IBM Security Verify Governance Identity Manager
10.0

UNIX and Linux Adapter Installation and Configuration Guide

IBM

Contents

Figures

Tables

Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server.

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.

The UNIX and Linux Adapter enables communication between the Identity server and any of the following operating systems:

- AIX®
- HPUX
- Linux®
- Solaris

Features

The adapter automates several administrative and management tasks.

The adapter automates the following user management tasks:

- Adding user accounts
- Modifying user account attributes
- Modifying user account passwords
- Suspending, restoring, and deleting user accounts
- Managing groups
- Reconciling user accounts and groups

Related concepts

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

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

Architecture

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

You install the following components:

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

You must install the Dispatcher and the adapter profile; however, the Security Directory Integrator connector might already be installed with the base Security Directory Integrator product.

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

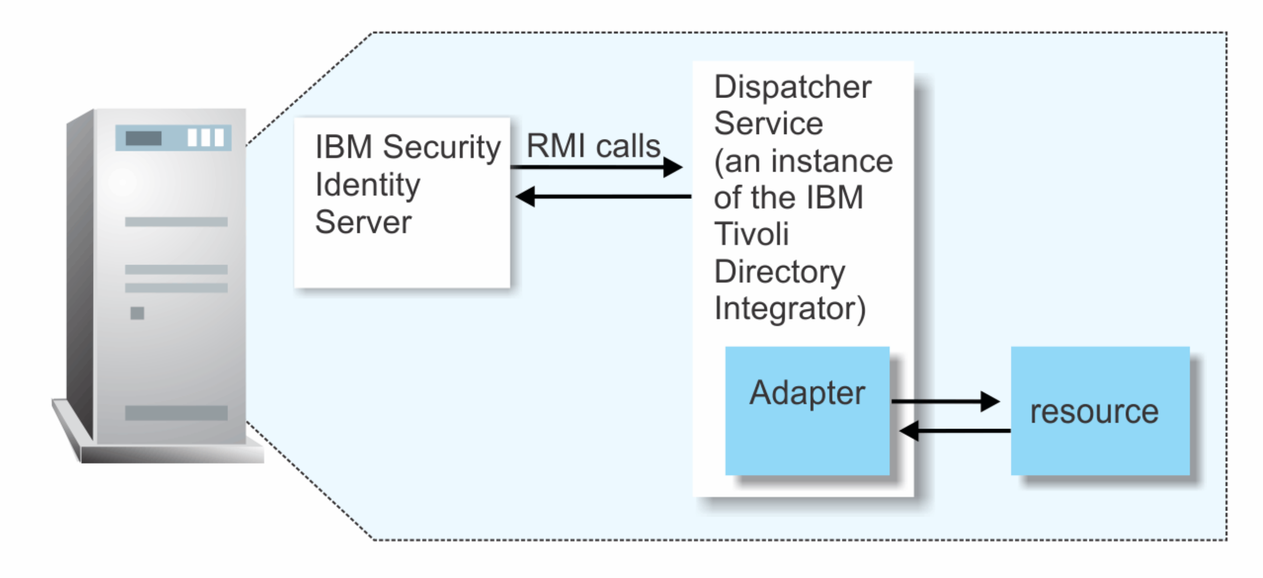
IBM Security Identity Server
RMI calls
Dispatcher Service (an instance of the IBM Tivoli Directory Integrator)
Adapter
resource

Figure 1. The architecture of the UNIX and Linux Adapter

Related concepts

Features
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.

There are fundamental components in each environment.

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

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

Single server configuration

Install the Identity server, the Security Directory Integrator server, and the UNIX and Linux Adapter on one server to establish communication with the UNIX or Linux operating system. Install the UNIX or Linux operating system on a different server as described Figure 2 on page 3.

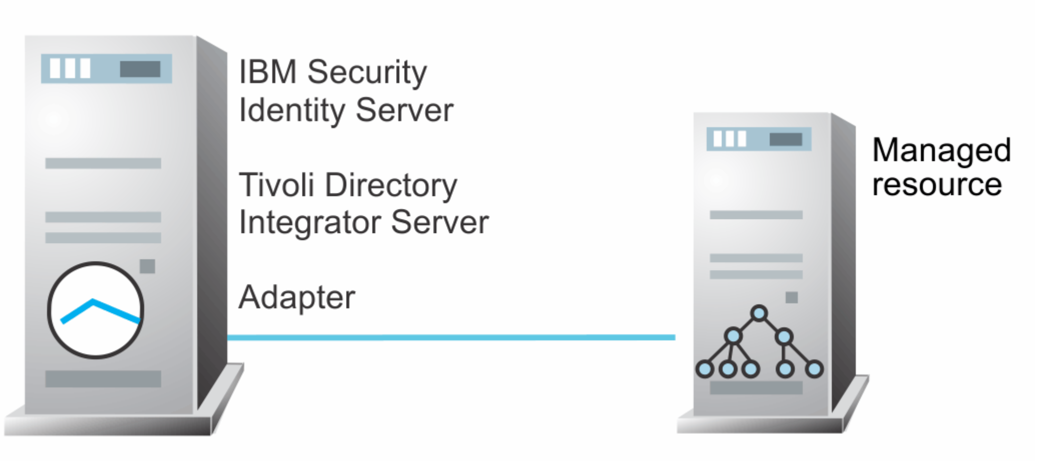

Figure 2. Example of a single server configuration

Multiple server configuration

Install the Identity server, the Security Directory Integrator server, the UNIX and Linux Adapter, and the UNIX or Linux operating system on different servers. Install the Security Directory Integrator server and the UNIX and Linux Adapter on the same server as described Figure 3 on page 3.

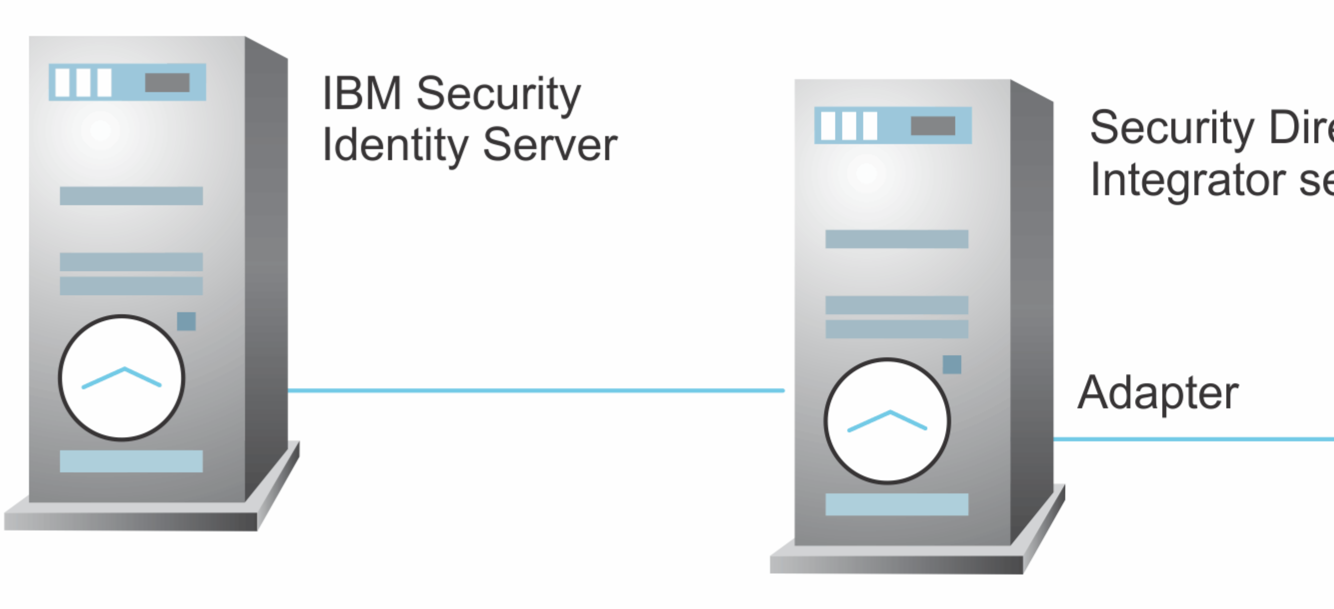

Figure 3. Example of multiple server configuration

Related concepts

Features

The adapter automates several administrative and management tasks.

Architecture

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

Chapter 2. Planning

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

Use the Preinstallation roadmap to prepare the environment.

Table 1. Preinstallation roadmap

Task	For more information, see
Verify that your environment meets the software and hardware requirements for the adapter.	"Prerequisites" on page 9.
Obtain the installation software.	Software download.
Obtain the necessary information for the installation and configuration.	"Installation worksheet" on page 12.

Use the Installation and configuration roadmap to complete the actual installation and configuration of the adapter.

Table 2. Installation and configuration roadmap

Task	For more information, see
Install the dispatcher.	Installing the dispatcher.
Install the adapter.	"Installing the adapter using the installation wizard" on page 15
Verify the adapter installation.	"Verifying the adapter installation" on page 16
Import the adapter profile into the Identity server.	Importing the adapter profile.
Enable secure communication.	"Enabling secure communication" on page 25.
Create an adapter service.	Creating an adapter service.
Configure the adapter.	Adapter configuration.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager 10.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

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

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

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

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.

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

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

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

Pre-installation

Complete these tasks.

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

Installation

Complete these tasks.

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

Upgrade

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

Configuration

Complete these tasks.

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

Troubleshooting

See the following topics.

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

Uninstallation

Complete these tasks.

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

Reference

See the following topics.

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

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager 10.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.

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.

This adapter is installed into IBM Security Directory Integrator. The adapter can be installed on any operating system that is supported by Security Directory Integrator and supported by the target system libraries or client.

Install Security Directory Integrator on each node of the WebSphere® Application Server cluster. Then, install this adapter on each instance of Security Directory Integrator.

Table 3 on page 9 identifies the software and operating system prerequisites for the adapter installation.

See the Release Notes bundled with this adapter package for the most current information about supported versions and minimum fix pack levels.

Table 3. Prerequisites to install the adapter

Prerequisite	**Description**
Directory Integrator	• IBM Security Directory Integrator 7.2 + FP6 + 7.2.0-ISS-SDI-LA0019 **Note:** • Earlier versions of IBM Security Directory Integrator that are still supported might function properly. However, to resolve any communication errors, you must upgrade your Directory Integrator release to the versions that the adapter officially supports. • The adapter supports IBM Security Directory Integrator 7.2, which is available only to customers who have the correct entitlement. Contact your IBM representative to find out whether you have the entitlement to download IBM Security Directory Integrator 7.2.
Identity server	The following servers are supported: • IBM Security Verify Governance Identity Manager v10.0 • IBM Security Verify Governance v10.0 • IBM Security Identity Manager v7.0.x • IBM Security Identity Manager v6.0.x • IBM Security Privileged Identity Manager v2.x • IBM Security Identity Governance and Intelligence v5.2.x

Table 3. Prerequisites to install the adapter (continued)

Prerequisite	Description
Operating systems	Use the UNIX and Linux Adapter for user provisioning on the following operating systems. **AIX** AIX 7.1 AIX 7.2 **HP-UX** HP-UX 11i v3 Supported operating system modes: non-trusted, trusted, and non-secure **Solaris** Solaris 11 **Oracle Linux** Linux 6.3 Linux 6.6 Linux 7 Linux 7.1 Linux 7.2 Linux 7.3 **Red Hat Linux** At the time of the adapter 10.0.1 release, the most recent Red Hat Linux Enterprise Server releases and upgrades were: Red Hat Linux Enterprise Server 8.0 Red Hat Linux Enterprise Server 8.2 Red Hat Linux Enterprise Server 8.4 Red Hat Enterprise Server supported operating system modes are standard and SE Linux Red Hat Linux Enterprise Server release updates might introduce changes and/or features that are not supported by the adapter. In such a case, support for the changes or features will be added in a future release of the adapter. **SuSE Enterprise Linux Server** SUSE SLES 12.4 SUSE SLES 12.5 SUSE SLES 15 SP3 **z System and LinuxONE** Red Hat Linux Enterprise Server 8.3 Ubuntu 20.04 SUSE SLES 15

Table 3. Prerequisites to install the adapter (continued)

Prerequisite	**Description**
System Administrator Authority	To complete the adapter installation procedure, you must have system administrator authority.
Security Directory Integrator adapters solution directory	A Security Directory Integrator adapters solution directory is a Security Directory Integrator work directory for adapters. See the *Dispatcher Installation and Configuration Guide*.
The `/etc/passwd` and `/etc/shadow/passwd` files in a standard format on the managed resource	The `/etc/passwd` and `/etc/shadow/passwd` files must be in a standard format on the managed resource. Any non-standard deviation in these files, such as more fields or characters, might cause adapter operations to fail.
The Secure Shell (SSH) protocol	The Secure Shell (SSH) protocol must be installed and running on the managed resource. **Note:** The adapter supports OpenSSH and Tectia SSH package.

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

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager 10.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

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

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

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

Software downloads

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

Go to IBM Passport Advantage.

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

Note:

You can also obtain additional adapter information from IBM Support.

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager 10.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

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

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

Installation worksheet

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

Installation worksheet

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

Table 4. Required information to install the adapter

Required information	**Description**	**Value**

Security Directory Integrator Home Directory	The *ITDI_HOME* directory contains the `jars/connectors` subdirectory. This subdirectory contains adapter JAR files.	IBM Security Directory Integrator can be automatically installed with your IBM Security Verify Governance Identity ManagerIBM Security Verify GovernanceIBM Security Privileged Identity Manager product. In this case, one of the following is the default directory path that is used for Security Directory Integrator.
		Windows:
		`drive:\Program Files\IBM\TDI\TDI_VERSION`
		UNIX:
		`/opt/IBM/TDI/TDI_VERSION`

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

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager 10.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

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

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

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

Chapter 3. Installing in the Verify Governance virtual appliance

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

About this task

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

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

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

Procedure

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

   The adapter package includes the following files:

Table 5. Adapter package contents

Files	Descriptions
`bundledefinition.json`	The adapter definition file. It specifies the content of the package, and the adapter installation and configuration properties that are required to install and update the adapter.
Adapter JAR profile	An Security Directory Integrator adapter always include a JAR profile which contains: • `targetProfile.json` – Service provider configuration – Resource type configuration – SCIM schema extensions – List of assembly lines • A set of assembly lines in XML files • A set of forms in XML files • Custom properties that include labels and messages for supported languages. Use the **Target Administration** module to import the target profile.

Table 5. Adapter package contents (continued)

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

2. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **SDI Management**.
3. Select the instance of the Security Directory Integrator for which you want to manage the adapters and click **Manage** > **SDI Adapters**

   The **SDI Adapters** window is displayed with a table that list the name, version, and any comments about the installed adapters.
4. On the **SDI Adapters** window, click **Install**.
5. On the **File Upload** window, click **Browse** to locate the adapter package and then click **OK**.
   For example, `Adapter-`*`<Adaptername>`*`.zip`.
6. Provide the missing 3rd party libraries when prompted.
   a) On the **File Upload** for Pre-requisite files window, click **Select Files**.

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

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

   c) Click **Open**.

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

   d) Click **OK**.

      The missing files are uploaded and the adapter package is updated with the 3rd party libraries.
7. Enable secure communication.
   a) Select the instance of the Security Directory Integrator for which you want to manage the adapter.

   b) Click **Edit**.

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

   d) Click **Save Configuration**.
8. Import the SSL certificate to the IBM Security Directory Integrator server.
   a) Select the instance of the Security Directory Integrator for which you want to manage the adapter.

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

   c) Click the **Signer** tab.

   d) Click **Import**.

      The **Import Certificate** window is displayed.

   e) Browse for the certificate file.

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

   g) Click **Save**.

Chapter 4. Installing

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

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

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

Installing the dispatcher

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

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

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

Installing the adapter using the installation wizard

Use these steps to install the UNIX and Linux Adapter software.

About this task

Use the `PosixAdapterInstall_70.jar` file to install the adapter.

Procedure

1. Create a temporary directory on the workstation where you want to install the adapter.
2. Extract the contents of the compressed file in the temporary directory.
3. Run the adapter installation wizard.

   Use the Java™ executable file that comes with Security Directory Integrator to start the installation program. The Java executable file is in the *ITDI_HOME*`/jvm/jre/bin` directory. Run the following command to start the installation program:

   ```
   ITDI_HOME/jvm/jre/bin/java -jar PosixAdapterInstall_70.jar
   ```
4. On the **Welcome** page, click **Next**.
5. In the **Directory Name** field, specify the location of the Tivoli® Directory Integrator home directory.
6. Review the installation settings on the **Install Summary** page and do one of the following steps:
   - Click **Back** to return to a previous page to modify any of the settings.
   - Click **Next** when you are ready to begin the installation.
7. Click **Finish** when the software displays the **Install Completed** window.

Installing the adapter binaries or connector

The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.This topic is not applicable for this adapter.

About this task

Procedure

Installing 3rd party client libraries

Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

About this task

Procedure

Setting up the adapter environment

In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

About this task

Procedure

Verifying the adapter installation

Adapter components are created on the Security Directory Integrator server after you install the adapter.

Table 6. Adapter components

Directory	**Adapter component**
ITDI_HOME/jars/connectors*ITDI_HOME*\jars\connectors	PosixConnector.jar
adapter_solution_directory	• AIXPConnRes.sh • SolarisPConnRes.sh • HPTrustPConnRes.sh • LinuxPConnRes.sh • LinuxShadowPConnRes.sh • HPNTrustPConnRes.sh • CryptPwd

Review the installer log files, `POSIXAdapter_Installer.log,`and `POSIXAdapter_Installer_opt.log` that are in the adapter installer directory for any errors.

If this installation is to upgrade a connector, then send a request from IBM Security Verify Governance Identity ManagerIBM Security Verify GovernanceIBM Security Privileged Identity Manager. Verify that the version number in the `ibmdi.log` matches the version of the connector that you installed. The `ibmdi.log` file is at *`ITDI_HOME`*`\`*`adapter solution directory`*`\logs`*`ITDI_HOME`*`/`*`adapter solution directory`*`/logs`.

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*.

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 Verify Governance 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.

The adapter profile is already imported into the IBM Security Verify Governance Identity Manager virtual appliance. Read the adapter release notes for any specific instructions before you import a new adapter profile on IBM Security Verify Governance Identity Manager.

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. .

Importing the adapter profile

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

Before you begin

- The Identity server is installed and running.
- You have administrator authority on the Identity server.
- The file to be imported must be a Java archive (JAR) file. The `<Adapter>Profile.jar` file includes all the files that are required to define the adapter schema, account form, service/target form, and profile properties. If necessary, you can extract the files from the JAR file, modify the files, and repackage the JAR file with the updated files.

About this task

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

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

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

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

Procedure

1. Log in to the Verify Governance Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.

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

Results

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

What to do next

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

- Import the attribute mapping file. See "Importing attribute mapping file" on page 19.
- Create a connector that uses the target profile. See "Adding a connector" on page 20.

Importing attribute mapping file

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

About this task

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

Procedure

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

Adding a connector

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

Before you begin

Complete Importing the adapter profile.

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

About this task

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

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

Procedure

To add a connector, complete these steps.

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

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

   The **Connector Details** pane is enabled for your input.
7. On the **Connector Details** tab, complete these steps:

   a) Assign a name and description for the connector.

   b) Select the target profile type as `Identity Brokerage` and its corresponding target profile.

   c) Select the entity, such as **Account** or **User**.

   Depending on the connector type, this field might be preselected.

   d) Optional: Select **Trace ON** and the corresponding **Trace Level** to enable trace logs.

   The available trace levels are DEBUG, INFO, and ERROR.

   e) Optional: Select **History ON** to save and track the connector usage.

   f) Click **Save**.

   The fields for enabling the channels for sending and receiving data are now visible.

   g) Select and set the connector properties in the **Global Config** accordion pane.

   For information about the global configuration properties, see Global Config accordion pane.

   h) Click **Save**. The fields for enabling the channels for sending and receiving data are now visible.

Results

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

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

What to do next

Enable the channel modes to synchronize the data between the target systems and Verify Governance. For more information, see "Enabling connectors" on page 21.

Enabling connectors

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

Before you begin

Table 7. Prerequisites for enabling a connector

Prerequisite	Find more information
A connector must exist in Verify Governance.	"Adding a connector" on page 20.
Ensure that you enabled the appropriate channel modes for the connector.	"Reviewing and setting channel modes for each new connector" on page 22.

Procedure

To enable a connector, complete these steps:

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

   A list of connectors is displayed on the **Connectors** tab.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Optional: To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Select the connector that you want to enable.
7. On the **Connector Details** tab, complete these steps:

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

   Enable write-to channel

   Propagates every change in the Access Governance Core repository into the target system.

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

   Enable read-from channel

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

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

   Enable reconciliation

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

Results

The connector is enabled

What to do next

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

Reviewing and setting channel modes for each new connector

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

About this task

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

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

Procedure

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

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

   A list of connectors is displayed on the **Connectors** tab.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Optional: To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Select the connector that you want to enable.
7. On the **Connector Details** tab, complete these steps:

   a) Select the channel modes that you want to enable, and then click **Save**. Depending on the channels that you enable, the corresponding **Channel** tabs are displayed, in which you can do more configuration, such as mapping attributes and setting up rules.

      Enable write-to channel

      Propagates every change in the Access Governance Core repository into the target system.

      Enable read-from channel

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

      Enable reconciliation

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

   A list of connectors is displayed.
9. On the **Change Log Sync Status** tab, complete these steps:

   a) Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.

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

      The synchronization process begins.

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

      Information about the synchronization is displayed in the **Sync History** tab.
10. Set the change log synchronization schedule for each new connector that you migrated.
11. When the connector configuration is complete, enable the connector by completing these steps:

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

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

   c) Click **Save**.

   For more information, see "Enabling connectors" on page 21.

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

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

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

Attribute Mapping

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

About this task

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

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

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

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

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

Note:

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

Procedure

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

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

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

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

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

6. Map the following attributes for **Chanel-Write To** and **Chanel-Read From**

Attribute	Mapped Attribute
eruid	CODE
erpassword	PASSWORD

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

Attribute mapping

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

About this task

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

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

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

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

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

Note:

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

Procedure

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

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

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

   ```

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

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

Enabling secure communication

The adapter uses the Secure Shell (SSH) protocol to communicate with the managed resource. This protocol must be installed and running before the adapter connects to the managed resource.

About this task

The adapter supports SSH protocol version 2.0. The SSH configuration file lists the SSH protocol version that is supported by your system.

Note: OpenSSH is the only supported SSH package on HP-UX and Solaris. OpenSSH and Tectia SSH packages are supported on AIX and Linux systems.

The following list provides information to help you ensure that the UNIX based managed resources in your network can operate with the UNIX and Linux Adapter.

HP-UX, Linux, and Solaris systems
SSH is installed and enabled by default on these operating systems. However, check to ensure that the SSH daemon is running before you attempt to connect a managed resource to the Identity server. If SSH is not enabled, the connection fails.

AIX systems
SSH is not installed on AIX operating systems. If a supported version of SSH is not installed on your system, you might download and install SSH from an open source website. You must install OpenSSL if you are going to use OpenSSH because OpenSSH uses functions that are provided by OpenSSL. Install the OpenSSL first and then install OpenSSH. The AIX operating system requires the OpenSSH product version 4.7 or later. After SSH is installed, check to ensure that the SSH daemon is running. Then, connect the managed resource to the Identity server. If SSH is not enabled, the connection fails.

Note: On an IPv6 environment, you might be required to configure SSH to listen on an IPv6 address. See the SSH man page on your workstation for detailed information.

Note: The following procedure is applicable to OpenSSH packages only.

Procedure

1. Open the `sshd_config` file.

   This file can be found in different locations, depending on the operating system. Common locations are `/etc/ssh` or `/opt/ssh/etc`.
2. Search for the following attributes and use the corresponding settings:

Table 8. Secure Shell configuration

Attribute	Setting and description
`UsePrivilegeSeparation`	Yes Use this setting so that the adapter account is not locked after you do a user account operation.
`ClientAliveInterval`	0 This setting disables the **`ClientAliveInterval`** attribute. The adapter does not acknowledge client-keep-alive messages. If the managed resource sends such messages, the connection is ended as a result.
`PasswordAuthentication`	Yes Use this setting only if you are using password based authentication for your adapter service.

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 17.

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.

Service/Target form details

Complete the service/target form fields.

To use SSH to remotely connect to the managed resource, the adapter user account must be one of the following types:

- A root account
- A super user account (SUDO user)
- An account that has root UID permissions

See “Enabling secure communication” on page 25 for information about SSH.

The adapter user account must have:

- Permissions to do user administration tasks, such as add accounts, delete accounts, change passwords for accounts, suspend accounts, restore accounts, and retrieve account data.
- Permissions to do group tasks, such as add groups, modify attributes of a group, and delete groups.

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.

- **User registry**
- **Use a shadow file?**

- **Delete home directory when the account is deleted?**
- **Is sudo user?**
- **Execute user profile?**
- **Authentication method**
- **Passphrase (Required for key-based authentication)**
- **Private key file (Required for key-based authentication)**
- **AL FileSystem Path**
- **Max Connection Count**

On the **Select the Type of Service** page, select:

For AIX operating system:
Select **POSIX AIX Profile**.

For HP-UX operating system:
Select **POSIX HP-UX Profile**.

For Solaris operating system:
Select **POSIX Solaris Profile**.

For Linux operating system:
Select **POSIX Linux Profile**.

On the Service form:

On the General Information 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
Optionally, specify a description that identifies the service for your environment.

IBM Security Directory Integrator URL

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

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

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

Table 9. Ports

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

Table 9. Ports (continued)

Instance	Ports
SDI10	11099, 11098, 11097, 11096, 11095, 11094

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

- 1099
- 2099
- 3099

Managed resource location

Specify the IP address or host name of the managed resource. This location uses the default SSH port, which is port 22. If the SSH port is different, then `ip/host:port` can be used.

Note: An IPv6 address must be enclosed in brackets. An example of a valid IPv6 address format is

```
[fedc:ba98:7654:3210:fedc:ba98:7654:3210]:22
```

RXA Internal Command TimeOut

Specify a value, in milliseconds, to control how long the adapter waits for a response after a remote command is issued to a managed resource. The default value is 5000 milliseconds. Modify this default value if operations on the managed resource timeout frequently.

User registry

This input field is available only on service forms for AIX profiles. This adapter supports user management and authentication by using files or by using LDAP.

Note:

- This field is case-sensitive.
- AIX roles are not reconciled or managed by the adapter for any AIX service with a user registry that is defined as LDAP.

1. If the users on the managed resource are to be managed only through the `/etc/password` file, leave the field blank.
2. If this setup is a mixed and the users are to be managed through the `/etc/password` file, type `files`.

   Note: A mixed setup means that some users on the managed resource are defined in LDAP and some users are defined in files. These users are mutually exclusive and cannot be managed by a single service. If you want Identity server to manage users that are defined in LDAP as well, ensure that you also create a service to manage users through LDAP.
3. If this setup is a mixed setup and the users are to be managed through LDAP, type `LDAP`.

   Note: A mixed setup means that some users on the managed resource are defined files and some users are defined in LDAP. These users are mutually exclusive and cannot be managed by a single service. If you want Identity server to manage users that are defined in files as well, ensure that you also create a service to manage users through files.

Use a shadow file?

Select this check box if shadow passwords are enabled on the managed resource. This field applies to service forms only when you use the Linux or HP-UX service profiles.

For Linux operating systems, shadow passwords are enabled by default. When you create a service for HP-UX, by default the **Use a shadow file?** field is enabled. If the HP-UX system you are connecting to is an HP-UX trusted system, then the **Use a shadow file?** field is irrelevant and the adapter ignores the field.

Delete home directory when the account is deleted?

Select this check box if you want the home directory of the user to be deleted when the user is deleted.

Owner
Optionally specify a user as a service owner.

Service Prerequisite
Optionally, specify a service that is a prerequisite to this service.

On the Additional Configuration tab:
This tab applies only to Linux systems.

Command used to query failed logins
Specifies the system command that is used to detect and tally failed login attempts and enforce account lockout. This command must be configured through the PAM mechanism. If no value is specified, the default **`faillog`** command is used. This command is not available on some operating systems, such as RHEL 6.1 and later versions.

File or directory where failed login records are found
Specifies the absolute path to the location of the failed login attempt datastore, if it is not the default datastore. This field applies to **`faillock`** and **`pam_tally2`** only. The field is ignored when **`faillog`** is used.

If you use **`faillock`**, specify the directory that contains the login record files for individual users. If you use **`pam_tally2`**, specify the full path of the file that contains the login record data for all users.

Maximum failed logins allowed
Specifies the maximum number of failed logins that can occur before an account is locked. This field applies to **`faillock`** and **`pam_tally2`** only. The field is ignored when **`faillog`** is used.

On the Authentication tab:

Administrator name
Specify the user name for the administrator. If you are specifying a super user, instead of a root user, see "Super user creation on a supported operating system" on page 94.

Is sudo user?
Select this check box if the administrator name is a super user. Sudo user privileges must be carefully configured on the resource. For more information about sudo users, see "Super user creation on a supported operating system" on page 94.

Execute user profile?
Available for HP-UX services only.

Click this check box to run the profile of the adapter user before you run operations on the endpoint.

When you create a service for HP-UX, by default the **Execute user profile?** field is disabled. You might want to enable this field if the adapter user profile remaps special terminal control characters on HP-UX (for example @ and #). The profile can remap these characters when the **Execute user profile?** field is enabled. In this case, you can use those special characters in passwords when you add or change accounts. If the field is not enabled and you use a special character, the add or modify operations for the account fail when the password is set.

Running the user profile can affect the runtime environment of the adapter at the endpoint and the outcome of adapter operations. Running the profile has some limitations and must be used with care. For example:

- Do not call another shell from the profile scripts. Doing so can cause the remote operation to hang.
- Do not echo any strings from the profile when you trap signals. The profile must not echo any output from **`trap`** commands. The echoed string might be merged with the results of the command that is running.

Use the default settings for the owner, group, and permissions settings on both the `/etc/profile` and the adapter user `.profile` file. Changing the values for these attributes can cause the remote operation to fail.

Authentication method

From the drop-down menu, select the authentication method to be used by the adapter when it communicates with the managed resource for user management. Select `Password-Based Authentication` or `Key-Based Authentication`. For more information about key-based authentication, see "Key-based authentication for the UNIX and Linux Adapter" on page 109.

Note: This authentication method is only for adapter communication and does not apply to users created on the managed resource by this adapter.

Password

Required for password-based authentication: Specify the password for the administrator.

Passphrase (Required for key-based authentication)

Specify the pass-phrase that is associated with the private key. For more information about private keys, see "Enabling RSA key-based authentication on UNIX and Linux operating systems" on page 109.

Private key file (Required for key-based authentication)

Specify the full path and file name of the keystore that contains the private key of the client. This keystore must be on the workstation that runs the Security Directory Integrator server. For more information about keystore, see "Key-based authentication for the UNIX and Linux Adapter" on page 109.

Allow $ in password

Select this check box to use $ in a password.

Allowed password maximum age limit in Linux and Solaris

If the password maximum age value is greater than the LDAP limit value, then adapter will set LDAP limit value for password maximum age. See Adapter attributes and object classes.

On the Dispatcher Attributes tab:

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. 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\`*`TDI_VERSION`*`\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/`*`TDI_VERSION`*`/profiles`

Max Connection Count

Specify the maximum number of assembly lines that the dispatcher can run 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 run simultaneously for the service.

Disable AL Caching

Select the check box to disable the assembly line caching for add, modify, and delete operations in the dispatcher 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. You can verify the work station name or the IP address of the managed resource and the port.

Installing the adapter language package

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

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

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 serverIdentity server.
2. Run a full reconciliation from the Identity serverIdentity 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

User home directory creation
The UNIX and Linux Adapter provides a user-selectable option to create a default home directory for a user or an account.

Customizing the adapter
The adapters can be customized or extended or both. The type and method of this customization varies depending on the adapter.

Customizing the adapter attributes
Depending on your needs, the adapter has attributes that you can optionally configure for the following capabilities.

Password management for account restoration

When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must change the adapter profile JAR file. You might customize the adapter profile to change the account form or the service form. You can also change the labels on the forms by using the Form Designer or the `CustomLabels.properties` file. Each adapter has a `CustomLabels.properties` file.

Running user-defined scripts
The UNIX and Linux Adapter is configured to run user-defined scripts before a request is processed (preexec), after a request is processed (postexec), or both.

Defining the maximum connection count for adapter operations
You can limit the number of connections that can be made to a resource based on the service, service type, and operation. You can modify the `service.def` file in the service profile. Alternatively, you can specify a value for the **Max Connection Count** field on the service form of a resource.

Editing adapter profiles on the UNIX or Linux operating system
The adapter profile `.jar` file might contain ASCII files that are created by using the MS-DOS ASCII format.

Configuring self-password change
Configure self-password change with the AIX, Linux and Solaris profile jar files.

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.

Installing and uninstalling in silent mode

You can use the `-i silent` option to install or uninstall the adapter in silent mode.

Silent installation suppresses the adapter installation wizard and the Launcher User Interfaces (UIs). It does not display any information or require interaction.

Installing the adapter in silent mode

You can either use the default settings or override those settings when you install the adapter in silent mode.

About this task

If you accept the default setting for the silent installation, the adapter is installed in a location that depends on your operating system.

Windows operating systems

```
%SYSTEM_DRIVE_ROOT%\Program Files\IBM\TDI\V7.1
```

UNIX and Linux operating systems

```
/opt/IBM/TDI/V7.1
```

You can override the default settings with the **-D** parameter. The **-D** must be followed immediately by an option-value pair. No space exists after **-D**.

Note: If an argument contains spaces, you must wrap the argument in quotation marks.

Table 10. silent mode parameters for installing

Parameter	Description
`-DUSER_INSTALL_DIR`	This parameter overrides the default installation path. For example, `-DUSER_INSTALL_DIR="D:/security/MyFolder"`
`-DFORCE_DISPATCHER_SERVICE_START_ONINSTALL`	If the dispatcher service is running before the installation, the installer stops the service. It restarts the service after the installation is completed. If the dispatcher service is not running before the installation, use this parameter to start the service after the installation. Set the value of the parameter to YES.

Procedure

1. Go to a command line.
2. Run either of the following commands:
   - To install the adapter in silent mode with the default settings, issue the command:

     ```
     java -jar PosixAdapterInstall_70.jar -i silent
     ```

   - To install the adapter in silent mode and changing one or more default settings, use the **-D** parameter. For example, this command overrides the default installation directory for a Windows operating system.

     ```
     java -jar PosixAdapterInstall_70.jar -i silent
     -DUSER_INSTALL_DIR="E:\Program Files\IBM\TDI\V7.1"
     ```

Results

The adapter is installed in the adapter installation directory.

Uninstalling the adapter in silent mode

You can uninstall the adapter with the –silent option.

About this task

Run the command from the `PosixAdapterUninstall` directory in the installation directory of the adapter. If you run the command from a different directory, you must specify the full file path to the `uninstaller.jar` file. For example, this command is run from outside the `PosixAdapterUninstall` directory.

```
java
-jar "E:\Program Files\IBM\TDI\V7.1\PosixAdapterUninstall\uninstaller.jar"
-i silent
```

Table 11. silent mode parameter for uninstalling

Parameter	Description
`-DFORCE_DISPATCHER_SERVICE_START_ONUNINSTALL`	If the dispatcher service is running before the uninstallation, the installer stops the service. It restarts the service after the uninstallation is completed. If the dispatcher service is not running before the uninstallation, use this parameter to start the service after the uninstallation. Set the value of the parameter to YES.

Procedure

1. Go to a command line.
2. Run either of the following commands:

   - To uninstall the adapter with the default settings, run the command:

     ```
     java -jar uninstaller.jar -i silent
     ```

   - To ensure that the dispatcher service is restarted after you uninstall the adapter, run the command:

     ```
     java -jar uninstaller.jar -i silent
     -DFORCE_DISPATCHER_SERVICE_START_ONUNINSTALL=yes
     ```

Results

The adapter is removed without any additional user response or interaction.

Chapter 5. Upgrading

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

To verify the required version of these adapter components, see the adapter release notes.

Upgrading the adapter binaries or connector

The new adapter package might require you to upgrade the connector.

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

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

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

Upgrading the dispatcher

The new adapter package might require you to upgrade 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.

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.

Chapter 6. Configuring

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

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

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

Customizing the adapter profile

To customize the adapter profile, you must change the adapter profile JAR file. You might customize the adapter profile to change the account form or the service form. You can also change the labels on the forms by using the Form Designer or the `CustomLabels.properties` file. Each adapter has a `CustomLabels.properties` file.

About this task

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

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

AIX (`PosixAixProfile.jar`)

The following files are included in the AIX profile JAR file:

- `CustomLabels.properties`
- `erPosixAixAccount.xml`
- `erPosixAixRMIService.xml`
- `posixAdd.xml`
- `posixDelete.xml`
- `posixModify.xml`
- `posixSearch.xml`
- `posixTest.xml`
- `schema.dsml`
- `service.def`
- `posixGroupAdd.xml`
- `posixGroupDelete.xml`
- `posixGroupModify.xml`
- `posixRoleAdd.xml`
- `posixRoleDelete.xml`
- `posixRoleModify.xml`

HP-UX (`PosixHpuxProfile.jar`)

The following files are included in the HP-UX profile JAR file:

- `CustomLabels.properties`
- `erPosixHpuxAccount.xml`
- `erPosixHpuxRMIService.xml`
- `posixAdd.xml`
- `posixDelete.xml`
- `posixModify.xml`
- `posixSearch.xml`
- `posixTest.xml`
- `schema.dsml`
- `service.def`
- `posixGroupAdd.xml`
- `posixGroupDelete.xml`
- `posixGroupModify.xml`

Solaris (`PosixSolarisProfile.jar`)

The following files are included in the Solaris profile JAR file:

- `CustomLabels.properties`
- `erPosixSolarisAccount.xml`
- `erPosixSolarisRMIService.xml`
- `posixAdd.xml`
- `posixDelete.xml`
- `posixModify.xml`
- `posixSearch.xml`
- `posixTest.xml`
- `schema.dsml`
- `service.def`
- `posixGroupAdd.xml`
- `posixGroupDelete.xml`
- `posixGroupModify.xml`

Linux (`PosixLinuxProfile.jar`)

The following files are included in the Linux profile JAR file:

- `CustomLabels.properties`
- `erPosixLinuxAccount.xml`
- `erPosixLinuxRMIService.xml`
- `posixAdd.xml`
- `posixDelete.xml`
- `posixModify.xml`
- `posixSearch.xml`
- `posixTest.xml`
- `schema.dsml`
- `service.def`
- `posixGroupAdd.xml`

- `posixGroupDelete.xml`
- `posixGroupModify.xml`

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

Procedure

1. Edit the profile JAR file.
   a) Log in to the system where the UNIX and Linux Adapter is installed.
   b) Copy the JAR file into a temporary directory.
   c) Extract the contents of the JAR file into the temporary directory.

      Run the following command. The following example applies to the Linux adapter profile. Type the name of the JAR file for your operating system.

      ```
      cd c:\temp #cd /tmp
      #jar -xvf PosixLinuxProfile.jar
      ```

      The **`jar`** command extracts the files into the PosixLinuxProfile directory.
   d) Edit the file that you want to change.
   e) Save the file.
2. Import the file.
   a) Create a JAR file by using the files in the `\temp/tmp` directory

      Run the following command:

      ```
      #cd /tmp cd c:\temp
      #jar -cvf PosixLinuxProfile.jar PosixLinuxProfile
      ```
   b) Import the JAR file into the IBM Security Verify Governance Identity ManagerIBM Security Verify GovernanceIBM Security Privileged Identity Manager application server.
   c) Stop and start the Identity server
   d) Restart the adapter service.

Related concepts

User home directory creation
The UNIX and Linux Adapter provides a user-selectable option to create a default home directory for a user or an account.

Customizing the adapter
The adapters can be customized or extended or both. The type and method of this customization varies depending on the adapter.

Customizing the adapter attributes
Depending on your needs, the adapter has attributes that you can optionally configure for the following capabilities.

Password management for account restoration
When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account.

Related tasks

Running user-defined scripts
The UNIX and Linux Adapter is configured to run user-defined scripts before a request is processed (preexec), after a request is processed (postexec), or both.

Defining the maximum connection count for adapter operations
You can limit the number of connections that can be made to a resource based on the service, service type, and operation. You can modify the `service.def` file in the service profile. Alternatively, you can specify a value for the **Max Connection Count** field on the service form of a resource.

Editing adapter profiles on the UNIX or Linux operating system

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

Configuring self-password change
Configure self-password change with the AIX, Linux and Solaris profile jar files.

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

Running user-defined scripts

The UNIX and Linux Adapter is configured to run user-defined scripts before a request is processed (preexec), after a request is processed (postexec), or both.

About this task

Running user-defined scripts can be useful when external activities are required to manage the resource. Use these attributes that are defined in the relevant Posix account form:

- Pre-execution options:

  erPosixPreExec
  Always continue the operation regardless of the pre-execution script outcome (succeed or fail).

  erPosixPreExecRunOption
  Continue the operation only when the pre-execution script succeeds.

- Post-execution options:

  erPosixPostExec
  Always continue the operation regardless of the post-execution script outcome (succeed or fail).

  erPosixPostExecRunOption
  Continue the operation only when the post-execution script succeeds.

Note:

1. The term *operation* refers to any account management request. For example, **`user add`** or **`user modify`**.
2. The status or outcome of the **`preexec`** and **`postexec`** commands are not returned to the Identity server.
3. On a modify request, the Identity server sends only those attributes whose values are changed. This behavior differs from an add operation in which all the attributes are always sent. The modify behavior applies to the **`preexec`** and **`postexec`** attributes.

To send these attributes on a modify operation regardless of actual value changes, update the `service.def` file for the relevant Posix adapter profile.

Procedure

1. Extract the adapter profile JAR file.
   For example, `PosixAIXProfile.jar`
2. Open the `service.def` file in a text editor.
3. Insert the following lines in `service.def`, under `<operation cn="posixModify">`

```
<input name="erPosixPreExec" source="erPosixPreExec"></input>
<input name="erPosixPostExec" source="erPosixPostExec""></input>
<input name="erPosixPreExecRunOption" source="erPosixPreExecRunOption">
</input>
<input name="erPosixPostExecRunOption" source="erPosixPostExecRunOption">
</input>
```

4. Save the changes and create another adapter profile JAR file.

```
jar -cvf PosixAixProfile.jar PosixAixProfile
```

Related concepts

User home directory creation
The UNIX and Linux Adapter provides a user-selectable option to create a default home directory for a user or an account.

Customizing the adapter
The adapters can be customized or extended or both. The type and method of this customization varies depending on the adapter.

Customizing the adapter attributes
Depending on your needs, the adapter has attributes that you can optionally configure for the following capabilities.

Password management for account restoration
When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must change the adapter profile JAR file. You might customize the adapter profile to change the account form or the service form. You can also change the labels on the forms by using the Form Designer or the `CustomLabels.properties` file. Each adapter has a `CustomLabels.properties` file.

Defining the maximum connection count for adapter operations
You can limit the number of connections that can be made to a resource based on the service, service type, and operation. You can modify the `service.def` file in the service profile. Alternatively, you can specify a value for the **Max Connection Count** field on the service form of a resource.

Editing adapter profiles on the UNIX or Linux operating system
The adapter profile `.jar` file might contain ASCII files that are created by using the MS-DOS ASCII format.

Configuring self-password change
Configure self-password change with the AIX, Linux and Solaris profile jar files.

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

Defining the maximum connection count for adapter operations

You can limit the number of connections that can be made to a resource based on the service, service type, and operation. You can modify the `service.def` file in the service profile. Alternatively, you can specify a value for the **Max Connection Count** field on the service form of a resource.

About this task

Limit the number of concurrent connections to a resource if you see errors that are caused by contention for files or other objects on the resource. For example, when many operations occur at the same time for account add, some might fail because they cannot get write access to the `/etc/passwd` file. To reduce contention, lower the maximum connection count for the resource or the add operation.

To set a default or an absolute maximum connection count for a service type, modify the `service.def` file. A default count can be overridden on a per-resource basis; an absolute count cannot be overridden.

To change the `service.def` file, take these steps:

Procedure

1. Extract the adapter profile JAR file.
   For example, extract `PosixAIXProfile.jar` with this command:

```
jar -xvf PosixAixProfile.jar
```

2. Open the `service.def` file in a text editor.
3. To limit the maximum connections for an operation type, first locate the type.
   A maximum connection count is defined for each operation type such as add (**posixAdd**) or modify (**posixModify**). Locate the type of operation whose maximum connection count you want to set. For example, locate the **posixModify** operation:

   ```
   <operation cn="posixModify">
   ```

4. Find the `<dispatcherParameter name="MaxConnectionCnt"...>` element under the **posixModify** operation entry.
5. Edit the **dispatcherParameter** element to specify a default value or an absolute value.

   - Specify a default value.

     Create an entry similar to this example:

     ```
     <dispatcherParameter name="MaxConnectionCnt" source= "erPosixMaxConnectionCnt">
         <default>value</default>
     </dispatcherParameter>
     ```

     For any AIX resource, the maximum number of concurrent operations for account modify has a default of *value*. To override this default, specify a different value in the **Max Connection Count** field on the **Dispatcher Attributes** tab of the service form of the AIX resource.

   - Specify an absolute value.

     Create an entry similar to this example:

     ```
     <dispatcherParameter name="MaxConnectionCnt">
         <value>value</value>
     </dispatcherParameter>
     ```

     For any AIX resource, the maximum number of concurrent operations for account modify is *value*, which cannot be overridden.

   Note:

   - The maximum number of connections for search (recon) operations is always one, regardless of the settings in the `service.def` file or on the service form.
   - If no maximum connection count is defined in the `service.def` file or on the service form, the connection count is unlimited.

6. Save the changes and create another adapter profile JAR file.
   For example:

   ```
   jar -cvf PosixAixProfile.jar PosixAixProfile
   ```

7. Import the modified profile JAR file into the Identity server.

Related concepts

User home directory creation
The UNIX and Linux Adapter provides a user-selectable option to create a default home directory for a user or an account.

Customizing the adapter
The adapters can be customized or extended or both. The type and method of this customization varies depending on the adapter.

Customizing the adapter attributes
Depending on your needs, the adapter has attributes that you can optionally configure for the following capabilities.

Password management for account restoration

When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must change the adapter profile JAR file. You might customize the adapter profile to change the account form or the service form. You can also change the labels on the forms by using the Form Designer or the `CustomLabels.properties` file. Each adapter has a `CustomLabels.properties` file.

Running user-defined scripts
The UNIX and Linux Adapter is configured to run user-defined scripts before a request is processed (preexec), after a request is processed (postexec), or both.

Editing adapter profiles on the UNIX or Linux operating system
The adapter profile `.jar` file might contain ASCII files that are created by using the MS-DOS ASCII format.

Configuring self-password change
Configure self-password change with the AIX, Linux and Solaris profile jar files.

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

User home directory creation

The UNIX and Linux Adapter provides a user-selectable option to create a default home directory for a user or an account.

The default home directory is created by concatenating the base directory value that is defined on that system with the account name or user name to be created.

Example

The base directory value on the target system is `/home`. The user name for the account that is being created is `testuser`. The default home directory is `/home/testuser`.

Note: AIX systems ignore this option. The AIX operating systems create a home directory by default for each new account.

Related concepts

Customizing the adapter
The adapters can be customized or extended or both. The type and method of this customization varies depending on the adapter.

Customizing the adapter attributes
Depending on your needs, the adapter has attributes that you can optionally configure for the following capabilities.

Password management for account restoration
When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must change the adapter profile JAR file. You might customize the adapter profile to change the account form or the service form. You can also change the labels on the forms by using the Form Designer or the `CustomLabels.properties` file. Each adapter has a `CustomLabels.properties` file.

Running user-defined scripts

The UNIX and Linux Adapter is configured to run user-defined scripts before a request is processed (preexec), after a request is processed (postexec), or both.

Defining the maximum connection count for adapter operations
You can limit the number of connections that can be made to a resource based on the service, service type, and operation. You can modify the `service.def` file in the service profile. Alternatively, you can specify a value for the **Max Connection Count** field on the service form of a resource.

Editing adapter profiles on the UNIX or Linux operating system
The adapter profile `.jar` file might contain ASCII files that are created by using the MS-DOS ASCII format.

Configuring self-password change
Configure self-password change with the AIX, Linux and Solaris profile jar files.

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

User home directory creation
The UNIX and Linux Adapter provides a user-selectable option to create a default home directory for a user or an account.

Customizing the adapter
The adapters can be customized or extended or both. The type and method of this customization varies depending on the adapter.

Customizing the adapter attributes
Depending on your needs, the adapter has attributes that you can optionally configure for the following capabilities.

Password management for account restoration
When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must change the adapter profile JAR file. You might customize the adapter profile to change the account form or the service form. You can also change the labels

on the forms by using the Form Designer or the `CustomLabels.properties` file. Each adapter has a `CustomLabels.properties` file.

Running user-defined scripts
The UNIX and Linux Adapter is configured to run user-defined scripts before a request is processed (preexec), after a request is processed (postexec), or both.

Defining the maximum connection count for adapter operations
You can limit the number of connections that can be made to a resource based on the service, service type, and operation. You can modify the `service.def` file in the service profile. Alternatively, you can specify a value for the **Max Connection Count** field on the service form of a resource.

Configuring self-password change
Configure self-password change with the AIX, Linux and Solaris profile jar files.

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

Configuring self-password change

Configure self-password change with the AIX, Linux and Solaris profile jar files.

About this task

The adapter package contains a new folder called **PIM-Specific**. This folder contains AIX, Linux and Solaris profile jar files.

Note: The profiles must only be installed on an IBM Security Privileged Identity Manager server.

These profiles support the following limited functionality:

- Self-password change
- User look up

Note: For these functionalities to work correctly, the IBM Security Privileged Identity Manager user must have the permission to `/usr/bin/logins`: `'execute'` permission to others.

The service forms in the IBM Security Privileged Identity Manager profile have a new required field called **Authentication Mode**. Set this field to `admin` if the adapter user is privileged -- root or a sudo user. Set this field to `self` if the adapter user is not privileged.

During a password change operation, the adapter uses an interactive secure shell (SSH) session. The adapter waits for default password prompts from the managed resource to complete the transaction. If the managed resource has customized password prompts, you must specify those prompts on the adapter service form. The **PIM-Specific** profiles introduce a new password prompt attribute, **`erPosixOldRegx`** that holds the regular expression string for the old password prompt. The old password prompt is required for the self-password change operations.

The default old password prompt is **`.*old password:$.`**. If the managed system old password prompt differs from this regular expression, customize the prompt on the service form by performing the following steps on the IBM Security Privileged Identity Manager console:

Procedure

1. Log on to IBM Security Privileged Identity Manager Administrative Console as an administrator.
2. From the navigation pane, select **Configure System** > **Design Forms**.
3. From the applet, double click **Service** to display the service form profiles.
4. Double click one of the following the service form profiles that you require for customization:
   - Posix AIX Account
   - Posix Linux Account
   - Posix Solaris Account

5. From the **Attributes List**, select the **erPosixOldRegx** attribute to add it to the service form.
6. Click the **Save Form Template** icon to save the changes and click **OK**.

   Once the form is saved, the **Old Password Regular expression** field is present on the service form and can be used to customize the prompt.

Related concepts

User home directory creation
The UNIX and Linux Adapter provides a user-selectable option to create a default home directory for a user or an account.

Customizing the adapter
The adapters can be customized or extended or both. The type and method of this customization varies depending on the adapter.

Customizing the adapter attributes
Depending on your needs, the adapter has attributes that you can optionally configure for the following capabilities.

Password management for account restoration
When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must change the adapter profile JAR file. You might customize the adapter profile to change the account form or the service form. You can also change the labels on the forms by using the Form Designer or the `CustomLabels.properties` file. Each adapter has a `CustomLabels.properties` file.

Running user-defined scripts
The UNIX and Linux Adapter is configured to run user-defined scripts before a request is processed (preexec), after a request is processed (postexec), or both.

Defining the maximum connection count for adapter operations
You can limit the number of connections that can be made to a resource based on the service, service type, and operation. You can modify the `service.def` file in the service profile. Alternatively, you can specify a value for the **Max Connection Count** field on the service form of a resource.

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.

Customizing the adapter

The adapters can be customized or extended or both. The type and method of this customization varies depending on the adapter.

Customizing and extending adapters requires a number of skills. The developer must be familiar with the following concepts and skills:

- IBM Security Verify Governance Identity ManagerIBM Security Verify GovernanceIBM Security Privileged Identity Manager administration
- IBM Security Directory Integrator management
- Security Directory Integrator Assembly Line development
- LDAP schema management
- Working knowledge of Java scripting language
- Working knowledge of LDAP object classes and attributes
- Working knowledge of XML document structure

Note: If the customization requires a new Security Directory Integrator connector, the developer must also be familiar with Security Directory Integrator connector development and working knowledge of Java programming language.

IBM Security Verify Governance Identity ManagerIBM Security Verify GovernanceIBM Security Privileged Identity Manager resources

See the "Learn" section of the IBM Security Verify Governance Identity Manager Support website for links to training, publications, and demonstrations.

Security Directory Integrator resources

See the "Learn" section of the Security Directory Integrator Support website for links to training, publications, and demonstrations.

IBM Security Verify Governance Identity Manager adapter development resources

Adapter Development Tool

The Adapter Development Tool (ADT) is a tool that is used by IBM Security Verify Governance Identity ManagerIBM Security Verify GovernanceIBM Security Privileged Identity Manager customers and consultants to create custom adapters. It reduces adapter delivery time and it helps in the development of custom adapters. The ADT is available from the IBM Open Process Automation Library (OPAL) website.

Support for customized adapters

The integration to the Identity server server, the adapter framework, is supported. However, IBM does not support the customizations, scripts, or other modifications. You might experience a problem with a customized adapter. In this case, IBM Support might require the problem to be demonstrated on the GA version of the adapter before a PMR is opened.

Related concepts

User home directory creation
The UNIX and Linux Adapter provides a user-selectable option to create a default home directory for a user or an account.

Customizing the adapter attributes
Depending on your needs, the adapter has attributes that you can optionally configure for the following capabilities.

Password management for account restoration
When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must change the adapter profile JAR file. You might customize the adapter profile to change the account form or the service form. You can also change the labels on the forms by using the Form Designer or the `CustomLabels.properties` file. Each adapter has a `CustomLabels.properties` file.

Running user-defined scripts
The UNIX and Linux Adapter is configured to run user-defined scripts before a request is processed (preexec), after a request is processed (postexec), or both.

Defining the maximum connection count for adapter operations
You can limit the number of connections that can be made to a resource based on the service, service type, and operation. You can modify the `service.def` file in the service profile. Alternatively, you can specify a value for the **Max Connection Count** field on the service form of a resource.

Editing adapter profiles on the UNIX or Linux operating system
The adapter profile `.jar` file might contain ASCII files that are created by using the MS-DOS ASCII format.

Configuring self-password change

Configure self-password change with the AIX, Linux and Solaris profile jar files.

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

Customizing the adapter attributes

Depending on your needs, the adapter has attributes that you can optionally configure for the following capabilities.

Related concepts

User home directory creation
The UNIX and Linux Adapter provides a user-selectable option to create a default home directory for a user or an account.

Customizing the adapter
The adapters can be customized or extended or both. The type and method of this customization varies depending on the adapter.

Password management for account restoration
When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must change the adapter profile JAR file. You might customize the adapter profile to change the account form or the service form. You can also change the labels on the forms by using the Form Designer or the `CustomLabels.properties` file. Each adapter has a `CustomLabels.properties` file.

Running user-defined scripts
The UNIX and Linux Adapter is configured to run user-defined scripts before a request is processed (preexec), after a request is processed (postexec), or both.

Defining the maximum connection count for adapter operations
You can limit the number of connections that can be made to a resource based on the service, service type, and operation. You can modify the `service.def` file in the service profile. Alternatively, you can specify a value for the **Max Connection Count** field on the service form of a resource.

Editing adapter profiles on the UNIX or Linux operating system
The adapter profile `.jar` file might contain ASCII files that are created by using the MS-DOS ASCII format.

Configuring self-password change
Configure self-password change with the AIX, Linux and Solaris profile jar files.

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

Customizing password prompt attributes

The UNIX and Linux Adapter does password changes by using an interactive Secure Shell (SSH) session. The adapter searches for the default password prompts on the managed resource to complete the transaction successfully. If the managed resource has customized password prompts, then you can specify the password prompts on the service form that the adapter must search for.

About this task

The password prompt attributes are:

- **erPosixNewRegx** - the new password prompt
- **erPosixRetypeRegx** - the retype password prompt

To customize these password prompt attributes on the service form, do the following steps from IBM Security Verify Governance Identity ManagerIBM Security Verify GovernanceIBM Security Privileged Identity Manager. The customized password prompt attributes are displayed on the service form. The adapter does a case-insensitive match on these password prompts.

Procedure

1. Log on to IBM Security Verify Governance Identity ManagerIBM Security Verify GovernanceIBM Security Privileged Identity Manager as an administrator.Edit the profile JAR file.
   a) Log in to the system where the UNIX and Linux Adapter is installed.
   b) Copy the JAR file into a temporary directory.
   c) Extract the contents of the JAR file into the temporary directory. Run the following command. The following example applies to the Linux adapter profile.
   d) Type the name of the JAR file for your operating system.

   ```
   #cd /tmp
   #jar -xvf PosixLinuxProfile.jar
   ```

   The jar command extracts the files into the `PosixLinuxProfile` directory.
   e) Edit the `Service.xml` file for your respective profile. For example, `erPosixLinuxRMIService.xml` in the case of the Linux adapter.
   f) Remove the comment for the following attributes section so that these two attributes are visible on service form on IBM Security Verify Governance.

   ```
   <!-- Remove Following Comments to Add Password Expression On Service Form Statically -->
                           <!-- <formElement label="$erposixnewregx"
   name="data.erposixnewregx"> -->
                   <!--          <input type="text" size="50" name="data.erposixnewregx"/>
   -->
                           <!--  </formElement> -->
                           <!-- <formElement label="$erposixretyperegx"
   name="data.erposixretyperegx"> -->
                   <!--          <input type="text" size="50"
   name="data.erposixretyperegx"/> -->
                           <!-- </formElement> -->
   ```

   g) Save the changes.
2. Import the file.
   a) Create a JAR file by using the files in the /tmp directory Run the following command:

   ```
   #cd /tmp
   #jar -cvf PosixLinuxProfile.jar PosixLinuxProfile
   ```

   b) Import the JAR file into the Identity server.
   c) Stop and start the Identity server.
   d) Restart the adapter service.

   POSIX AIX account
   Customize the **erPosixNewRegx** and **erPosixRetypeRegx** attributes on the AIX service form. The default values of these attributes on this account are:

   ```
   erPosixNewRegx = ".*new password:$"
   erPosixRetypeRegx = "re-enter .* new password:"
   ```

   POSIX HP-UX account
   Customize the **erPosixNewRegx** and **erPosixRetypeRegx** attributes on the HP-UX service form.The default values of these attributes on this account are:

   ```
   erPosixNewRegx = ".*new password:$"
   erPosixRetypeRegx = ".*re-enter new password:$"
   ```

POSIX Linux account

Customize the **erPosixNewRegx** and **erPosixRetypeRegx** attributes on the Linux service form The default values of these attributes on this account are:

```
erPosixNewRegx = ".*new password:$"
erPosixRetypeRegx = ".*re-enter new password:$"
```

POSIX Solaris account

Customize the **erPosixNewRegx** and **erPosixRetypeRegx** attributes on the Solaris service form. The default values of these attributes on this account are:

```
erPosixNewRegx = ".*new password:$"
erPosixRetypeRegx = ".*re-enter new password:$"
```

3. After reimporting the changed profile on Identity server, the following attributes are available on the service form:

   - New Password Regular expression
   - Retype Password Regular expression

4. In the My Work pane, expand **Configure System** and click **Design Forms** to display the **Design Forms** page.
5. From the applet, double-click **Service** to display the service form profiles.
6. Double-click the service form profile whose service form you want to customize.

   Select one of the following profiles:

   POSIX AIX account

   Select this option to customize the **erPosixNewRegx** and **erPosixRetypeRegx** attributes on the AIX service form. The default values of these attributes on this account are:

   ```
   erPosixNewRegx = ".*new password:$"
   erPosixRetypeRegx = "re-enter .* new password:"
   ```

   POSIX HP-UX account

   Select this option to customize the **erPosixNewRegx** and **erPosixRetypeRegx** attributes on the HP-UX service form.The default values of these attributes on this account are:

   ```
   erPosixNewRegx = ".*new password:$"
   erPosixRetypeRegx = ".*re-enter new password:$"
   ```

   POSIX Linux account

   Select this option to customize the **erPosixNewRegx** and **erPosixRetypeRegx** attributes on the Linux service form The default values of these attributes on this account are:

   ```
   erPosixNewRegx = ".*new password:$"
   erPosixRetypeRegx = ".*re-enter new password:$"
   ```

   POSIX Solaris account

   Select this option to customize the **erPosixNewRegx** and **erPosixRetypeRegx** attributes on the Solaris service form. The default values of these attributes on this account are:

   ```
   erPosixNewRegx = ".*new password:$"
   erPosixRetypeRegx = ".*re-enter new password:$"
   ```

7. From the **Attributes List** window, double-click the **erPosixNewRegx** attribute to add it to the service form.
8. From the **Attributes List** window, double-click the **erPosixRetypeRegx** attribute to add it to the service form.
9. Click **Save Form Template** icon.

   After you customize the password prompt attributes, the following attributes are available on the service form:

   - New Password Regular expression

- Retype Password Regular expression

Adding home directory permissions on the account form

You might want to add or modify the home directory permissions of the user on the managed resource.

About this task

To modify the home directory permissions, you must customize the **erPosixHomeDir** attribute on the account form. Do the following steps on IBM Security Verify Governance Identity ManagerIBM Security Verify GovernanceIBM Security Privileged Identity Manager:

Procedure

1. Log on to IBM Security Verify Governance Identity ManagerIBM Security Verify GovernanceIBM Security Privileged Identity Manager as an administrator.Edit the profile JAR file.
   a) Log in to the system where the UNIX and Linux Adapter is installed.
   b) Copy the JAR file into a temporary directory.
   c) Extract the contents of the JAR file into the temporary directory. Run the following command. The following example applies to the Linux adapter profile.
   d) Type the name of the JAR file for your operating system.

```
#cd /tmp
#jar -xvf PosixLinuxProfile.jar
```

   The jar command extracts the files into the `PosixLinuxProfile` directory.
   e) Edit the `Account.xml` file for your respective profile. For example, `erPosixLinuxAccount.xml` in the case of the Linux adapter.
   f) Add `erPosixPerHomeDir` attribute under `$tabemployee` info tab on account.xml for your respective profile. See the following example:

```

<formElement direction="inherit" label="$erposixperhomedir” name="data.erposixperhomedir">
                    <input type="text" name="data.erposixperhomedir"/>
                </formElement>
```

   g) Save the changes.
2. Import the file.
   a) Create a JAR file by using the files in the `/tmp` directory Run the following command:

```
#cd /tmp
#jar -cvf PosixLinuxProfile.jar PosixLinuxProfile
```

   b) Import the JAR file into the Identity server.
   c) Stop and start the Identity server.
   d) Restart the adapter service.
3. To manage this attribute on account form, discover attributes from target system on Identity server. See Discovering attributes from a target system in the Identity server documentation.

   After performing the steps above, `erPosixPerHomeDir` is visible on account form on Identity server.

   POSIX AIX account
   Select this option to customize the **erPosixHomeDir** attribute on the AIX account form.

   POSIX HP-UX account
   Select this option to customize the **erPosixHomeDir** attribute on the HP-UX account form.

   POSIX Linux account
   Select this option to customize the **erPosixHomeDir** attribute on the Linux account form.

POSIX Solaris account
Select this option to customize the **erPosixHomeDir** attribute on the Solaris account form.

4. In the My Work pane, expand **Configure System** and click **Design Forms** to display the **Design Forms** page.
5. From the applet, double-click **Account** to display the account form profiles.
6. Double-click the account form profile to add the **erPosixHomeDir** attribute on the account form.

   Select one of the following profiles:

   POSIX AIX account
   Select this option to customize the **erPosixHomeDir** attribute on the AIX account form.

   POSIX HP-UX account
   Select this option to customize the **erPosixHomeDir** attribute on the HP-UX account form.

   POSIX Linux account
   Select this option to customize the **erPosixHomeDir** attribute on the Linux account form.

   POSIX Solaris account
   Select this option to customize the **erPosixHomeDir** attribute on the Solaris account form.
7. From the **Attributes List** window, double-click the **erPosixHomeDir** attribute to add it to the **$tabemployeeinfo** tab.
8. Right-click **erposixperhomedir** and click **Change To**>**UMask**.
9. Click the **Save Form Template** icon.

   After you customize the attribute, the **Home directory permissions** attribute is available on the account form.

Adding umask settings on the account form

You might want to add or modify the umask permissions of the user on the managed resource. The umask settings control how file permissions are set for newly created files.

About this task

To modify the umask permissions, you must customize the **erPosixUmask** attribute on the account form. Do the following steps on IBM Security Verify Governance Identity ManagerIBM Security Verify GovernanceIBM Security Privileged Identity Manager:

Procedure

1. Log on to IBM Security Verify Governance Identity ManagerIBM Security Verify GovernanceIBM Security Privileged Identity Manager as an administrator.Edit the profile JAR file.
   a) Log in to the system where the UNIX and Linux Adapter is installed.
   b) Copy the JAR file into a temporary directory.
   c) Extract the contents of the JAR file into the temporary directory. Run the following command. The following example applies to the Linux adapter profile.
   d) Type the name of the JAR file for your operating system.

   ```
   #cd /tmp
   #jar -xvf PosixLinuxProfile.jar
   ```

   The jar command extracts the files into the `PosixLinuxProfile` directory.

   e) Edit the `Account.xml` file for your respective profile. For example, `erPosixLinuxAccount.xml` in the case of the Linux adapter.
   f) Add `erPosixUmask` attribute under `$tabemployee` info tab on account.xml for your respective profile. See the following example:

   ```

   <formElement direction="inherit" label="$erposixumask" name="data.erposixumask">
   ```

```
                    <input type="text" name="data.erposixumask"/>
                </formElement>
```

g) Save the changes.

2. Import the file.

   a) Create a JAR file by using the files in the `/tmp` directory Run the following command:

   ```
   #cd /tmp
   #jar -cvf PosixLinuxProfile.jar PosixLinuxProfile
   ```

   b) Import the JAR file into the Identity server.

   c) Stop and start the Identity server.

   d) Restart the adapter service.

3. To manage this attribute on account form, discover attributes from target system on Identity server. See Discovering attributes from a target system in the Identity server documentation.

   After performing the steps above, `erPosixUmask` is visible on account form on Identity server.

   POSIX AIX account
   Select this option to customize the **`erPosixUmask`** attribute on the AIX account form.

   POSIX HP-UX account
   Select this option to customize the **`erPosixUmask`** attribute on the HP-UX account form.

   POSIX Linux account
   Select this option to customize the **`erPosixUmask`** attribute on the Linux account form.

   POSIX Solaris account
   Select this option to customize the **`erPosixUmask`** attribute on the Solaris account form.

4. After you customize the attribute, use it when you are creating or modifying a user account.

   Locate the attribute that is labeled UNIX umask on the account form and use the **Access Type** permission boxes to change or set the read, write, and execute permissions for user, group, and other access.

5. In the **My Work** pane, expand **Configure System** and click **Design Forms** to display the **Design Forms** page.

6. From the applet, double-click **Account** to display the account form profiles.

7. Double-click the account form profile to add the **`erPosixUmask`** attribute on the account form.

   Select one of the following profiles:

   POSIX AIX account
   Select this option to customize the **`erPosixUmask`** attribute on the AIX account form.

   POSIX HP-UX account
   Select this option to customize the **`erPosixUmask`** attribute on the HP-UX account form.

   POSIX Linux account
   Select this option to customize the **`erPosixUmask`** attribute on the Linux account form.

   POSIX Solaris account
   Select this option to customize the **`erPosixUmask`** attribute on the Solaris account form.

8. From the **Attributes List** window, double-click the **`erPosixUmask`** attribute to add it to the **$tabemployeeinfo** tab.

9. Right-click **erPosixUmask** and click **Change To**>**UMask**.

10. Click the **Save Form Template** icon.

    After you customize the attribute, you can use it when you create or modify a user account.

    Locate the attribute that is labeled **UNIX umask** on the account form and use the **Access Type** permission boxes to change or set the read, write and execute permissions for user, group and other access.

Setting up locales

You can specify a particular code page for the adapter to use when encoding and decoding data. By default, the adapter uses the same locale and code page that are specified for the administrative user account that the adapter uses on the managed resource. The locale and code page are typically the same as the system locale and code page. If the locales and code pages are different, use this task to configure the adapter to use the system locale and code page.

About this task

The **erPosixEncoding** attribute provides enhanced support in the Posix adapter for characters sets from user-specified locales.

Procedure

1. Open the DESIGN FORMS feature of the Identity server. Click **Configure System** > **Design Forms**.Edit the profile JAR file.
   a) Log in to the system where the UNIX and Linux Adapter is installed.
   b) Copy the JAR file into a temporary directory.
   c) Extract the contents of the JAR file into the temporary directory. Run the following command. The following example applies to the Linux adapter profile.
   d) Type the name of the JAR file for your operating system.

   ```
   #cd /tmp
   #jar -xvf PosixLinuxProfile.jar
   ```

   The jar command extracts the files into the `PosixLinuxProfile` directory.
   e) Edit the `Service.xml` file for your respective profile. For example, `erPosixLinuxRMIService.xml` in the case of the Linux adapter.
   f) Add the attribute `erposixencoding` on the Service form for your respective profile See the following example:

   ```
   <formElement direction="inherit" label="$erposixencoding" name="data.erposixencoding">
                       <input type="text" name="data.erposixencoding"/>
                   </formElement>
   ```

   g) Save the changes.
2. Import the file.
   a) Create a JAR file by using the files in the /tmp directory Run the following command:

   ```
   #cd /tmp
   #jar -cvf PosixLinuxProfile.jar PosixLinuxProfile
   ```

   b) Import the JAR file into the Identity server.
   c) Stop and start the Identity server.
   d) Restart the adapter service.
3. Once the steps above are performed, `erPosixEncoding` attribute is visible on service form.
4. Create a service with following parameter on IBM Security Verify Governance:

   ```
   Code Page to be used for data encoding(Default to UTF-8) : Code page for data
   Code page for data on the service form is the corresponding code page to the
   LOCALE in use. For example, the code page for the German locale is
   ISO-8859-1.
   Code Page to be used for data encoding(Default to UTF-8) : ISO-8859-1
   ```

5. Click **Service** and select a POSIX Profile.
6. Add the attribute **erposixencoding** on the Service form from the **Attribute List**.
7. Save the form and close the **Design Form** window.

8. Create a service with following parameter:

   ```
   Code Page to be used for data encoding(Default to UTF-8) : Code page for data
   ```

   Code page for data on the service form is the corresponding code page to the LOCALE in use.

   For example, the code page for the German locale is ISO-8859-1.

   ```
   Code Page to be used for data encoding(Default to UTF-8) : ISO-8859-1
   ```

Configuring alternative adapter scripts location

You can specify where the adapter script files are stored on the managed UNIX or Linux system.

Before you begin

The administrator that is defined on the service form for the managed system must have sufficient permission to access the specified location or directory.

About this task

A configurable option, `erPosixCopyAdpFilesTo`, can be used to store adapter script files in a location other than the default location `/tmp`. This option is configurable by service and is not automatically displayed on the service form.

To add this attribute:

Procedure

1. Open the DESIGN FORMS feature of the Identity server. Click **Configure System** > **Design Forms**. Edit the profile JAR file.
   a) Log in to the system where the UNIX and Linux Adapter is installed.
   b) Copy the JAR file into a temporary directory.
   c) Extract the contents of the JAR file into the temporary directory. Run the following command. The following example applies to the Linux adapter profile.
   d) Type the name of the JAR file for your operating system.

   ```
   #cd /tmp
   #jar -xvf PosixLinuxProfile.jar
   ```

   The jar command extracts the files into the `PosixLinuxProfile` directory.
   e) Edit the `Service.xml` file for your respective profile. For example, `erPosixLinuxRMIService.xml` in the case of the Linux adapter.
   f) Add the attribute `erPosixCopyAdpFilesTo` on the Service form for your respective profile.

   ```

   <formElement direction="inherit" label="$erposixcopyadpfilesto"
   name="data.erposixcopyadpfilesto">
                       <input type="text" name="data.erposixcopyadpfilesto"/>
                   </formElement>
   ```

   g) Save the changes.
2. Import the file.
   a) Create a JAR file by using the files in the /tmp directory Run the following command:

   ```
   #cd /tmp
   #jar -cvf PosixLinuxProfile.jar PosixLinuxProfile
   ```

   b) Import the JAR file into the Identity server.
   c) Stop and start the Identity server.

   d) Restart the adapter service.
3. Once the steps above are performed, `erPosixCopyAdpFilesTo` attribute is visible on service form.
4. Create a service with following parameter:

   `Location of temporary files on resource : full path to file location`
5. Click **Service** and select any POSIX **Profile**.
6. Add the attribute `erPosixCopyAdpFilesTo` on the **Service** form from the **Attribute List**.
7. Save the form.
8. Create a service with following parameter:

   ```
   Location of temporary files on resource : full path to file location
   ```

Reconciling with custom scripts

You can run reconciliation with either the reconciliation script bundled with the adapter or your own customized reconciliation script that is optimized for your setup.

Before you begin

Ensure that these conditions are true:

- The customized reconciliation script name is user definable, and must be present in the *timsol* folder.
- You must have executable permission on reconciliation script. You must have similar permissions on the specified folder as on the `/tmp` folder.
- The reconciliation script and folder cannot contain double quotation marks or spaces.
- The names of the reconciliation script and folder must follow the naming conventions of the operating system.

About this task

To use this feature, select the **`Use recon script from this folder on managed resource`** attribute on the service form. The adapter uses the reconciliation script present at that location. If this option is not selected, then the standard reconciliation script that is bundled with the adapter is used.

Note:

1. If a value for both **`Location of temporary files on resource`** and **`Use recon script from this folder on managed resource`** are selected, then U**`se recon script from this folder on managed resource`** is used.
2. If a folder is specified on the managed resource without a script file name, the adapter looks for the standard reconciliation script name. The script name is based on the operating system type in the specified folder. On an AIX operating system, if the file path given for this attribute is `/reconfolder`, the adapter looks for the `/reconfolder/AixPConnRes.sh` file.

Procedure

1. Open the DESIGN FORMS feature of the Identity server. Click **Configure System** > **Design Forms**. Edit the profile JAR file.
   a) Log in to the system where the UNIX and Linux Adapter is installed.
   b) Copy the JAR file into a temporary directory.
   c) Extract the contents of the JAR file into the temporary directory. Run the following command. The following example applies to the Linux adapter profile.
   d) Type the name of the JAR file for your operating system.

   ```
   #cd /tmp
   #jar -xvf PosixLinuxProfile.jar
   ```

The jar command extracts the files into the `PosixLinuxProfile` directory.

e) Edit the `Service.xml` file for your respective profile. For example, `erPosixLinuxRMIService.xml` in the case of the Linux adapter.

f) Add the attribute `erPosixReconScriptLocation` on the Service form for your respective profile.

```
<formElement direction="inherit" label="$erposixreconscriptlocation"
name="data.erposixreconscriptlocation">
                    <input type="text" name="data.erposixreconscriptlocation"/>
                </formElement>
```

g) Save the changes.

2. Import the file.

a) Create a JAR file by using the files in the /tmp directory Run the following command:

```
#cd /tmp
#jar -cvf PosixLinuxProfile.jar PosixLinuxProfile
```

b) Import the JAR file into the Identity server.

c) Stop and start the Identity server.

d) Restart the adapter service.

3. Once the steps above are performed, `erPosixReconScriptLocation` attribute is visible on the service form.
4. Click **Service** and select **POSIX Solaris Profile**.
5. Add the attribute **`erPosixReconScriptLocation`** on the Service form from the Attribute List.
6. Save the form.

Ending a user session after suspension

The adapter can be configured to end active user sessions after the user is suspended.

About this task

The default behavior of the adapter is not to end active sessions after the user is suspended. Use this task to configure the adapter to end active sessions after the successful completion of a suspension request.

This option is configurable by service. The option is not displayed automatically on the Service Form.

Note:

1. This option must not be used on systems that allow duplicate user IDs.
2. An error condition or hang occurs if a user attempts to suspend itself when this option is set.

To add this attribute to the Service Form:

Procedure

1. Open the DESIGN FORMS feature of the Identity server. Click **Configure System** > **Design Forms**. Edit the profile JAR file.

a) Log in to the system where the UNIX and Linux Adapter is installed.

b) Copy the JAR file into a temporary directory.

c) Extract the contents of the JAR file into the temporary directory. Run the following command. The following example applies to the Linux adapter profile.

d) Type the name of the JAR file for your operating system.

```
#cd /tmp
#jar -xvf PosixLinuxProfile.jar
```

The jar command extracts the files into the `PosixLinuxProfile` directory.

    e) Edit the `Service.xml` file for your respective profile. For example, `erPosixLinuxRMIService.xml` in the case of the Linux adapter.

    f) Add the attribute `erPosixKillUserProcess` on the Service form for your respective profile with checkbox UI.

    ```
    <formElement name="data.erposixkilluserprocess" label="$erposixkilluserprocess">
                        <checkbox name="checkbox" value="false"/>
    </formElement>
    ```

    g) Save the changes.

2. Import the file.

    a) Create a JAR file by using the files in the /tmp directory Run the following command:

    ```
    #cd /tmp
    #jar -cvf PosixLinuxProfile.jar PosixLinuxProfile
    ```

    b) Import the JAR file into the Identity server.

    c) Stop and start the Identity server.

    d) Restart the adapter service.

3. Once the steps above are performed, `erPosixKillUserProcess` attribute is visible on service form.
4. Create a service with following parameter:

    `Kill active user process on suspending an account`
5. Click **Service** and select any **POSIX Solaris Profile**.
6. Add the attribute **`erPosixKillUserProcess`** on the Service form from the **Attribute List**.
7. Change display type to **CheckBox** and save the form.
8. Create a service with following parameter:

    ```
    Kill active user process on suspending an account
    ```
9. Restart the Dispatcher.

Ending user processes to delete a user account

On a Linux operating system, you cannot delete a user if any user processes are running. The adapter can be configured for Linux operating systems to end all user processes when a user is deleted.

About this task

The default behavior of the Linux operating system is to fail a user delete request if any user processes are running. Use this task to configure the adapter to end any active user processes when you submit a delete user request.

This option is configurable by service. The option is not displayed automatically on the Service Form.

Note: This option must not be used on systems that permit duplicate user IDs.

To add this attribute to the Service Form:

Procedure

1. Open the DESIGN FORMS feature of the Identity server. Click **Configure System** > **Design Forms**. Edit the profile JAR file.

    a) Log in to the system where the UNIX and Linux Adapter is installed.

    b) Copy the JAR file into a temporary directory.

    c) Extract the contents of the JAR file into the temporary directory. Run the following command. The following example applies to the Linux adapter profile.

    d) Type the name of the JAR file for your operating system.

```
#cd /tmp
#jar -xvf PosixLinuxProfile.jar
```

The jar command extracts the files into the `PosixLinuxProfile` directory.

e) Edit the `Service.xml` file for your respective profile. For example, `erPosixLinuxRMIService.xml` in the case of the Linux adapter.

f) Add the attribute **`erPosixDelUserInUse`** on the Service form for your respective profile.

```
<formElement name="data.erposixdeluserinuse" label="$erposixdeluserinuse">
                    <checkbox name="checkbox" value="false"/>
</formElement>
```

g) Save the changes.

2. Import the file.

   a) Create a JAR file by using the files in the /tmp directory Run the following command:

   ```
   #cd /tmp
   #jar -cvf PosixLinuxProfile.jar PosixLinuxProfile
   ```

   b) Import the JAR file into the Identity server.

   c) Stop and start the Identity server.

   d) Restart the adapter service.

   Once the steps above are performed, `erPosixDelUserInUse` attribute is visible on service form.
3. Click **Service** and select any **POSIX Linux Profile**.
4. Add the attribute **`erPosixDelUserInUse`** on the Service form from the **Attribute List**.
5. Change display type to **CheckBox** and save the form.
6. Create a service with following parameter:

   ```
   Delete user account even when it is in use
   ```
7. Restart the Dispatcher.

Non-login account (`passwd-N`) support

The adapter supports "No Password" accounts. A "No Password" account does not have a password. Accounts without passwords cannot be used to log in to the system interactively with commands such as **`login`**, **`telnet`**, **`ftp`**, or **`ssh`**.

The adapter supports "No Password" accounts on Solaris 10 and higher and HP-UX Trusted and Non-Trusted operating systems.

The **Is No Password Account?** check box on the account form is used to enable and disable the behavior. The possible values for this option are TRUE when selected and FALSE when not selected. When the option is selected, adapter creates a "No Password" account. The adapter creates a "Password" account when the option is not selected.

Note:

1. Password aging attributes for "No Password" accounts on HP-UX Trusted operating systems cannot be set.
2. When run from a sudo-super user account, HP-UX systems require these conditions.
   - `/usr/sam/lbin` and `/usr/bin` be in the user path.
   - `/usr/sam/lbin/usermod.sam` and `/usr/bin/test` be in the user entry in the `sudoers` file.

Attribute usage

The following examples demonstrate the usage of the attribute in various operations:

Add

A new user account can be requested with the **Is No Password Account?** option that is selected on the account form. In this case, the adapter creates a "No Password" account on Solaris 10 and higher and HP-UX Trusted and Non-Trusted operating systems.

Modify

When an account is modified with the option selected on the account form, the account is set to "No Password". When the option is not selected, the adapter sets the account to "Password". In this case, a password must also be provided.

Note: Changing an account from No Password to Password is not available through the UI. An error is returned: `Cannot change No Password Accounts to Password Accounts without password`

This modify operation can be done only through Workflows by providing a password along with a value of FALSE for **`erPosixNpAccount`**.

Password change

A change password request is valid for "Password" accounts only.

Suspend

The suspend operation for “No Password” accounts works similar to "Password" accounts.

Restore

Restore operation for “No Password” accounts is as follows:

- "No Password" accounts on Solaris 10 and HP-UX Trusted operating systems can be restored. However, a password cannot be set. If a password is supplied in the restore request, the `Can't set password for No Password Accounts` error is returned.
- After a “No Password” account is restored on HP-UX Non-Trusted systems, the resource requires a new password at the next user login. Because of HP-UX Non-Trusted resource behavior, the adapter is not able to distinguish a "Password" account from a “No Password” account on subsequent reconciliation requests. Therefore, use caution when you suspend and restore “No Password” accounts on HP-UX Non-Trusted systems.

Reconciliation

You can select "Is No Password Account?" on the account form. The adapter reconciles the value for the account as TRUE. If it is not selected, the adapter reconciles the value for the account as FALSE.

This table lists possible outcomes for "No Password" accounts during a modify operation when either:

- A password is provided.
- The value of the "Is No Password Account?" attribute is not sent in the request.

Table 12. No Password Account possible outcomes

		1	2	3	4	5	6	7	8
Password	Null					√	√	√	√
	Not null	√	√	√	√				
Np Account `1/TRUE`	Unchanged	√				√			
	Replace		√				√		
Np Account `0/False`	Unchanged			√				√	
	Replace				√				√
		It is already an Np Account	Request to make Np Account (that is from 0 to 1).	Not an Np account.	Request to make password Account from Np Account (that is from 1 to 0).	It is already an Np Account	Request to make Np Account (that is from 0 to 1).	Not an Np account.	Request to make password Account from Np Account (that is from 1 to 0).
		PASSWORD IS PRESENT				PASSWORD IS NOT PRESENT			

Table 12. No Password Account possible outcomes (continued)

		1	2	3	4	5	6	7	8
Work Flow		Fail the request as it is requesting for password change on NP Account.	Set as Np Account. Do not set the password.	Set Password for the account.	Set as Password account by setting the password.	Do other modify operations.	Set as Np Account.	Do other modify operations.	Cannot change to Password account without providing the password.
UI without the **Password** field		Fail the request as it is requesting for password change on NP Account.	N.A. The Password and Np Account value cannot come together.	Set Password for the account.	WARNING: Cannot set as password account. - No means to get the password here.	Do other modify operations.	Set as Np Account.	Do other modify operations.	

Password management for account restoration

When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account.

However, in some cases you might not want to be prompted for a password. The password requirement to restore an account falls into two categories: allowed and required.

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 Governance Identity ManagerIBM Security Verify GovernanceIBM Security Privileged Identity Manager to forego the new password requirement. You can set the adapter to require a new password if your company requires that passwords are reset when accounts are restored.

The adapter profile JAR file contains a `service.def` file. 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 enable remote services to determine whether you discard a password that the user entered while multiple accounts on disparate resources are being restored. In this scenario, only some of the accounts that are being restored might require a password. Remote services discard the password from the restore action for those managed resources that do not require them.

Edit the `<properties>...</properties>` section of the `service.def` file to add the new protocol options, for example:

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

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

Note: Before you set the property **`PASSWORD_NOT_REQUIRED_ON_RESTORE`** to `true`, ensure that the operating system supports restoring of an account without a password.

Related concepts

User home directory creation
The UNIX and Linux Adapter provides a user-selectable option to create a default home directory for a user or an account.

Customizing the adapter
The adapters can be customized or extended or both. The type and method of this customization varies depending on the adapter.

Customizing the adapter attributes

Depending on your needs, the adapter has attributes that you can optionally configure for the following capabilities.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must change the adapter profile JAR file. You might customize the adapter profile to change the account form or the service form. You can also change the labels on the forms by using the Form Designer or the `CustomLabels.properties` file. Each adapter has a `CustomLabels.properties` file.

Running user-defined scripts
The UNIX and Linux Adapter is configured to run user-defined scripts before a request is processed (preexec), after a request is processed (postexec), or both.

Defining the maximum connection count for adapter operations
You can limit the number of connections that can be made to a resource based on the service, service type, and operation. You can modify the `service.def` file in the service profile. Alternatively, you can specify a value for the **Max Connection Count** field on the service form of a resource.

Editing adapter profiles on the UNIX or Linux operating system
The adapter profile `.jar` file might contain ASCII files that are created by using the MS-DOS ASCII format.

Configuring self-password change
Configure self-password change with the AIX, Linux and Solaris profile jar files.

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 serverIdentity server.
2. Run a full reconciliation from the Identity serverIdentity 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

User home directory creation
The UNIX and Linux Adapter provides a user-selectable option to create a default home directory for a user or an account.

Customizing the adapter
The adapters can be customized or extended or both. The type and method of this customization varies depending on the adapter.

Customizing the adapter attributes
Depending on your needs, the adapter has attributes that you can optionally configure for the following capabilities.

Password management for account restoration
When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must change the adapter profile JAR file. You might customize the adapter profile to change the account form or the service form. You can also change the labels

on the forms by using the Form Designer or the `CustomLabels.properties` file. Each adapter has a `CustomLabels.properties` file.

Running user-defined scripts
The UNIX and Linux Adapter is configured to run user-defined scripts before a request is processed (preexec), after a request is processed (postexec), or both.

Defining the maximum connection count for adapter operations
You can limit the number of connections that can be made to a resource based on the service, service type, and operation. You can modify the `service.def` file in the service profile. Alternatively, you can specify a value for the **Max Connection Count** field on the service form of a resource.

Editing adapter profiles on the UNIX or Linux operating system
The adapter profile `.jar` file might contain ASCII files that are created by using the MS-DOS ASCII format.

Configuring self-password change
Configure self-password change with the AIX, Linux and Solaris profile jar files.

Chapter 7. Troubleshooting

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

Techniques for troubleshooting problems

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

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

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

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

What are the symptoms of the problem?

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

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

Where does the problem occur?

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

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

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

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

When does the problem occur?

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

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

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

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

Under which conditions does the problem occur?

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

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

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

Can the problem be reproduced?

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

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

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

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 13 on page 69 contains warnings or errors that might be displayed on the user interface if the adapter is installed on your workstation.

Table 13. Warning and error messages

Warning or error message	**Corrective action**
The following error occurred - *Error Description.*	IBM Security Verify Governance Identity ManagerIBM Security Verify GovernanceIBM Security Privileged Identity Manager cannot establish a connection with IBM Security Directory Integrator. To fix this problem, ensure that: • Security Directory Integrator is running • The URL specified on the service form for IBM Security Directory Integrator is correct
The login credential is missing or incorrect.	You must provide correct information for the adapter to function properly. To fix this problem, ensure that: • The managed resource is functioning properly and that you are connected to the correct resource • The Managed Resource Location that is specified on the service form is correct • The administrator ID specified on the service form is correct • The administrator password that is specified on the service form is correct • SSH is enabled and running on the managed resource
The account exists.	The user is already added to the resource. This error might occur if you are attempting to add a user to the managed resource and IBM Security Verify Governance Identity ManagerIBM Security Verify GovernanceIBM Security Privileged Identity Manager is not synchronized with the resource. To fix this problem, schedule a reconciliation between IBM Security Verify Governance Identity ManagerIBM Security Verify GovernanceIBM Security Privileged Identity Manager and the resource. See the online help for information about scheduling a reconciliation.
• The adapter does not have permission to add an account. • The adapter does not have permission to modify an account. • The adapter does not have permission to delete an account.	The administrator ID specified on the service form does not have permissions to add, modify, or delete the account. To fix this problem, do one of these steps: • Assign the correct privileges to the current administrator ID • Change the administrator ID to an administrator ID that has the correct privileges.
• The required attributes are missing from the request. • There were no attributes that were passed to the adapter in the request. • One or more required attributes are missing in the request.	One or more required attributes were not provided when you attempted to add, modify, delete, or search for a user. Type the required attributes for each field and try the action again.

Table 13. Warning and error messages (continued)

Warning or error message	**Corrective action**
• A system error occurred adding an account. The account was not added. • A system error occurred modifying an account. The account was not changed. • A system error occurred deleting an account. The account was not deleted. • The search failed because of a system error.	This error might occur for several reasons. To fix this problem, ensure that: • The administrator ID specified on the service form is correct. • The administrator password that is specified on the service form is correct. • The administrator ID has the correct privileges to add, modify, or delete a user account. • The network connection is not slow between IBM Security Verify Governance Identity ManagerIBM Security Verify GovernanceIBM Security Privileged Identity Manager and IDI or IDI and the managed resource.
`CTGIMT022E The search failed because of a system error: Error running script with Failed value:126`	Verify that the sudo user configuration file does not contain syntax errors.
• The account was added but some attributes failed. • The account was modified but some attributes failed. • The account was deleted successfully, but other steps failed.	The account was created, modified, or deleted, but some of the specified attributes in the request were not set. See the list of attributes that failed and the error message that explains why the attribute failed. Correct the errors that are associated with each attribute and try the action again. **Note:** Review the documentation for the operating system of the managed resource to determine the correct values for some attributes.
• The user cannot be modified because it does not exist. • An error occurred deleting the account because the account does not exist.	This error might occur when you attempt to modify or delete a user. This error might also occur if you attempt to change the password for a user. To fix the problem, ensure that: • The location that is specified for the managed resource is correct. • The user was created on the resource. • The user was not deleted from the resource. If the user does not exist on the resource, create the user on the resource and then schedule a reconciliation. See the online help for information about scheduling a reconciliation.
• Search filter error. • Invalid search filter.	The filter that is specified in the search request is not correct. Specify the correct filter and try the search action again.
The account is already suspended.	This error might occur if you attempt to suspend an account that was already suspended.

Table 13. Warning and error messages (continued)

Warning or error message	Corrective action
The account was not suspended.	The request failed to suspend the account. To fix this problem, ensure that: • The specified administrator ID is correct. • The specified administrator password is correct. • The administrator has the necessary privileges to suspend an account. • The user exists on the specified managed resource. See the `ibmdi.log` file in the solutions directory of the IBM Security Directory Integrator for specific details about the error.
The account is already restored.	This error might occur if you attempt to restore an account that was already restored.
The account was not restored.	The request failed to restore the account. To fix this problem, ensure that: • The specified administrator ID is correct. • The specified administrator password is correct. • The administrator has the necessary privileges to restore an account. • The user exists on the specified managed resource. See the `ibmdi.log` file in the solutions directory of the IBM Security Directory Integrator for specific details about the error.
The reconciliation is successful, but no accounts were added to your service.	• On the service form, check or clear the **Use a Shadow File** check box. • Check the IDI log to ensure that there is no mismatch for shadow file usage.
The application cannot establish a connection to *hostname*.	Ensure that SSH is enabled on the managed resource and that the managed resource is operational and attached to the network.
Attribute names are not displayed in the user interface.	For IBM Security Verify Governance Identity ManagerIBM Security Verify GovernanceIBM Security Privileged Identity Manager to refresh the list of attribute names, you must either: • Stop and restart the Identity server. • Wait until the cache times out (up to 10 minutes).
Adapter profile is not displayed in the user interface after you install the profile.	For Identity server to refresh the list of attribute names, you must either: • Stop and restart the Identity server. • Wait until the cache times out (up to 10 minutes).
The group cannot be added because it exists.	This error occurs when a request is made to add a group that exists. Create a group with another group name.

Table 13. Warning and error messages (continued)

Warning or error message	Corrective action
The group cannot be added because a group with the GID *Group ID number* exists.	This error occurs when a request is made to add a group with a group ID number that exists. Create a group with another group ID number.
The group *Group name* cannot be modified or deleted because it does not exist.	This error occurs when a request is made to modify or delete a group that does not exist on the managed resource. Do a reconciliation operation to ensure that the group exists on the managed resource.
An error occurred creating, modifying, or deleting the *Group name* group. The application cannot establish a connection to *managed resource*.	Ensure that these conditions are true. • The name in the **Administrator name** field on the service form is specified correctly. • The value of the Password attribute on the service form is specified correctly. • The managed resource is operational and connected to the network.
The IBM Security Directory Integrator detected the following error. Error: Connector parameter **`executeUserProfile`** has a value that is not valid: `true`.	Clear the **`Execute user profile?`** check box for the service that is used in the operation.
Sudo message: `sudo: sorry, you must have a tty to run sudo`	Comment out the line `Defaults requiretty` in the `sudouser` file.

Solving adapter installation and operational problems

You can obtain information that might be helpful in troubleshooting adapter installation and operational problems.

About this task

The term "adapter user name" is used throughout this procedure. The "adapter user name" is the UNIX account that is supplied on the IBM Security Verify Governance Identity ManagerIBM Security Verify GovernanceIBM Security Privileged Identity Manager service form for the administrator name. This account is the account that is used by the adapter to open a connection to the target workstation.

Note: The following steps are written for the AIX operating system and must be updated with correct commands for other UNIX or Linux operating systems.

Procedure

1. Set log level to Debug.

   See the *IBM Security Dispatcher Installation and Configuration Guide*. If possible, get only the log file with the failed request.
2. Get the software versions from the log files.

   Perform the following searches:

   Table 14. Search strings for software versions

Software	Log file search string
Dispatcher	RMIDispatcherImpl: Starting
Assembly line	UNIX/Linux Adapter AL version

Table 14. Search strings for software versions (continued)

Software	Log file search string
Posix connector	Loaded com.ibm.di.connector.osconnector.PosixConnector
RXA library	RXA Version

3. Get the operating system version.

   On an AIX workstation issue the commands:

   ```
   % instfix -i | grep AIX_ML
   % oslevel -q –s
   ```

4. Ensure that sh is the default shell for the adapter user name.
5. Ensure that OpenSSH is used. OpenSSH is the only supported ssh package. No other ssh vendors are supported. To get the OpenSSH version on an AIX workstation issue the command:

   ```
   $ ssh –V
   ```

   Note: This note pertains to AIX systems. Although other versions of OpenSSH function properly with this adapter, the AIX development team requires the installation of OpenSSH version 4.7 or later.
6. Ensure that OpenSSH version 4.7 or later is installed. Other versions of OpenSSH might function properly with this adapter, however if an issue is traced to OpenSSH, you might need to update your OpenSSH version to get support.
7. For OpenSSH configuration issues, do the following steps:

   a) Ensure that the **`UsePrivilegeSeparation`** attribute is set to `yes` in the `sshd_config` file.

      The default value of **`UsePrivilegeSeparation`** is `yes`. If set to no the adapter account is locked.

   b) Ensure that the **`ClientAliveInterval`** attribute in the `sshd_config` file is either commented out or set to `0`.

      The default value of **`ClientAliveInterval`** is `0`.
8. On a remote workstation, issue the following ssh commands and capture the results.

   ```
   % ssh username@ip-address "ssh -V"
   ```

   If sudo is used, issue these commands:

   ```
   % ssh username@ip-address "sudo ls /tmp"
   % ssh username@ip-address "which sudo"
   ```

   The *username* is the adapter user name. The *ip-address* is the IP address of the UNIX system that is being managed.
9. For reconciliation issues, do the following steps:

   a) Copy the AIXPConnRes.sh reconciliation file from the adapter solution directory to the AIX `/tmp` directory.

   b) Log in to the AIX system with the "adapter user name".

   c) Change the directory to the `/tmp` directory.

   d) Ensure that you have `execute` permission on the `AIXPConnRes.sh` file, `chmod 777 AIXPConnRes.sh`.

   e) Run the following command and save the `recon.out` file:

      ```
      AIXPConnRes.sh "grep -e :" true > recon.out 2>&1
      ```

For Linux systems, depending on the command that is specified on the service form for the **Command used to query failed logins** field, use one of these commands:

```
LinuxPConnRes.sh "grep -e :" true : "faillog -u %USER%"

LinuxPConnRes.sh "grep -e :" true : "faillock --user %USER%"

LinuxPConnRes.sh "grep -e :" true : "pam_tally2 --user %USER%"
```

If sudo is not used, replace the value true with false. False is the value for the root user.

All reconciliation files are in the adapter solution directory. The following table lists the names of the reconciliation files for various operating systems.

Table 15. Reconciliation file names

Platform	**Reconciliation file name**
AIX file system	AIXPConnRes.sh
HPUX not trusted	HPNTrustPConnRes.sh
HPUX trusted	HPTrustPConnRes.sh
Linux no shadow	LinuxPConnRes.sh
Linux with shadow	LinuxShadowPConnRes.sh
Solaris	SolarisPConnRes.sh

10. For sudo issues, do the following steps:
    a) Verify sudo setup per installation guide.

    See "Super user creation on a supported operating system" on page 94.

    b) Use the adapter user name to log in to the target system.

    c) Use sudo to do manual commands on the target system.
    For example,

    ```
    sudo mkuser test1
    sudo passwd test1
    sudo rmuser test1
    ```

11. For ssh issues, use **ssh** and **sudo** to do manual commands on the target system.
    For example, log in to a system that has connectivity to the target system and issue the commands:

    For sudo users

    ```
    ssh user@target "sudo mkuser test1"
    ssh user@target "sudo passwd test1"
    ssh user@target "sudo rmuser test1"
    ```

    For nonsudo users

    ```
    ssh user@target "mkuser test1"
    ssh user@target "passwd test1"
    ssh user@target "rmuser test1"
    ```

Known adapter issues

You can use information about permissions, passwords, and other data to correct known issues with the adapter.

/tmp directory permissions

The permissions for the /tmp directory on the managed resource must be set to 777 to do the reconciliation operation by using the sudo user.

Related concepts

Home directory permissions
The adapter requires home directory permissions that are set to 755 to set the umask value.

HP-UX password age issues
The password age attributes have certain restrictions for HP-UX Trusted and Non-Trusted systems.

No support for adding the primary group of a user to the secondary groupset of the user
SUSE Linux and Solaris operating systems do not support adding the primary group of a user to the secondary groupset of the user.

No support for accessing the endpoint as a user with sudo log_output enabled
The adapter is unable to connect to the endpoint if the `Defaults log_output` is defined, or if `log_output` is defined for the adapter user ID in sudoers.

Home directory permissions

The adapter requires home directory permissions that are set to 755 to set the umask value.

The sudo user must have permissions on the home directory of the user whose umask value is added or changed. Otherwise, the adapter might not work as expected

Related concepts

/tmp directory permissions
The permissions for the /tmp directory on the managed resource must be set to 777 to do the reconciliation operation by using the sudo user.

HP-UX password age issues
The password age attributes have certain restrictions for HP-UX Trusted and Non-Trusted systems.

No support for adding the primary group of a user to the secondary groupset of the user
SUSE Linux and Solaris operating systems do not support adding the primary group of a user to the secondary groupset of the user.

No support for accessing the endpoint as a user with sudo log_output enabled
The adapter is unable to connect to the endpoint if the `Defaults log_output` is defined, or if `log_output` is defined for the adapter user ID in sudoers.

HP-UX password age issues

The password age attributes have certain restrictions for HP-UX Trusted and Non-Trusted systems.

The HP-UX Non-Trusted operating system sets password **MAX_AGE** and **MIN_AGE** to -1 during account creation if no values are supplied. However, on a modify operation, the operating system does not allow -1 for password **MIN_AGE**. The adapter account form is modified with a constraint on password **MIN_AGE** that prevents the user from entering a value less than 0.

The HP-UX Trusted operating system sets password **MAX_AGE** and **MIN_AGE** to 0 during account creation if no values are supplied. The operating system does not allow -1 for password **MIN_AGE** and **MAX_AGE**. The adapter account form is modified with a constraint on password **MIN_AGE** that prevents the user from entering a value less than 0. No constraint exists on password **MAX_AGE** because it can be -1 for HP-UX_Non-Trusted operating systems.

The following attributes cannot be managed on HP-UX Non-Trusted systems:

password warning age

maximum number of days the account can remain valid after the password expires For AIX systems the duration is specified in weeks.

number of days the account can remain idle

allowed number of login retries before locking the account

account expiration date

Related concepts

/tmp directory permissions
The permissions for the `/tmp` directory on the managed resource must be set to 777 to do the reconciliation operation by using the sudo user.

Home directory permissions
The adapter requires home directory permissions that are set to 755 to set the umask value.

No support for adding the primary group of a user to the secondary groupset of the user
SUSE Linux and Solaris operating systems do not support adding the primary group of a user to the secondary groupset of the user.

No support for accessing the endpoint as a user with sudo log_output enabled
The adapter is unable to connect to the endpoint if the `Defaults log_output` is defined, or if `log_output` is defined for the adapter user ID in sudoers.

No support for adding the primary group of a user to the secondary groupset of the user

SUSE Linux and Solaris operating systems do not support adding the primary group of a user to the secondary groupset of the user.

The UNIX and Linux Adapter cannot support a function that is not supported by the operating system. If you attempt to add the primary group to the secondary groupset of the user, the operation fails on SUSE Linux and Solaris systems. Although the primary group is not added, no error message is returned. The command that is used for this function does not generate an error message.

Related concepts

/tmp directory permissions
The permissions for the `/tmp` directory on the managed resource must be set to 777 to do the reconciliation operation by using the sudo user.

Home directory permissions
The adapter requires home directory permissions that are set to 755 to set the umask value.

HP-UX password age issues
The password age attributes have certain restrictions for HP-UX Trusted and Non-Trusted systems.

No support for accessing the endpoint as a user with sudo log_output enabled
The adapter is unable to connect to the endpoint if the `Defaults log_output` is defined, or if `log_output` is defined for the adapter user ID in sudoers.

No support for accessing the endpoint as a user with sudo `log_output` enabled

The adapter is unable to connect to the endpoint if the `Defaults log_output` is defined, or if `log_output` is defined for the adapter user ID in sudoers.

Defining `log_output` for the adapter user ID in sudoers causes the creation of a pseudo-TTY that is used for command output redirection. The pseudo-TTY interacts poorly with the SSH session opened by the adapter and causes the SSH server to close the connection after a single command is run.

To prevent this issue, do any of following workarounds:

- Use root user to connect to the resource.

- Change the Defaults line as follows:

```
Defaults: !tdiuser log_output
```

- Define the adapter user to not capture log output:

```
tdiuser ALL=NOLOG_OUTPUT: NOPASSWD:list_of_commands...
```

Related concepts

/tmp directory permissions
The permissions for the `/tmp` directory on the managed resource must be set to 777 to do the reconciliation operation by using the sudo user.

Home directory permissions
The adapter requires home directory permissions that are set to 755 to set the umask value.

HP-UX password age issues
The password age attributes have certain restrictions for HP-UX Trusted and Non-Trusted systems.

No support for adding the primary group of a user to the secondary groupset of the user
SUSE Linux and Solaris operating systems do not support adding the primary group of a user to the secondary groupset of the user.

Chapter 8. Uninstalling

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

Uninstalling the adapter

When the adapter is installed, the JAR file that is required for uninstalling the adapter is created in the `ITDI_HOME/PosixAdapterUninstall` directory.

Procedure

1. Stop the adapter service.

   See Start, stop, and restart the adapter service.
2. Run the `PosixAdapterUninstall.jar` file from `PosixAdapterUninstall` directory.

   If you run the command from a different directory, you must specify the full file path to the `uninstaller.jar` file.

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

Deleting the adapter profile

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

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

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

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

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

Chapter 9. Reference

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

Adapter attributes and object classes

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

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

Table 16. Account form attributes, descriptions, permissions, and applicable operating systems

Attribute	Description	Permissions	Operating systems
erUid	Specifies the login name and user name.	Read and Write	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
erPosixUid	Specifies the user ID.	Read and Write	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
erPosixDupUid	Specifies that a non-unique ID can be assigned to the user.	Write	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
erPosixSudoersPath	Specifies the path to the sudoers file on the resource.	Write	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris

Table 16. Account form attributes, descriptions, permissions, and applicable operating systems (continued)

Attribute	Description	Permissions	Operating systems
erPosixSudoPrivileges	Specifies the sudo privileges for the user or group that is associated with the account.	Read	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
erPosixReturnSudoPrivileges	Specifies whether to return sudo privileges during account reconciliation.	Write	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
erPassword	Specifies the password for the account.	Read and Write	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
erPosixForcePwdChange	Specifies whether the user is required to change the login password upon next login.	Read and Write	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
erPosixMaxPwdAge	Specifies the maximum age for a password.	Read and Write	AIX Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
erPosixMinPwdAge	Specifies the minimum age for a password.	Read and Write	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris

Table 16. Account form attributes, descriptions, permissions, and applicable operating systems (continued)

Attribute	Description	Permissions	Operating systems
`erPosixPwdMaxRepeats`	Specifies the maximum repeated characters that are allowed in a password.	Read and Write	AIX Linux Shadow HP-UX-Trusted Solaris
`erPosixPwdWarnAge`	Specifies the age of a password before a message that warns the user about password expiration is sent.	Read and Write	AIX Linux Shadow HP-UX-Trusted Solaris
`erPosixPwdLastChange`	Specifies the date on which a password was last changed.	Read	Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
`erPosixExpireDate`	Specifies the date on which the account expires.	Read and Write	AIX Linux Shadow HP-UX-Nontrusted Solaris
`erPosixIdleDays`	Specifies the number of days the account can remain idle before the account is suspended.	Read and Write	HP-UX-Trusted Solaris
`erPosixGecos`	Specifies a descriptive comment for the user account. **Note:** The back quotation mark character (`) is not allowed.	Read and Write	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
`erPosixPrimaryGroup`	Specifies the primary group for the user.	Read and Write	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris

Table 16. Account form attributes, descriptions, permissions, and applicable operating systems (continued)

Attribute	Description	Permissions	Operating systems
`erPosixSecondGroup`	Specifies the secondary groups for the user.	Read and Write	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
`erPosixHomeDir`	Specifies the home directory for the user **Note:** The back quotation mark character (`) and the semicolon (;) are not allowed.	Read and Write	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
`erPosixDefaultHomeDir`	Specifies to create a home directory while the account is created. This attribute does not apply to RHEL.	Read and Write	Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
`erPosixNPAaccount`	Specifies that the account has no password.	Read and Write	HP-UX-Trusted HP-UX-Nontrusted Solaris
`erPosixPerHomeDir`	Specifies the permissions for the home directory.	Read and Write	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
`erPosixShell`	Specifies the login shell of the user. The default account shell in the picklist is changed from `/bin/csh to /bin/sh` on the account form. Any accounts created using the adapter will have the `/bin/sh` shell unless a different shell is explicitly selected.	Read and Write	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris

Table 16. Account form attributes, descriptions, permissions, and applicable operating systems (continued)

Attribute	Description	Permissions	Operating systems
erPosixUmask	Specifies the umask.	Read and Write	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
erPosixLastAccessDate	Specifies the date on which the account was last accessed.	Read	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
erPosixAT	Specifies whether AT jobs are allowed.	Read and Write	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
erPosixCron	Specifies whether CRON jobs are allowed.	Read and Write	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
erPosixPwdMaxAge	Specifies the maximum amount of time that a password can be changed after the maximum password age.	Read and Write	AIX Linux Shadow HP-UX-Trusted
erPosixKillUserProcess	Specifies whether to end the user sessions when a suspend user request is processed.	Write	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris

Table 16. Account form attributes, descriptions, permissions, and applicable operating systems (continued)

Attribute	Description	Permissions	Operating systems
erPosixCopyAdpFilesTo	Specifies an alternative directory location to store the adapter scripts. The default location is /tmp.	Write	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
erPosixPreExec	Specifies a user-defined command to run before a resource request.	Write	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
erPosixPreExecRunOption	Specifies to run a resource request only if a pre-exec command succeeds.	Write	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
erPosixPostExec	Specifies a user-defined command to run after a resource request.	Write	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
erPosixPostExecRunOption	Specifies to run a user-defined post-exec command only if the resource command succeeds.	Write	AIX Linux NonShadow Linux Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
erPosixAdminUser	Specifies whether the password belongs to an administrator.	Read and Write	AIX
erPosixAuth1	Specifies the primary authorization methods for a user.	Read and Write	AIX

Table 16. Account form attributes, descriptions, permissions, and applicable operating systems (continued)

Attribute	Description	Permissions	Operating systems
erPosixAuth2	Specifies the secondary authorization methods for a user.	Read and Write	AIX
erPosixDaemonAllowed	Specifies whether the user is allowed to run daemon processes.	Read and Write	AIX
erPosixLoginRetries	Specifies the maximum number of unsuccessful logins that are allowed before the account is locked.	Read and Write	AIX Suse Linux HP-UX-Trusted HP-UX-Nontrusted Solaris
erPosixSuGroup	Specifies the groups whose members can use the **su** command to switch to this user.	Read and Write	AIX
erPosixAdmGroups	Specifies the groups for which the user is an administrator.	Read and Write	AIX
erPosixRoles	Specifies the roles that the user is assigned.	Read and Write	AIX
erPosixSuAllowed	Specifies whether another user can switch to this user with the **su** command.	Read and Write	AIX
erPosixRLoginAllowed	Specifies whether the user is allowed to log in remotely with the **telnet** or **rlogin** commands.	Read and Write	AIX
erPosixLoginAllowed	Specifies whether the user is allowed to log in to the system with the **login** command.	Read and Write	AIX
erAccountStatus	Specifies the status of the account. See "Account status determination on AIX" on page 93.	Read and Write	AIX
erPosixAuditClasses	Specifies the list of audit classes for a user.	Read and Write	AIX
erPosixSoftCore	Specifies the soft limit, any value less than the maximum, for the largest core file a user process can create.	Read and Write	AIX

Table 16. Account form attributes, descriptions, permissions, and applicable operating systems (continued)

Attribute	Description	Permissions	Operating systems
erPosixHardCore	Specifies the largest core file a user process can create.	Read and Write	AIX
erPosixSoftCPU	Specifies the soft limit, any value less than the maximum, for the largest amount of system unit time a user process can use. The time is specified in seconds.	Read and Write	AIX
erPosixHardCPU	Specifies the largest amount of system unit time a user process can use. The time is specified in seconds.	Read and Write	AIX
erPosixSoftData	Specifies the soft limit, any value less than the maximum, for the largest data segment that a user process can contain.	Read and Write	AIX
erPosixHardData	Specifies the limit for the largest data segment that a user process can contain.	Read and Write	AIX
erPosixSoftFileSize	Specifies the soft limit, any value less than the maximum, for the largest file a user process can create.	Read and Write	AIX
erPosixHardFileSize	Specifies the limit for the largest file a user process can create.	Read and Write	AIX
erPosixLoginTimes	Specifies the days and times a user is allowed to log in.	Read and Write	AIX
erPosixSoftStack	Specifies the soft limit, any value less than the maximum, for the largest stack segment for a user process.	Read and Write	AIX
erPosixHardStack	Specifies the limit for the largest stack segment for a user process.	Read and Write	AIX
erPosixTrustedPath	Specifies the trusted path status of the user.	Read and Write	AIX
erPosixAuthGrammar	Specifies the user authentication method.	Read and Write	AIX

Table 16. Account form attributes, descriptions, permissions, and applicable operating systems (continued)

Attribute	Description	Permissions	Operating systems
erPosixPwdMinAlphaChar	Specifies the minimum number of alphabetic characters in a password.	Read and Write	AIX
erPosixPwdMinOtherChar	Specifies the minimum number of non-alphabetic characters in a password.	Read and Write	AIX
erPosixPwdMinDiff	Specifies the minimum difference in characters that are allowed between passwords.	Read and Write	AIX
erPosixPwdMinLen	Specifies the minimum length for a password.	Read and Write	AIX
erPosixPwdCheck	Specifies whether to check the password in a dictionary.	Read and Write	AIX
erPosixPwdDiction	Specifies the dictionary files to check for the password.	Read and Write	AIX
erPosixPwdHistory	Specifies the number of passwords to be remembered before reuse.	Read and Write	AIX
erPosixPwdHistoryExpire	Specifies the number of weeks that must pass before the password history is erased.	Read and Write	AIX
erPosixValidTtys	Specifies the terminal types through which the user can log in.	Read and Write	AIX
erPosixRegistry	Specifies the registry to be used for authentication.	Read and Write	AIX
erPosixSoftRss	Specifies the soft limit, any value less than the maximum, for the largest amount of physical memory that can be allocated by a user process. This limit is not enforced by the system.	Read and Write	AIX
erPosixHardRss	Specifies the largest amount of physical memory that can be allocated by a user process. This limit is not enforced by the system.	Read and Write	AIX

Table 16. Account form attributes, descriptions, permissions, and applicable operating systems (continued)

Attribute	Description	Permissions	Operating systems
erPosixSoftNoFiles	Specifies the soft limit, any value less than the maximum, for the number of file descriptors a user process can have open at one time.	Read and Write	AIX
erPosixHardNoFiles	Specifies the maximum number of file descriptors a user process can have open at one time.	Read and Write	AIX
erPosixHostsAllowedLogin	Specifies the workstations to which a user can log in.	Read and Write	AIX
erPosixerPosixHostsDeniedLogin	Specifies the workstations to which a user cannot log in.	Read and Write	AIX
erPosixDelUserInUse	Specifies whether to end the user processes when a delete account request is processed.	Read and Write	Linux NonShadow Linux Shadow

Group form attributes

The Identity server communicates with the adapter for group management by using specific attributes.

Table 17 on page 90 lists the attributes that are used by the adapter. The table also gives the permissions that are needed for the attribute.

Table 17. Group form attributes

Attribute name on the UNIX and Linux operating systems group form on IBM Security Verify Governance Identity Manager	Permissions	Supported operating system			
		AIX	HP-UX	Linux	Solaris
Group name	Read and Write	√	√	√	√
Group ID number	Read and Write	√	√	√	√
Administrator group	Read and Write	√			
Group administrators	Read and Write	√			
Group projects	Read and Write	√			
Allow duplicate group IDs	Write		√	√	√
Sudo privileges	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.

System Login Add

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

Table 18. Add request attributes for AIX, HPUX, Linux, and Solaris

Required attribute	Optional attribute
erUid	All other supported attributes

System Login Change

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

Table 19. Change request attributes for AIX, HPUX, Linux, and Solaris

Required attribute	Optional attribute
erUid	All other supported attributes

System Login Delete

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

Table 20. Delete request attributes for AIX and Solaris

Required attribute	Optional attribute
erUid	erPosixHomeDirRemove

Table 21. Delete request attributes for HPUX and Linux

Required attribute	Optional attribute
erUid	erPosixHomeDirRemove erPosixUseShadow

System Login Suspend

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

Table 22. Suspend request attributes for AIX and Solaris

Required attribute	Optional attribute
erUid erAccountStatus	erPosixHomeDirRemove erPosixKillUserProcess

Table 23. Suspend request attributes for HP-UX and Linux

Required attribute	Optional attribute
erUid erAccountStatus	erPosixHomeDirRemove erPosixUseShadow erPosixKillUserProcess

System Login Restore

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

Table 24. Restore request attributes for AIX

Required attribute	Optional attribute
erUid erAccountStatus	erPosixHomeDirRemove

Table 25. Restore request attributes for Solaris

Required attribute	Optional attribute
erUid erAccountStatus erPassword	erPosixHomeDirRemove

Test

No attributes are needed to test the connection to the managed resource.

The following table identifies attributes that are needed to test the connection.

Table 26. Test attributes

Required attribute	Optional attribute
None	None

Reconciliation

The Reconciliation request synchronizes user account information between IBM Security Verify Governance Identity ManagerIBM Security Verify GovernanceIBM Security Privileged Identity Manager and the managed resource.

Table 27. Reconciliation request attributes for AIX and Solaris

Required attribute	Optional attribute
None	erPosixHomeDirRemove erPosixSudoersPath erPosixReturnSudoPrivileges

Table 28. Reconciliation request attributes for HP-UX and Linux

Required attribute	Optional attribute
None	erPosixHomeDirRemove erPosixUseShadow erPosixSudoersPath erPosixReturnSudoPrivileges

Group add

Group add is a request to create a group with the specified attribute.

Group add is a request to create a group with the specified attribute.

Table 29. Group add request attribute for AIX, HPUX, Linux, and Solaris

Required attribute	Optional attribute
erPosixGroupName	All other supported attributes

Group change

Group change is a request to modify group attributes with the specified attribute.

Table 30. Group change request attribute for AIX, HPUX, Linux, and Solaris

Required attribute	Optional attribute
erPosixGroupName	All other supported attributes

Group delete

Group delete is a request to delete a group with the required **erPosixGroupName** attribute on the account form of the AIX, HPUX, Linux, and Solaris operating systems.

Account status determination on AIX

Use the following information to understand how the adapter determines an account status on AIX systems.

On AIX systems, to determine the account status values such as active account or inactive account, the adapter performs both of the following tests.

- Checks the `account_locked` attribute.
- Checks the condition `unsuccessful_login_count >= loginretries`.

If either of these tests return `true`, the account is marked as an inactive account.

Special attributes

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

Super user creation on a supported operating system

You can specify a super user instead of a root user to do administration tasks. To create a super user, follow the directions that are specified for your operating system.

Creating a super user on an AIX operating system

You can create a user with required permissions to run the adapter correctly on a workstation that uses an AIX operating system.

About this task

In this task, the user is "tdiuser".

Procedure

1. Create a user.

   a) Issue the command:

   ```
   mkuser home="/home/tdiuser" shell="/usr/bin/ksh" tdiuser
   ```

   b) Set the following statement in the user PATH environment variable:

   ```
   PATH=/usr/bin:/etc:/usr/sbin:/usr/ucb:$HOME/bin:/usr/bin/X11:/sbin:
   /usr/local/bin
   ```

   The following commands must be in the user path:

   `mv`, **`tee`**, **`cp`**, **`kill`**, **`chsec`**, **`mkdir`**, **`rm`**, **`sudo`**

   If the super user is used to log in and run commands, then '.' can be added to the PATH environment variable.

2. Grant sudo permissions to the user for AIX commands.

   Note: By default, the **sudo** command requires user authentication before it runs a command. To modify this behavior, add the NOPASSWD tag to the sudoers file entry.

   a) Open the `sudoers` file.

   Issue the following command:

   ```
   bash-2.05b$ visudo
   ```

   b) If the line `Defaults requiretty` exists in the file, comment it out.

   ```
   #Defaults requiretty
   ```

   c) Insert the following lines to allow sudo access.

   The entry beginning with `tdiuser` must be entered on a single line. It is displayed here as multiple lines for readability.

   ```
   # User privilege specification
   tdiuser ALL=NOPASSWD:/usr/bin/pwdadm,/usr/bin/passwd,/usr/bin/mkuser,
   /usr/sbin/rmuser,/usr/bin/chuser,/usr/bin/chmod,/usr/bin/cat,
   /usr/bin/rm,/usr/bin/tee,/usr/bin/ed,/usr/bin/groups,/usr/bin/ls,
   /usr/bin/logins,/usr/sbin/lsuser,/usr/bin/mv,/usr/sbin/lsgroup,
   /usr/bin/chpasswd,/usr/bin/chsec,/usr/sbin/usermod,/usr/sbin/lsrole,
   /usr/bin/mkgroup,/usr/sbin/rmgroup,/usr/bin/chgroup,/usr/bin/mkrole,
   /usr/sbin/rmrole,/usr/bin/chrole,/usr/bin/mkdir,/usr/bin/rm,
   /usr/bin/kill,/usr/bin/hostname
   ```

   The following commands are used by the connector but are not needed in the sudoers file. However, if the sudo user is used, the user needs execute permissions on these commands.

```
/usr/bin/tr, /usr/bin/cut, /usr/bin/egrep, /usr/bin/awk,
/usr/bin/sort, /usr/bin/ps, /usr/bin/sed
```

Note: The UNIX and Linux Adapter does not support accessing the endpoint as a user with sudo `log_output` enabled.

d) Validate the format of the `/etc/sudoers` file

Issue the command:

```
visudo -c
```

If syntax is wrong the command prompts an error message, for example:

```
$ visudo -c
        >>> sudoers file: syntax error, line 30 <<<
        parse error in /etc/sudoers near line 30
```

Note: The sudo access command paths that are listed here are an example. The actual command paths vary depending upon the resource. Ensure that the correct path is specified in the `sudoers` file.

3. Set the password for the newly created user.

   Issue the command:

```
bash-2.05b$passwd tdiuser
```

Creating a super user on a Linux operating system

You can create a user with required permissions to run the adapter correctly on a workstation that uses a Linux operating system.

About this task

The adapter supports both SUSE and RHEL. In this example, the user is "tdiuser".

Procedure

1. Create a user with security group permission.

   a) Issue the command:

```
useradd –d "/home/tdiuser" –s "/bin/bash" –m tdiuser
```

   b) Set the following statement in the user PATH environment variable:

```
PATH=/usr/bin:/usr/sbin:/etc:
```

   The following commands must be in the user path:

   `mv`, **`tee`**, **`cp`**, **`kill`**, **`mkdir`**, **`rm`**, **`faillog`**, **`faillock`**, **`pam_tally2`**, **`grep`**, **`lastlog`**, **`sudo`**

   Note: For SLES 11 and higher, the **`faillog`** command full path is `/usr/sbin/faillog`.

   If the super user is used to log in and run commands, then '.' can be added to the PATH environment variable.

2. Grant sudo permissions to the user for all commands.

   Note: By default, the **sudo** command requires user authentication before it runs a command. To modify this behavior, add the NOPASSWD tag to the sudoers file entry.

   a) Open the sudoers file.

   Issue the following command:

```
bash-2.05b$ visudo
```

b) If the line `Defaults requiretty` exists in the file, comment it out.

```
#Defaults requiretty
```

c) Insert the following lines to allow sudo access.

The entry beginning with `tdiuser` must be entered on a single line. It is displayed here as multiple lines for readability.

Modify the command paths to match your operating system. Update the user path if necessary.

```
# User privilege specification
tdiuser ALL=NOPASSWD:/usr/bin/passwd,/usr/sbin/useradd,
/usr/sbin/usermod,/usr/sbin/userdel,/usr/bin/tee,/bin/chmod,
/bin/cat,/bin/ls,/usr/bin/chage,/usr/bin/groups,/bin/ed,
/bin/cp,/usr/bin/faillog,/usr/sbin/groupadd,/usr/sbin/groupmod,
/usr/sbin/groupdel,/usr/bin/kill,/bin/hostname,/sbin/faillock,
/sbin/pam_tally2,/bin/mkdir,/bin/rm,/usr/bin/lastlog
```

The following commands are used by the connector but are not needed in the sudoers file. However, if the sudo user is used, the user needs execute permissions on these commands:

```
tr, cut, awk, sed, sort, grep, ps
```

Note: The UNIX and Linux Adapter does not support accessing the endpoint as a user with sudo `log_output` enabled.

d) Validate the format of the `/etc/sudoers` file

Issue the command:

```
visudo -c
```

If syntax is wrong the command prompts an error message, for example:

```
$ visudo -c
        >>> sudoers file: syntax error, line 30 <<<
        parse error in /etc/sudoers near line 30
```

Note: The sudo access command paths that are listed here are an example. The actual command paths vary depending upon the resource. Ensure that the correct path is specified in the `sudoers` file.

For example, the complete path of **ed** command is `/bin/ed` for RHEL systems, `/usr/bin/ed` for SUSE systems and `/bin/ed` for Debian systems.

3. Set the password for the newly created user.

   Issue the command:

```
bash-2.05b$passwd tdiuser
```

Creating a super user on a Solaris operating system

You can create a user with the required permissions to run the adapter correctly on a workstation that uses a Solaris operating system.

About this task

In this example, the user is "tdiuser".

Procedure

1. Create a user and specify the home directory.

   a) Issue the command:

```
useradd –d "/home/tdiuser" –s "/sbin/sh" –m tdiuser
```

b) Ensure that the `/home/tdiuser/.profile` file exists. If not, you must create the `.profile` file.

c) Set the following statement in the user PATH environment variable:

```
PATH=/usr/bin:/etc:/usr/local/sbin:/usr/local/bin
```

The following commands must also be in the user path:

mv, **tee**, **cp**, **kill**, **mkdir**, **rm**, **sudo**

If the super user is used to log in and run commands, then '.' can be added to the PATH environment variable.

2. Grant sudo permissions to the user for all commands.

Note: By default, the **sudo** command requires user authentication before it runs a command. To modify this behavior, add the NOPASSWD tag to the sudoers file entry.

a) Open the sudoers file.

Issue the following command:

```
bash-2.05b$ visudo
```

b) If the line `Defaults requiretty` exists in the file, comment it out.

```
#Defaults requiretty
```

c) Insert the following lines to allow sudo access.

The entry beginning with `tdiuser` must be entered on a single line. It is displayed here as multiple lines for readability.

```
# User privilege specification
tdiuser ALL=NOPASSWD:/usr/bin/passwd,/usr/sbin/useradd,
/usr/sbin/usermod,/usr/sbin/userdel,/usr/bin/tee,/usr/bin/chmod,
/usr/bin/cat,/usr/bin/logins,/usr/bin/ls,/usr/bin/ed,/usr/bin/cp,
/usr/sbin/groupadd,/usr/sbin/groupmod,/usr/sbin/groupdel,
/usr/bin/mkdir,/usr/bin/rm,/usr/bin/kill,/usr/bin/hostname
```

The following commands are used by the connector but are not needed in the sudoers file. However, if the sudo user is used, the user needs execute permissions on these commands.

```
/usr/bin/tr, /usr/bin/cut, /usr/bin/egrep, /usr/bin/awk,
/usr/bin/sort, /usr/bin/ps, /usr/bin/sed
```

Note: The UNIX and Linux Adapter does not support accessing the endpoint as a user with sudo `log_output` enabled.

d) Validate the format of the `/etc/sudoers` file

Issue the command:

```
visudo -c
```

If syntax is wrong the command prompts an error message, for example:

```
$ visudo -c
        >>> sudoers file: syntax error, line 30 <<<
        parse error in /etc/sudoers near line 30
```

Note: The sudo access command paths that are listed here are an example. The actual command paths vary depending upon the resource. Ensure that the correct path is specified in the `sudoers` file.

3. Set the password for the newly created user.

Issue the command:

```
bash-2.05b$passwd tdiuser
```

Creating a super user on an HP-UX Non-Trusted operating system

You can create a user with required permissions to run the adapter correctly on a workstation that uses an HP-UX Non-Trusted operating system.

About this task

In this example, the user is "tdiuser".

Procedure

1. Create a user and specify the home directory.

   a) Issue the command:

   ```
   useradd -d "/home/tdiuser" -s "/sbin/sh" -m tdiuser
   ```

   b) Ensure that the `/home/tdiuser/.profile` file exists. If not, you must create the `.profile` file.

   c) Set the following statement in the user PATH environment variable:

   ```
   PATH=/usr/bin:/usr/sbin:/etc:/usr/local/bin:/usr/sam/lbin:/usr/sbin/acct:
   ```

   The following commands must be in the user path:

   `mv`, **`tee`**, **`cp`**, **`kill`**, **`usermod.sam`**, **`mkdir`**, **`rm`**, **`fwtmp`**, **sudo**

   If the super user is used to log in and run commands, then '.' can be added to the PATH environment variable.

2. Grant sudo permissions to the user for all commands.

   Note: By default, the **sudo** command requires user authentication before it runs a command. To modify this behavior, add the NOPASSWD tag to the sudoers file entry.

   a) Open the sudoers file.

   Issue the following command:

   ```
   bash-2.05b$ visudo
   ```

   b) If the line `Defaults requiretty` exists in the file, comment it out.

   ```
   #Defaults requiretty
   ```

   c) Insert the following lines to allow sudo access.

   The entry beginning with `tdiuser` must be entered on a single line. It is displayed here as multiple lines for readability.

   ```
   # User privilege specification
   tdiuser ALL=NOPASSWD:/usr/bin/chmod,/usr/bin/cat,/usr/sbin/logins,
   /usr/bin/ls,/usr/bin/passwd,/usr/sbin/useradd,/usr/sbin/usermod,
   /usr/sbin/userdel,/usr/bin/tee,/usr/bin/ed,/usr/sbin/groupadd,
   /usr/sbin/groupdel,/usr/sbin/groupmod,/usr/bin/cp,/usr/bin/mkdir,
   /usr/bin/rm,/usr/bin/kill,/usr/bin/hostname,/usr/sbin/acct/fwtmp,
   /usr/bin/test
   ```

   The following commands are used by the connector but are not needed in the sudoers file. However, if the sudo user is used, the user needs execute permissions on these commands.

   ```
   /usr/bin/tr, /usr/bin/cut, /usr/bin/egrep, /usr/bin/awk,
   /usr/bin/head, /usr/bin/sort, /usr/bin/ps, /usr/bin/sed
   ```

   Note: The UNIX and Linux Adapter does not support accessing the endpoint as a user with sudo `log_output` enabled.

   d) Validate the format of the `/etc/sudoers` file

   Issue the command:

```
visudo -c
```

If syntax is wrong the command prompts an error message, for example:

```
$ visudo -c
        >>> sudoers file: syntax error, line 30 <<<
        parse error in /etc/sudoers near line 30
```

Note: The sudo access command paths that are listed here are an example. The actual command paths vary depending upon the resource. Ensure that the correct path is specified in the `sudoers` file.

3. Set the password for the newly created user.

   Issue the command:

   ```
   bash-2.05b$passwd tdiuser
   ```

Creating a super user on an HP-UX Trusted operating system

You can create a user with required permissions to run the adapter correctly on a workstation that uses an HP-UX Trusted operating system.

About this task

In this example, the user is "tdiuser".

Procedure

1. Create a user and specify the home directory.
   a) Issue the command:

   ```
   useradd –d "/home/tdiuser" –s "/sbin/sh" –m tdiuser
   ```

   b) Ensure that the `/home/tdiuser/.profile` file exists. If not, you must create the `.profile` file.

   c) Set the following statement in the user PATH environment variable:

   ```
   PATH=/usr/bin:/usr/sbin:/etc:/usr/local/bin:/usr/sam/lbin:/usr/sbin/acct:
   ```

   The following commands must be in the user path:

   mv, **tee**, **cp**, **kill**, **usermod.sam**, **mkdir**, **rm**, **fwtmp**, **sudo**

   If the super user is used to log in and run commands, then '.' can be added to the PATH environment variable.

2. Grant sudo permissions to the user for all commands.

   Note: By default, the **sudo** command requires user authentication before it runs a command. To modify this behavior, add the NOPASSWD tag to the sudoers file entry.

   a) Open the sudoers file.

   Issue the following command:

   ```
   bash-2.05b$ visudo
   ```

   b) If the line `Defaults requiretty` exists in the file, comment it out.

   ```
   #Defaults requiretty
   ```

   c) Insert the following lines to allow sudo access.

The entry beginning with `tdiuser` must be entered on a single line. It is displayed here as multiple lines for readability.

```
# User privilege specification
tdiuser ALL=NOPASSWD:/usr/bin/passwd,/usr/sbin/useradd,
/usr/sbin/usermod,/usr/sbin/userdel,/usr/bin/cat,/usr/lbin/getprpw,
/usr/lbin/modprpw,/usr/bin/chmod,/usr/bin/ls,/usr/bin/tee,
/usr/bin/ed,/usr/sbin/logins,/usr/sam/lbin/usermod.sam,
/usr/sbin/groupadd,/usr/sbin/groupdel,/usr/sbin/groupmod,
/usr/bin/cp,/usr/bin/mkdir,/usr/bin/rm,/usr/bin/kill,
/usr/bin/hostname,/usr/sbin/acct/fwtmp
```

The following commands are used by the connector but are not needed in the sudoers file. However, if the sudo user is used, the user needs execute permissions on these commands.

```
/usr/bin/tr, /usr/bin/cut, /usr/bin/egrep, /usr/bin/awk,
/usr/bin/head, /usr/bin/sort, /usr/bin/ps, /usr/bin/sed
```

Note: The UNIX and Linux Adapter does not support accessing the endpoint as a user with sudo `log_output` enabled.

d) Validate the format of the `/etc/sudoers` file

Issue the command:

```
visudo -c
```

If syntax is wrong the command prompts an error message, for example:

```
$ visudo -c
        >>> sudoers file: syntax error, line 30 <<<
        parse error in /etc/sudoers near line 30
```

Note: The sudo access command paths that are listed here are an example. The actual command paths vary depending upon the resource. Ensure that the correct path is specified in the `sudoers` file.

3. Set the password for the newly created user.

   Issue the command:

```
bash-2.05b$passwd tdiuser
```

Command setup for sudo

Some commands need sudo access.

The following table lists the files that are used by the commands. In this table:

- *homedirectory* is the complete path to a user's home directory. For example, `/home/username`.
- Shell can be `/bin/bsh`, `/bin/sh`, and others.
- *profilepath* is the complete path to a user's shell initialization file. For example, `homedirectory/.profile`.

Table 31. Sudo access command and file setup

Command	Files that are used by the command	Operation	Operating System

cat	`/var/adm/cron/at.allow`
	`/var/adm/cron/ at.deny`
	`/var/adm/cron/cron.allow`
	`/var/adm/cron/cron.deny`
		reconciliation
		useradd
		usermod
		userdel
			AIX

Table 31. Sudo access command and file setup (continued)

Command	Files that are used by the command	Operation	Operating System
	/etc/cron.d/at.allow /etc/cron.d/at.deny /etc/cron.d/cron.allow /etc/cron.d/cron.deny	reconciliation useradd usermod userdel	Solaris
	/var/adm/cron/at.allow /var/adm/cron/at.deny /var/adm/cron/cron.allow /var/adm/cron/cron.deny	reconciliation useradd usermod userdel	HP-UX-Trusted HP-UX-Nontrusted
	/etc/at.allow /etc/at.deny /etc/cron.allow /etc/cron.deny	reconciliation useradd usermod userdel	Linux
	$homedir/.profile $homedir/.bash_profile $homedir/.bash_login $homedir/.cshrc $homedir/.login	reconciliation	HP-UX-Trusted HP-UX-Nontrusted Linux Solaris
	/tcb/files/auth/ $usernamefolder/ $username, where $usernamefolder is the first letter of the user name	reconciliation	HP-UX-Trusted
	/etc/passwd	usermod userdel set home directory	AIX
	/etc/passwd	set umask	Linux - NonShadow Linux - Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
	/etc/passwd	reconciliation	Linux - NonShadow Linux - Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris

Table 31. Sudo access command and file setup (continued)			
Command	**Files that are used by the command**	**Operation**	**Operating System**
	`/etc/passwd`	set home directory permissions	AIX Linux - NonShadow HP-UX-Trusted HP-UX-Nontrusted Solaris
	`/etc/passwd`	suspend and restore account and userdel	Linux - NonShadow
	`/etc/passwd`	set password and userdel	HP-UX-Trusted
	`/etc/passwd`	usermod	Linux - NonShadow Linux - Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
	`/etc/passwd`	suspend and restore account and userdel	Linux - Shadow
	`/etc/shadow`	reconciliation change password	Linux - Shadow
	`/etc/shadow`	reconciliation	HP-UX-Nontrusted Solaris
chage	NA	Useradd Usermod	Linux
chgroup	`/etc/group/etc/passwd`	Group mod	AIX

chmod	`/var/adm/cron/at.allow`
	`/var/adm/cron/at.deny`
	`/var/adm/cron/cron.allow`
	`/var/adm/cron/cron.deny`
		set permissions	AIX
			HP-UX-Trusted
			HP-UX-Nontrusted
			Solaris

	`AIXPConnRes.sh`
	`ViosAixPConnRes.sh`
	`mkvios.sh`
		set permissions	AIX

	`HPNTrustPConnRes.sh`	set permissions	HP-UX-Nontrusted
	`HPTrustPConnRes.sh` `CryptPwd`	set permissions	HP-UX-Trusted
	`LinuxPConnRes.sh`	set permissions	Linux - NonShadow
	`LinuxShadowPConnRes.sh`	set permissions	Linux - Shadow

Table 31. Sudo access command and file setup (continued)

Command	Files that are used by the command	Operation	Operating System
	`SolarisPConnRes.sh`	set permissions	Solaris
	`homedirectory` Location of temporary files on resource. The default location is `/tmp`.	set permissions	AIX Linux - NonShadow Linux - Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris

	`/etc/at.allow`
	`/etc/at.deny`
	`/etc/cron.allow`
	`/etc/cron.deny`
		useradd
		usermod
			Linux - NonShadow
			Linux - Shadow

`chpasswd`	`/etc/passwd`	Set password for LDAP registry	AIX
`chrole`	NA	Role modify	AIX
`chsec`	`/etc/security/lastlog`	restore account	AIX
`chuser`	*homedirectory* and shell	usermod	AIX
`cp` **Note:** CP command not being used by adapter code for these platforms.	`/etc/skel/local.cshrc, profilepath`	Useradd Usermod	HP UX (trusted and non-trusted) AIX
	`/etc/csh.cshrc, profilepath`	set umask	Linux - NonShadow Linux - Shadow
echo	NA	Useradd Usermod Suspend Restore Reconciliation	Linux Solaris AIX
ed	*profilepath*	set umask	Linux - NonShadow Linux - Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris

Table 31. Sudo access command and file setup (continued)

Command	Files that are used by the command	Operation	Operating System

	`/var/adm/cron/at.allow`
	`/var/adm/cron/at.deny`
	`/var/adm/cron/cron.allow`
	`/var/adm/cron/cron.deny`
		useradd
		usermod
		userdel
			AIX
			HP-UX-Trusted
			HP-UX-Nontrusted
			Solaris

	`/etc/at.allow`
	`/etc/at.deny`
	`/etc/cron.allow`
	`/etc/cron.deny`
		useradd
		usermod
		userdel
			Linux - NonShadow
			Linux - Shadow

`faillock`	NA	Useradd Usermod Reconcillation Suspend Restore	Linux
`faillog`	NA	Useradd Usermod Reconcillation Suspend Restore	Linux
`fwtmp`	`/var/adm/wtmp` `/var/adm/wtmps`	reconciliation	HP-UX-Trusted HP-UX-Nontrusted
`getprpw``/usr/lbin/getprpw`	NA	Usermod Suspend Restore	HP-UX (trusted)

`grep`	`/etc/at.allow`
	`/etc/at.deny`
	`/etc/cron.allow`
	`/etc/cron.deny`
		reconciliation	Linux - NonShadow
			Linux - Shadow

	homedirectory
	`/etc/passwd`
	`/etc/shadow`
	`/var/adm/cron/at.allow`
	`/var/adm/cron/ at.deny`
	`/var/adm/cron/cron.allow`
	`/var/adm/cron/cron.deny`
		Useradd
		Usermod
		Userdel
		Suspend
		Restore
		Reconciliation
			AIX

Table 31. Sudo access command and file setup (continued)

Command	**Files that are used by the command**	**Operation**	**Operating System**

	homedirectory
	`/etc/passwd`
	`/etc/shadow`
	`/etc/cron.d/at.allow`
	`/etc/cron.d/at.deny`
	`/etc/cron.d/cron.allow`
	`/etc/cron.d/cron.deny`
		Useradd
		Usermod
		Userdel
		Suspend
		Restore
		Reconciliation
			Solaris

	homedirectory
	`/etc/passwd`
	`/etc/shadow`
	`/var/adm/cron/at.allow`
	`/var/adm/cron/at.deny`
	`/var/adm/cron/cron.allow`
	`/var/adm/cron/cron.deny`
		Useradd
		Usermod
		Userdel
		Suspend
		Restore
		Reconciliation
			HP-UX (trusted and non-trusted)

`groups`	`/etc/group/etc/passwd`	Usermod Reconciliation	Linux AIX
`groupadd`	NA	Add group	Linux Solaris HP-UX (trusted & non-trusted)
`groupdel`	NA	Delete group	Linux Solaris HP-UX (trusted & non-trusted)
`groupmod`	NA	Mod group	Linux Solaris HP-UX (trusted & non-trusted)
`hostname`	NA	reconciliation	Linux Solaris HP-UX (trusted & non-trusted) AIX

Table 31. Sudo access command and file setup (continued)

Command	Files that are used by the command	Operation	Operating System
`kill`	NA	Userdel	Linux Solaris HP-UX (trusted & non-trusted) AIX
`lastlog`	`/var/log/lastlog`	reconciliation	Linux - NonShadow Linux - Shadow
`logins`	`/etc/group/etc/passwd`	Suspend Restore Reconciliation	Linux Solaris HP-UX (trusted & non-trusted)
`lsgroup`	`/etc/group/etc/passwd`	Groupmod Reconciliation	AIX

`ls -la`	`/etc/SuSE-release`
	`/etc/redhat-release`
	`/etc/debian_version`
		identify operating system	Linux - NonShadow
			Linux - Shadow

	`/tcb/files/auth/system/default`	identify operating system	HP-UX-Trusted
	`/usr/ios/cli/ios.level`	identify operating system	AIX
	homedirectory	delete home directory	AIX
	profilepath	set umask	Linux - NonShadow Linux - Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris

	`/var/adm/cron/at.allow`
	`/var/adm/cron/at.deny`
	`/var/adm/cron/cron.allow`
	`/var/adm/cron/cron.deny`
		useradd
		usermod
		userdel
			AIX
			HP-UX-Trusted
			HP-UX-Nontrusted
			Solaris

	homedirectory	reconciliation	Linux - NonShadow Linux - Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris

Table 31. Sudo access command and file setup (continued)

Command	**Files that are used by the command**	**Operation**	**Operating System**
	Location of temporary files on resource. The default location is `/tmp`. For example, `/tmp/AIXPConnRes.sh`	reconciliation	AIX Linux - NonShadow Linux - Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris

	`/etc/at.allow`
	`/etc/at.deny`
	`/etc/cron.allow`
	`/etc/cron.deny`
		useradd
		usermod
		userdel
			Linux - NonShadow
			Linux - Shadow

`lsrole`	NA	Reconciliation	AIX
`lsuser`	*homedirectory*	Add Modify Reconciliation	AIX
`mkdir`	Location of temporary files on resource. The default location is `/tmp`.	useradd usermod userdel cat	AIX HP-UX-Trusted HP-UX-Nontrusted Solaris Linux - NonShadow Linux - Shadow
`mkgroup`	`/etc/group/etc/passwd`	Groupadd	AIX
`mkrole`	NA	Create role	AIX
`mkuser`	*homedirectory*	add user with home directory	AIX
`modprpw``/usr/lbin/modprpw`	NA	Usermod Suspend Restore	HP_UX (trusted)
`mv`	*homedirectory*	move home directory	AIX
`pam_tally2`	NA	Useradd Usermod Reconcillation Suspend Restore	Linux

Table 31. Sudo access command and file setup (continued)

Command	Files that are used by the command	Operation	Operating System
passwd	/etc/passwd/etc/shadow	Useradd Usermod Restore	Linux Solaris HP-UX (trusted & non-trusted) AIX
pwdadm	NA	Useradd Usermod Reconciliation	AIX
rmgroup	/etc/group	Groupdel	AIX
rm -rf	homedirectory	delete home directory	AIX
rmrole	NA	Role delete	AIX
rmuser	NA	Userdel	AIX
	Location of temporary files on resource. The default location is /tmp.	useradd usermod userdel cat	AIX HP-UX-Trusted HP-UX-Nontrusted Solaris Linux - NonShadow Linux - Shadow
tee	profilepath	set umask	Linux - NonShadow Linux - Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
	/var/adm/cron/at.allow /var/adm/cron/at.deny /var/adm/cron/cron.allow /var/adm/cron/cron.deny	useradd usermod userdel	AIX HP-UX-Trusted HP-UX-Nontrusted Solaris
	/etc/at.allow /etc/at.deny /etc/cron.allow /etc/cron.deny	useradd usermod userdel	Linux - NonShadow Linux - Shadow

Table 31. Sudo access command and file setup (continued)

Command	Files that are used by the command	Operation	Operating System
test	/tcb/files/auth/ usernamefolder/username reconScriptLoc (user-specified location on resource for reconscripts)	reconciliation	Linux Aix Solaris HP-UX (trusted and non - trusted)
useradd	*homedirectory*	add user with home directory	Linux - NonShadow Linux - Shadow HP-UX-Trusted HP-UX-Nontrusted Solaris
userdel	*homedirectory*	Delete user	Linux Solaris HP-UX (trusted & non-trusted)
usermod	*homedirectory* and shell	Useradd Usermod	AIX
usermod.sam /usr/sam/ lbin/ usermod.sam	NA	Useradd Usermod	HP-UX (trusted & non-trusted)

Key-based authentication for the UNIX and Linux Adapter

An alternative to password-based authentication is Identity/Pubkey authentication. This type of authentication eliminates the need for static passwords.

A password can be captured by a keystroke logger or witnessed as you type it. Instead of providing a password, you have a key pair on your disk that you use to authenticate.

The following sections describe a typical SSH connection between a server and a client. For this setup example, the workstation that runs the IBM Security Directory Integrator server is the SSH client and the managed resource is the SSH server.

Enabling RSA key-based authentication on UNIX and Linux operating systems

You can use RSA key-based authentication as an alternative to simple password authentication.

About this task

Depending upon the **ssh-keygen** availability on the machine where Security Directory Integrator is installed, perform this task on either of the following machines.

- If **ssh-keygen** is not installed or unavailable on the machine where Security Directory Integrator is installed, perform this task on the managed resource.

- If **ssh-keygen** is installed or available, prefer to perform this task on the machine where Security Directory Integrator is installed.

Procedure

1. Use the **ssh-keygen** tool to create a key pair.
   a) Log in as the administrator user defined on the service form.
   b) Start the **ssh-keygen** tool. Issue the following command.

   ```
   mydesktop$# ssh-keygen -t rsa
   ```

   c) At the following prompt, accept the default or enter the file path where you want to save the key pair and press Enter.

   ```
   Generating public/private dsa key pair.
   Enter the file in which to save the key (home/root/.ssh/id_rsa):
   ```

   d) At the following prompt, accept the default or enter the passphrase and press Enter.

   ```
   Enter the passphrase (empty for no passphrase): passphrase
   ```

   e) At the following prompt, confirm your passphrase selection and press Enter.

   ```
   Enter the same passphrase again: passphrase
   ```

   This example is a sample of the system response:

   ```
   Your identification was saved in /home/root/.ssh/id_rsa.
   Your public key was saved in /home/root/.ssh/id_rsa.pub.
   The key fingerprint is this value:
   2c:3f:a4:be:46:23:47:19:f7:dc:74:9b:69:24:4a:44 root@ps701
   ```

   Note: Although the **ssh-keygen** tool accepts a blank passphrase, the passphrase is required on the service form.

2. Validate that the keys were generated.
   a) Issue the following commands.

   ```
   mydesktop$ cd $HOME/.ssh

    mydesktop$ ls -l
   ```

   A sample system response is:

   ```
   -rw------- 1 root   root   883 Jan 21 11:52 id_rsa
   -rw-r--r-- 1 root   root   223 Jan 21 11:52 id_rsa.pub
   ```

   b) Issue the following command.

   ```
   mydesktop$ cat id_rsa
   ```

   A sample system response is:

   ```
     -----BEGIN RSA PRIVATE KEY-----
   Proc-Type: 4,ENCRYPTED
   DEK-Info: DES-EDE3-CBC,7F4CF1E209817BA0

   GuIQh4EdIp2DY1KfgB3eHic1InCG5VC9/dumHd7AqEnlo241fRuIo8zgO87GV+tk
   cvKd/pPCGhmyCZy/are0wZt3KLYWUyoN7i+8H2Khk8LmaspD6Tx309VHTfCyoJsu
   jtuR5c4HbcRtOYhMByHEqllEst1azzlIrO75Qj5cUG01K1MbdTeXq1xUGjo97s+V
   gEOokMQ+JmaJD9lrbiMz4wjWRtREjHfc1VYTA+ZE1W3HT3PfrjCnHm9RKKFaA6kM
   fPInefQgdzhCa0mCz+HOKJfkpfPh8ufGM9Jfb99VjZdI77LHeNN4VqeQ/VyPH7pn
   wp7GbEJ8g6iX4BWUWpXUVStfYNQTV8Dis7ayZtr3g/o+AKnh/dGnk1SHHNFgUUFf/
   +E0EXMokHSqqOzwf4t8xp4upnnS/7ag5MIVcU5/iWGW4sDEw7xfB25zD4lbvVK5
   kSZeWLgm79wMipKP90iEELPqO6cS2yPXd+ADfHs7FWPQW0UYGFeMnHa/
   tlglO5Pxo7ek2iR57mazmx33cofIX6E/ZI9XLysp5TR6Npq1x8KCv2Dk2x3QSH8F54EQmQ2+
   5uDsPA9Hg1B+agkBh/1g3tfevT01cCtUkQGl2ubhrNGB2SiiyKgw9Ks0AL3TO0ul
   D69D18r6Y6s3pHQ9LYAs6EIq3/5dqNYW8eLQ5eINUIlHBp9ep8+quyqSfB3qPCBW
   Db+qI09pYhkTrGBD8l5eQqs1T1h2gJsY2yyYV/Cp2m4fI+uHItCgSlkPROnj27Xh
   p6HAPaFA0zWOz1lmVNYhTbJZlbbwYyf/OKmYuOklSuQ=
   -----END RSA PRIVATE KEY-----
   ```

   c) Issue the following command.

   ```
   mydesktop$ cat id_rsa.pub
   ```

A sample system response is this message:

```
ssh-rsaAAB3NzaC1yc2EAAAABIwAAAIEA9xjGJ+8DLrxSQfVxXYUx4lc9copCG4HwD3TLO5i
fezBQx0e9UnIWNFi4Xan3S8mYd6L+TfCJkVZ+YplLAe367/vhc1nDzfNRPJ95YnATefj
YEa48lElu7uq1uofM+sZ/b0p7fIWvIRRbuEDWHHUmneoX8U/ptKFZzRpb/
vTE6nE= root@ps0701
```

3. Enable key-based authentication in the /etc/ssh directory on the SSH server.

   a) Ensure that the following lines exist in the sshd_config file:

   ```
   # Should we allow Identity (SSH version 1) authentication?
       RSAAuthentication yes

       # Should we allow Pubkey (SSH version 2) authentication?
       PubkeyAuthentication yes

       # Where do we look for authorized public keys?
   # If it doesn't start with a slash, then it is
   # relative to the user's home directory
   AuthorizedKeysFile .ssh/authorized_keys
   ```

   b) Restart the SSH server.

4. Copy the rsa.pub file to the SSH server.
5. If you have an existing authorized_keys file, edit it to remove any **no-pty** restrictions.
6. Add the public key to the authorized_keys file, from the /.ssh directory.

   Issue the following command.

   ```
   ssh-server$ cat ../id_rsa.pub >> authorized_keys
   ```

   Note: This command concatenates the RSA public key to the authorized_keys file.

   For example, $HOME/.ssh/authorized_keys. If this file does not exist, the command creates it.

7. Copy the id_rsa private key file to the client workstation where Security Directory Integrator is running.
8. Set the private key ownership value. If the Security Directory Integrator server is either Unix or Linux, use **chmod** to set the private key permissions value to 600.

   Note:

   - Complete these steps. When you log in to the server from the client computer, you are prompted for a passphrase for the key instead of a user password.
   - If the installed ssh uses the AES-128-CBC cipher, RXA cannot fetch the private key from the file. RSA key-based authentication does not work. To support RSA key-based authentication, take one of the following actions:
     - Install an ssh that uses the DES-EDE3-CBC cipher.
     - Install the RXA 2.3.0.9 package in your environment. RXA 2.3.0.9 supports the AES-128-CBC cipher.

       RXA 2.3.0.9 is included in the base release of Security Directory Integrator version 7.1.1, and is also available in Security Directory Integrator version 7.0 fix pack 8 and Security Directory Integrator version 7.1 fix pack 7.

Enabling DSA key-based authentication on UNIX and Linux operating systems

You can use DSA key-based authentication as an alternative to simple password authentication.

About this task

Depending upon the **ssh-keygen** availability on the machine where Security Directory Integrator is installed, perform this task on either of the following machines.

- If **ssh-keygen** is not installed or unavailable on the machine where Security Directory Integrator is installed, perform this task on the managed resource.
- If **ssh-keygen** is installed or available, prefer to perform this task on the machine where Security Directory Integrator is installed.

Procedure

1. Use the **ssh-keygen** tool to create a key pair.

   a) Log in as the administrator user defined on the service form.

   b) Start the **ssh-keygen** tool.

   Issue the following command.

   ```
   [root@ps2372 root]# ssh-keygen -t dsa
   ```

   c) At the following prompt, accept the default or enter the file path where you want to save the key pair and press Enter.

   ```
   Generating public/private dsa key pair.
   Enter the file in which to save the key (/root/.ssh/id_dsa):
   ```

   d) At the following prompt, accept the default or enter the passphrase and press Enter.

   ```
   Enter the passphrase (empty for no passphrase): passphrase
   ```

   e) At the following prompt, confirm your passphrase selection and press Enter.

   ```
   Enter the same passphrase again: passphrase
   ```

   This is a sample of the system response:

   ```
   Your identification is saved in /root/.ssh/id_dsa.
   Your public key is saved in /root/.ssh/id_dsa.pub.
   The key fingerprint is this one:
   9e:6c:0e:e3:d9:4f:37:f1:dd:34:fc:20:36:67:b2:94 root@ps2372.persistent.co.in
   ```

   Note: Although the **ssh-keygen** tool accepts a blank passphrase, the passphrase is required on the service form.

2. Validate that the keys were generated.

   a) Issue the following commands.

   ```
    [root@ps2372 root]# cd root/.ssh

    [root@ps2372 .ssh]# ls –l
   ```

   A sample system response is this message:

   ```
    -rwxr-xr-x 1 root root 736 Dec 20 14:33 id_dsa
    -rw-r--r-- 1 root root 618 Dec 20 14:33 id_dsa.pub
   ```

   b) Issue the following command.

   ```
   [root@ps2372 .ssh]# cat id_dsa
   ```

   A sample system response is this message:

   ```
   -----BEGIN DSA PRIVATE KEY-----
   Proc-Type: 4,ENCRYPTED
   DEK-Info: DES-EDE3-CBC,32242D3525AEDC64
   MOZ0m/BCLFNS+ujlcnQR3gOIb5w5hwu1jByw8/kyvTMIHqAx1ANgqV1gFBGX7F0
   vdfmNQKnjLcH8cGueUYnmx4vSu9FnKK91abNW9Nd67MDtJEztHckahXDYy7oX1t
   LNh3QtaZ32AgHro7QxxCGIHQeDaiGePg7WhVqH8EXo3c+/L/5sQpfx0eG30nrDjl
   +cmXgmzU2uQsPL2ckP9NQTgRU4QgWYDBle0YhUXTAG8eW9XG9iCm9iFO4WLWtWd24
   Q799A1w6UJReHKQq+vdrN76PgK32NMNmindOqzKVzFL4TsjLyGyWofImpG65oO
   FSc4GXTsRkZ0OQxixakpKShRpJ5pW6V1PN4tR/RCRWmpW/yZTr4qtQzcw+AY6ONA
   QEVtJQeN69LJncuy9MY/K2F7hn5lCYy/TOnM1OOD6/a1R6U4xoH6qkasLGchiTIP
   /NIfrITQho49I7cIJ9HmW54Bmeqh2U9WiSD4aSyxL1Mm6vGoc81U2XjJmcUmQ9XHmhx
   R4iWaATaz6RTsxBksNhn7jVx34DDvRDJ4MSjLaNpjnvAdYTM7YislsBulDTr8ZF6P9
   Fa7VyFP4TyCjUM1w==
                     -----END DSA PRIVATE KEY-----
   ```

   c) Issue the following command.

```
[root@ps2372 .ssh]# cat id_dsa.pub
```

A sample system response is this message:

```
      ssh-dsa
AAAAB3NzaC1kc3MAAACBAIHozHi6CHwvGDt7uEYkEmn4STOj2neOo5mPOZFpBjs
KzzWBqBuAxoMwMgHy3zZAIgmzMwIVQum4/uIHlhOx0Q4QDLJbveFShuXxBjm5BOU1
rCCSeqYCOPdub9hx3uzZaTNqfFIvO4/NTcjp7pgQqBdvWs0loyYViYVWpVQmMdif
AAAAFQDhaD9m//n07C+R+X46g5iTYFA9/QAAAIBVbBXXL3/+cHfbyKgCCe2CqjRESQ
i2nwiCPwyVzzwfHw4MyoYe5Nk8sfTiweY8Lus7YXXUZCPbnCMkashsbFVO9w
/q3xmbrKfBTS+QOjs6nebftnxwk/RrwPmb9MS/kdWMEigdCoum9MmyJlOw5fwGl
P1ufVHn+v9uTKWpPgr0egAAAIArKV4Yr3mFciTbzcGCicW+axekoCKq520Y68mQ
1xrI4HJVnTOb6J1SqvyK68eC2I5lo1kJ6aUixJt/D3d/GHnA+i5McbJgLsNuiDs
RI3Q6v3ygKeQaPtgITKS7UY4S0FBQlw9q7qjHVphSOPvo2VUHkG6hYiyaLvLrX
Jo7JPk6tQ== root@ps2372.persistent.co.in
```

3. Enable key-based authentication in the `/etc/ssh` directory on the SSH server.

   a) Ensure that the following lines exist in the `sshd_config` file:

   ```
   # Should we allow Identity (SSH version 1) authentication?
       DSAAuthentication yes

       # Should we allow Pubkey (SSH version 2) authentication?
       PubkeyAuthentication yes

       # Where do we look for authorized public keys?
   # If it doesn't start with a slash, then it is
   # relative to the user's home directory
   AuthorizedKeysFile .ssh/authorized_keys
   ```

   b) Restart the SSH server.

4. Copy the `dsa.pub` file to the SSH server.
5. If you have an existing `authorized_keys` file, edit it to remove any **`no-pty`** restrictions
6. Add the public key to the `authorized_keys` file, from the `/.ssh` directory.

   Issue the command:

   ```
   [root@ps2372 .ssh]# cat id_dsa.pub >> authorized_keys
   ```

   Note: This command concatenates the DSA public key to the `authorized_keys` file.

   For example, `$HOME/.ssh/ authorized_keys`. If this file does not exist, the command creates it.

7. Copy the `id_dsa` private key file to the client workstation where Security Directory Integrator is running.
8. Set the private key ownership value. If the Security Directory Integrator server is either Unix or Linux, use **chmod** to set the private key permissions value to `600`.

   Note:

   - Complete these steps. When you log in to the server from the client computer, you are prompted for a passphrase for the key instead of a user password.
   - If the installed ssh uses the AES-128-CBC cipher, RXA cannot fetch the private key from the file. RSA key-based authentication does not work. To support RSA key-based authentication, take one of the following actions:
     - Install an ssh that uses the DES-EDE3-CBC cipher.
     - Install the RXA 2.3.0.9 package in your environment. RXA 2.3.0.9 supports the AES-128-CBC cipher.

       RXA 2.3.0.9 is included in the base release of Security Directory Integrator version 7.1.1, and is also available in Security Directory Integrator version 7.0 fix pack 8 and Security Directory Integrator version 7.1 fix pack 7.

Index