and Write
erOraEBSUserFax	Specifies the user's fax number	The fax number is limited to a maximum of 80 characters.	Read and Write
erOraEBSUserMail	Specifies the user's email address.	The email address is limited to a maximum of 240 characters.	Read and Write
erOraEBSUserStartDate	Specifies the user's effective start date.		Read and Write
erPassword	Specifies the password for the user name.	The password is limited to a maximum of 45 characters.	Write
erUid	Specifies the user name.	The user name is limited to a maximum of 100 characters.	Read and Write
erOraEBSAttr	Specifies an associated securing attribute formatted as Application_ID Attribute_Code Value. Do not use blank spaces. For example, 454 ONE_DAY_BOOK_TO_SHIP_PERCENT 2342. If the Value is DATE, the format is dd-mm-yyyy (For example. 31-12-2001). If the Value is DATETIME, the format is dd-mm-yyyy hh24:mi:ss. (For example 31-12-2001 13:45:00).		Read and Write

Attribute	Description	Constraints	Permissions
erOraEBSIndirectResp	Specifies an inherited responsibility formatted like erOraEBSResp .		Read
erOraEBSDirectRoles	Specifies a directly granted role formatted as a JSON object with the fields role (object) startDate (string) endDate (string) reason (string) The 'role' object is a JSON object with fields name (string), origSystem (string), and origSystemId (string). The date fields (startDate and endDate) are represented as strings with the format <code>yyyymmddhh24mi'Z'</code> . (For example <code>200112311345Z</code>). For example, <code>{"endDate":null,"reason":"Granted by XX","role":{"name":"UMX SECURITY_ADMIN","origSystem":"UMX","origSystemId":"0"},"startDate":"201103150000Z"}</code> .		Read and Write
erOraEBSIndirectRole	Specifies an inherited role formatted like erOraEBSDirectRoles .		Read

Adapter attributes by operations

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

The lists include more information about required and optional attributes sent to the Oracle eBS Adapter to complete that action.

System Login Add

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

Required attribute	Optional attribute
erUid erPassword	All other supported attributes

Related concepts

[System Login Change](#)

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

[System Login Delete](#)

This operation is not supported.

[System Login Suspend](#)

You might need to suspend a system login.

[System Login Restore](#)

You might need to restore a system login.

[Test](#)

The following table identifies attributes needed to test the connection.

[Reconciliation](#)

You might need to reconcile user account information.

System Login Change

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

<i>Table 6. Change request attributes for Oracle</i>	
Required attribute	Optional attribute
erUid	All other supported attributes

Related concepts

[System Login Add](#)

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

[System Login Delete](#)

This operation is not supported.

[System Login Suspend](#)

You might need to suspend a system login.

[System Login Restore](#)

You might need to restore a system login.

[Test](#)

The following table identifies attributes needed to test the connection.

[Reconciliation](#)

You might need to reconcile user account information.

System Login Delete

This operation is not supported.

Related concepts

[System Login Add](#)

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

[System Login Change](#)

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

[System Login Suspend](#)

You might need to suspend a system login.

[System Login Restore](#)

You might need to restore a system login.

[Test](#)

The following table identifies attributes needed to test the connection.

[Reconciliation](#)

You might need to reconcile user account information.

System Login Suspend

You might need to suspend a system login.

A System Login Suspend is a request to disable a user account. The user is neither removed nor are their attributes modified.

<i>Table 7. Suspend request attributes for Oracle</i>	
Required attribute	Optional attribute
erUid erAccountStatus	None

Related concepts

System Login Add

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

System Login Change

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

System Login Delete

This operation is not supported.

System Login Restore

You might need to restore a system login.

Test

The following table identifies attributes needed to test the connection.

Reconciliation

You might need to reconcile user account information.

System Login Restore

You might need to restore a system login.

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 using the same attributes as the ones before the Suspend function was called.

<i>Table 8. Restore request attributes for Oracle</i>	
Required attribute	Optional attribute
erUid erAccountStatus	None

Related concepts

System Login Add

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

System Login Change

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

System Login Delete

This operation is not supported.

System Login Suspend

You might need to suspend a system login.

Test

The following table identifies attributes needed to test the connection.

Reconciliation

You might need to reconcile user account information.

Test

The following table identifies attributes needed to test the connection.

<i>Table 9. Test attributes</i>	
Required attribute	Optional attribute
None	None

Related concepts

System Login Add

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

System Login Change

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

System Login Delete

This operation is not supported.

System Login Suspend

You might need to suspend a system login.

System Login Restore

You might need to restore a system login.

Reconciliation

You might need to reconcile user account information.

Reconciliation

You might need to reconcile user account information.

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

<i>Table 10. Reconciliation request attributes for Oracle</i>	
Required attribute	Optional attribute
None	None

Related concepts

System Login Add

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

System Login Change

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

System Login Delete

This operation is not supported.

System Login Suspend

You might need to suspend a system login.

System Login Restore

You might need to restore a system login.

Test

The following table identifies attributes needed to test the connection.

Index

A

adapter

- attributes
 - by adapter action [47](#)
 - descriptions [45](#)
 - permissions [45](#)
- customization
 - steps [35](#)
- features [1](#)
- installation
 - steps [12](#)
 - troubleshooting errors [39](#)
 - verifying [26](#), [37](#)
 - warnings [39](#)
 - worksheet [8](#)
- overview [1](#)
- profile
 - overview [1](#)
 - upgrading [29](#)
- SSL communication to the database [31](#)
- supported configurations [2](#)
- uninstall [43](#)
- upgrading [29](#)

adapters

- removing profiles [43](#)

architecture [1](#)

attributes

- adapter action, by
 - reconciliation [50](#)
 - restoring [49](#)
 - suspending [49](#)
- by Oracle eBS Adapter action
 - add [47](#)
 - change [48](#)
- by Oracle eBS Adapter action action
 - delete [48](#)
- descriptions [45](#)
- for the adapter [45](#)

authentication for the adapter [33](#)

C

changes to the service form for SSL [34](#)

configuring

- adapter authentication [33](#)

connection [50](#)

creating

- keystore [31](#)
- self-signed certificate authority [31](#)
- truststore [31](#)

custom subforms, deploying [17](#)

D

database

- SSL communication to the adapter [31](#)

database (*continued*)

- truststore configuration [31](#)

deploying custom subforms [17](#)

directory integrator

- connector [1](#)
- uninstalling the adapter [43](#)

dispatcher

- installation [11](#)
- upgrading [29](#)

download, software [8](#)

E

error messages [40](#)

I

installation

- first steps [31](#)
- language pack [25](#)
- planning roadmaps [5](#)
- uninstall [43](#)
- verification
 - adapter [26](#), [37](#)
 - worksheet [8](#)

J

JDBC Thin driver

- for SSL [34](#)

K

keystore for tier configuration [31](#)

L

language pack

- installation [25](#)
- same for adapters and server [25](#)

M

messages

- error [40](#)
- warning [40](#)

MS-DOS ASCII characters [36](#)

O

obtaining the JDBC Thin driver [34](#)

overview [1](#)

P

profile
 editing on UNIX or Linux [36](#)

R

reconciliation [50](#)
removing
 adapter profiles [43](#)
request attributes [50](#)
restore request [49](#)
restoring accounts
 files, changing [36](#)
 password requirements [36](#)
RMI dispatcher [1](#)
roadmaps
 planning [5](#)

S

self-signed certificate authority for tier configuration [31](#)
service
 form changes for SSL [34](#)
 restart [13](#)
 start [13](#)
 stop [13](#)
software
 download [8](#)
 website [8](#)
SSL
 adapter authentication [33](#)
 communication between adapter and database [31](#)
 information, service form [34](#)
 JDBC Thin driver [34](#)
subforms, custom [17](#)
supported
 attributes [45](#)
 configurations
 adapter [2](#)
 overview [2](#)
suspend request attribute [49](#)
system login
 restore [49](#)
 suspend [49](#)

T

test attributes [50](#)
tier
 configuration [31](#)
troubleshooting
 error messages [40](#)
 identifying problems [39](#)
 techniques for [39](#)
 warning messages [40](#)
troubleshooting and support
 troubleshooting techniques [39](#)
truststore for tier configuration [31](#)

U

uninstalling

uninstalling (*continued*)
 adapter [43](#)
 from the directory integrator [43](#)
updating
 adapter profile [35](#)
 form labels [35](#)
upgrade
 adapter [29](#)
 dispatcher [29](#)
upgrades
 adapter profiles [29](#)

V

verification
 dispatcher installation [11](#)
 installation [26, 37](#)
vi command [36](#)

W

warning messages [40](#)

