IBM Security Verify Identity
7

Amazon Web Services
Installation and Configuration Guide

BA21-8475-00

Contents

Tables

Chapter 1. Overview

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 Amazon Web Services adapter uses the Security Directory Integrator functions to facilitate communication between the Identity server and Amazon Web Services Identity and Access Management.

Features of adapter

The Amazon Web Services adapter automates several administrative tasks on the Identity and Access Management. The AWS IAM adapter checks the connection between the AWS Identity and Access Management and Identity server.

The adapter automates the following tasks:

- Reconcile group and group attributes.
- Reconcile role and role attributes.
- Reconcile policy and policy attributes.
- Reconcile user and user attributes.
- Create, modify, suspend, restore, change password, and delete a user.

Architecture of adapter

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

The adapter requires the following components:

- The Dispatcher
- The IBM Security Directory Integrator connector
- Identity server 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.

The AWS IAM adapter consists of IBM Security Directory Integrator Assembly Lines. When an initial request is made by Identity server to the AWS IAM adapter, the assembly lines are loaded into the Security Directory Integrator server. Subsequent service requests do not require those same assembly lines to be reloaded.

Supported configurations

The AWS IAM adapter supports a number of different configurations and is designed to operate with Identity server.

The following components are the fundamental components of an AWS IAM adapter environment:

- An Identity server
- An IBM Security Directory Integrator server
- The managed resource
- The AWS IAM adapter

As part of each configuration, the AWS IAM adapter must be installed on the computer that is running the IBM Security Directory Integrator server.

For a single-server configuration, you must install the Identity server, IBM Security Directory Integrator server, and the AWS IAM adapter on one server. That server communicates with the AWS IAM server.

Chapter 2. Planning

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

Prerequisites

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

The following table identifies the software and operating system prerequisites for the AWS IAM adapter installation.

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

Table 1. Prerequisites to install the adapter

Prerequisite	**Description**
Operating system	The AWS IAM can be used on any operating system that is supported by Security Directory Integrator.
Network Connectivity	Internet Protocol network
System Administrator authority	To complete the adapter installation procedure, you must have system administrator authority.
Directory Integrator	• IBM Security Directory Integrator 7.1.1 + 7.1.1-TIV-TDI-FP0004 + 7.2.0-ISS-SDI-LA0008 • IBM® Security Directory Integrator Version 7.2 **Note:** • Earlier versions of IBM Security Directory Integrator that are still supported might function properly. However, to resolve any communication errors, you must upgrade your Directory Integrator release to the versions that the adapter officially supports. • The adapter supports IBM Security Directory Integrator 7.2, which is available only to customers who have the correct entitlement. Contact your IBM representative to find out whether you have the entitlement to download IBM Security Directory Integrator 7.2.
Identity server	The following servers are supported: • Identity server Version 10.0 • Identity server Version 10.0 • IBM Security Identity Governance and Intelligence server Version 5.2.2 + 5.2.2.0- ISS-SIGI-FP0001 + 5.2.2.1-ISS-IGI-IF0002 • IBM Security Identity Governance and Intelligence server Version 5.2.3

Table 1. Prerequisites to install the adapter (continued)	
Prerequisite	**Description**
Security Directory Integrator adapters solution directory	A Security Directory Integrator adapters solution directory is a Security Directory Integrator work directory for adapters. For more information, see the *Dispatcher Installation and Configuration Guide*.
AWS SDK for Java	See the *AWS IAM Adapter Release Notes* for the supported API package name and version.

For more information about the prerequisites and supported operating systems for Security Directory Integrator, see the *IBM Security Directory Integrator 7.2: Administrator Guide*.

Software downloads

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

Go to IBM Passport Advantage.

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

Note:

You can also obtain additional adapter information from IBM Support.

Installation Worksheet

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

Table 2. Required information to install the adapter		
Required information	**Description**	**Value**
Security Directory Integrator Home Directory	The *ITDI_HOME* directory contains the jars/connectors subdirectory that contains adapter JAR files.	Windows: • *drive*\Program Files \IBM\TDI\V7.2 UNIX: • /opt/IBM/TDI/V7.2
Adapters solution directory	For more information about the solution directory, see the *Dispatcher Installation and Configuration Guide*.	The default solution directory is at: Windows: • *drive*\Program Files \IBM\TDI\V7.2*timsol* UNIX: • /opt/IBM/TDI/V7.2/ *timsol*

Chapter 3. Installing

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

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

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 binaries or connector

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

Before you begin

- The Dispatcher must be installed.

Procedure

1. Create a temporary directory on the workstation where you want to extract the adapter.
2. Extract the contents of the compressed file in the temporary directory.
3. Copy the `AWSIAMConnector.jar` file to the *`ITDI_HOME`*`/jars/connectors` directory.
4. Restart the adapter service.

Installing third-party client libraries

The adapter requires access to the AWS SDK Java Client Library at run time.

Before you begin

Download the API library from the Amazon Web Services website https://aws.amazon.com/sdk-for-java/.

About this task

Amazon Web Services might provide client library files, which are newer than what is documented in the guide or in the release notes. While the newer library files can work with the adapter, use these files with caution because they are not tested by IBM. If possible, use the same version as listed here or in the release notes.

Procedure

1. Go to the AWS SDK for Java website at https://aws.amazon.com/sdk-for-java/.
2. Download the AWS SDK for Java package to a temporary directory.

3. Extract SDK files.
4. From the `lib` directory, copy the file `aws-java-sdk-1.11.191.jar` into *ITDI_HOME*`\jars\patches` directory.
5. Under `third-party\lib`, copy all files except `spring* jars` into *ITDI_HOME*`\jars\patches`. See the *AWS IAM Adapter Release Notes* for these JAR files in the package.
6. Restart the Dispatcher service.

   For more information about starting and stopping the service, see the *Dispatcher Installation and Configuration Guide*.

Creating a service user

To create a service for the Amazon Web Services, you specify the Amazon Web Services user.

Before you begin

If you do not have an AWS account, you must create an account to use IAM. It is not mandatory to specifically sign up to use IAM. You can use IAM without any charge. To create an AWS account, perform the following steps.

1. Access the website http://aws.amazon.com.
2. Click **Create an AWS Account**.
3. Follow the on-screen instructions.

About this task

As a best practice, do not use the AWS account root user wherever possible. Instead, create a new IAM service user for Amazon Web Services that requires administrator access. Then, grant an administrator role to the user by adding the user into an `Administrators` group to which, you attach the administrator access managed policy.

Procedure

1. Open https://console.aws.amazon.com/iam with IAM account root user.
2. In the navigation pane, select **Users**, and then select **Add user**.
3. Specify a user name in **User name** box. The name can consist of letters, digits, and the following characters: plus (+), equal (=), comma (,), period (.), at (@), underscore (_), and hyphen (-). The name is not case-sensitive and can be a maximum of 64 characters in length.
4. Select the check box next to **Programmatic access**.
5. Select **Next: Permissions**.
6. On the **Set permissions for user** page, select **Add user to group** if you already have a group with an `AdministratorAccess`. If you do not have a group with `AdministratorAccess`, then choose `Attach existing policies directly`, and select `AdministratorAccess`.

   Note: If you do not want to grant `AdministratorAccess` to the service user, grant the permission that has administrator privileges on Amazon Web Services Identity and Access Management.
7. Choose **Next: Review** to see the list of group memberships to be added to the new user.
8. When you are ready to proceed, select **Create user**.

   In the next page, created user name, access key ID, and secret access key are displayed.
9. Save the `Access Key ID` and `Secret Access Key` to configure AWS IAM Adapter.

Importing the adapter profile

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

Before you begin

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

About this task

Service definition files are also called adapter profile files.

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

Procedure

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

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

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

Results

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

What to do next

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

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*.

Service or target form details

Complete the service/target form fields.

Service Details

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
Specify a description that identifies the service for your environment.

Security Directory Integrator location

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

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

Connection Details

Access Key ID
Secret Access Key
Own access keys to make programmatic calls to AWS from the AWS SDKs. When a user creates an access key, IAM returns the access key ID and secret access key. Access the website http://aws-portal.amazon.com/gp/aws/developer/account/index.html?action=access-key. See *Security Credentials* section of your account to obtain your access keys.

Region
The default region for Amazon Web Service Connection. The default value is `us-east-1`.

Enable Reconcile Roles
Select the check box to accumulate the AWS roles during the reconciliation.

Enable TDI Detailed Debugging
Select the check box to enable detailed log option of an assembly line.

Dispatcher Attributes

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 a file path to load the assembly lines from the `profiles` directory of the Windows operating system such as: *`drive`*`:\Program Files\IBM\TDI\V7.2\profiles`. You can also specify the following file path to load the assembly lines from the `profiles` directory of the UNIX and Linux® operating system: `/opt/IBM/TDI/V7.2/profiles`

Max Connection Count
Specify the maximum number of assembly lines that the dispatcher can run simultaneously for the service. Enter `10` when you want the dispatcher to run a maximum of 10 assembly lines

simultaneously for the service. If you enter `0` in the **Max Connection Count** field, the dispatcher does not limit the number of assembly lines that are run simultaneously for the service.

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

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

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

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

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

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

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

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

Dispatcher version
Specifies the version of the Dispatcher.

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

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

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

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

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

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

- Verify the adapter log to ensure that the test request was sent successfully to the adapter.
- Verify the adapter configuration information.
- Verify service parameters for the adapter profile. Verify parameters such as the work station name or the IP address of the managed resource and the port.

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.

Chapter 4. Configuring

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

Configuring the SSL connection between the Dispatcher and the AWS IAM server

To enable communication between the adapter and the AWS IAM server, you must configure keystores for the Dispatcher.

About this task

For more information about SSL configuration, see the *Dispatcher Installation and Configuration Guide*.

Procedure

1. Open a browser.
2. Log in to https://console.aws.amazon.com/iam with a user that is created. See "Creating a service user" on page 6.
3. View the certificate.
   - Click **SSL lock**.
   - If your browser reports that revocation information is not available, click **View Certificate**.
4. Click **Certification Path**
5. Select the **CA Root** certificate.
6. Export the certificate into a file that is encoded in the Base64 format.
7. Complete one of the following actions.
   - If the Dispatcher already has a configured keystore, use the **keytool.exe** program to import the AWS IAM Server certificate. Type the command on a single line.

     ```
     keytool -import -alias awsiam -file c:\AWSIAMCertificate.crt
     -keystore c:\truststore.jks -storepass passw0rd
     ```

   - If the keystore is not configured, create it by running the following command from a command prompt. Type the command on a single line.

     ```
     keytool -import -alias awsiam -file c:\AWSIAMCertificate.crt
     -keystore c:\truststore.jks -storepass passw0rd
     ```

     a. Download the Base-64 encoded X.509 (.CER) format of the CA certificate `Root 1 - Equifax Secure Certificate Authority`. Go to the GeoTrust website and search for `ca certificates`.

     b. Import the certificate into the keystore.

     ```
     keytool -import -alias Equifax -file C:\Equifax_Secure_Certificate_Authority.cer
      -keystore C:\truststore.jks -storepass passw0rd
     ```

8. Edit *ITDI_HOME*`/timsol/solution.properties` file to specify truststore and keystore information.

   In the current release, only **jks-type** is supported:

   ```
   # Keystore file information for the server authentication.
   # It is used to verify the server's public key.
   # example
   javax.net.ssl.trustStore=truststore.jks
   ```

```
javax.net.ssl.trustStorePassword=passw0rd
javax.net.ssl.trustStoreclass=jks
```

9. After you modify the `solution.properties` file, restart the Dispatcher.

   For more information about SSL configuration, see the *Dispatcher Installation and Configuration Guide*.

Creating accounts with programmatic access

An adapter user can select an access type on an account form to create a user account with programmatic access. Programmatic access supports to create a user with access key ID and secret access key as credentials.

Procedure

1. Open the Amazon Web Services account form.
2. Select `Programmatic Access` or `Console and Programmatic Access` to create a user with programmatic access.

   After a user account is created through the adapter, the `Secret Access Key` for that account is stored along with an `Access Key ID` in the `IDI_PS_DAFAULT(TABLE)` under the `Property Stores` of a Derby database in the Security Directory Integrator. Adapter user can see the `Secret Access Key` on account form after the first reconciliation of that account.

   Note: To preserve the `Secret Access Key` for the user accounts that are created through the adapter, the Derby database in the Security Directory Integrator must be in a listening mode.

Restore Amazon Web Services Account

Users can restore Amazon Web Services account.

Perform the following procedure to restore the Amazon Web Services account:

- **Programmatic Access Account**- Click **Suspend/Restore** and set the value from 1 to 0.
- **Console Access and Programmatic Access**- Click **Restore** and **Change Password** link.

Chapter 5. 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

You might encounter some problems at run time. Use this information to resolve some of these common runtime problems.

Runtime problems and corrective actions are described in the following table.

Table 3. Runtime problems

Problem	Corrective Action
Reconciliation does not return all AWS IAM accounts. Reconciliation is successful but some accounts are missing.	For the adapter to reconcile many accounts successfully, you might need to increase the WebSphere JVM memory. The complete the following steps on the WebSphere host computer: **Note:** Do not increase the JVM memory to a value higher than the system memory. 1. Log in to the administrative console. 2. Expand **Servers** in the left menu and select **Application Servers**. 3. A table displays the names of known application servers on your system. Click the link for your primary application server. 4. Select **Process Definition** from the **Configuration** tab. 5. Select the **Java Virtual Machine** property. 6. Enter a new value for the **Maximum Heap Size**. The default value is 256 MB. If the allocated JVM memory is not large enough, an attempt to reconcile many accounts with the adapter results in log file errors. The reconciliation process fails. The adapter log files contain entries that state `ErmPduAddEntry failed`. The *`WebSphere_install_dir`*`/logs/itim.log` file contains **`java.lang.OutOfMemoryError`** exceptions.
Create or delete operation status is displayed as `Pending` though the operation in adapter is complete.	The `Trace.log` file in TDI contains **`java.lang.ArrayIndexOutOfBoundsException`** exception. This issue might be a result of incompatible java version for the WebSphere servers on the appliance. For more information, see http://www.ibm.com/support/docview.wss?uid=swg21987814.

Chapter 6. Uninstalling

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

Removing the adapter binaries or connector

Use this task to remove the connector file for the AWS IAM adapter.

About this task

To uninstall the Dispatcher, see the *Dispatcher Installation and Configuration Guide*.

Procedure

1. Stop the Dispatcher service.
2. Delete the *ITDI_HOME*`/jars/connectors/AWSIAMConnector.jar` file.
3. Start the Dispatcher service.

Deleting the adapter profile

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

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

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

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

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

Chapter 7. 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

The Identity server communicates with the adapter by using attributes, which are included in transmission packets that are sent over a network. After you install the adapter profile, the AWS IAM adapter supports a standard set of attributes.

User attributes

The following tables contain the standard attributes and object classes that are supported by the AWS IAM adapter.

Table 4. Supported user attributes

Identity server name	Attribute name in schema	Data type	Note
User ID	eruid	String	None
Password	erpassword	Password	None
User ARN	erawsiamuserarn	String	None
List Policies	erawsiamlistpolicies	String	This attribute is associated with managed policies. Currently, AWS IAM adapter does not show inline policies.
User's Group Name	erawsiamusergroup	String	None
Change Password on Next Login	erawsiamchgpwdnextlogon	String	This attribute is used only when a user is created.
User Last Access Date	erawsiamlastaccessdate	String	None

Group attributes

Table 5. Supported group attributes

Identity server name	Attribute name in schema	Data type	Note
Group ID	erawsiamgroupid	String	This attribute is an object ID of the AWS IAM group.

Table 5. Supported group attributes (continued)			
Identity server name	**Attribute name in schema**	**Data type**	**Note**
Group Name	erawsiamgroupname	String	This attribute is mapped to the IBM Security Verify Identity erGroupName attribute. You cannot use the adapter to modify this attribute.
Group ARN	erawsiamgrouparn	String	This attribute is mapped to the IBM Security Verify Identity erGroupDescription attribute.
List Policies	erawsiamlistpolicies	String	This attribute is associated with managed policies. Currently, AWS IAM adapter does not show inline policies.

Object classes

Table 6. Supported object classes		
Description	**Object class name in schema**	**Superior**
Service class	erawsiamservice	Top
Account class	erawsiamaccount	Top
Group class	erawsiamgroups	Top
Role class	erawsiamroles	Top
Policy class	erawsiampolicies	Top

Supported user attributes and descriptions

Table 7. Supported user attributes and descriptions	
Attribute	**Description**
erawsiamaccesstype	Access Type
erawsiamaccesskeyid1	Access Key ID
erawsiamsecretaccesskey1	Secret Access Key
erawsiamaccesskeyid2	Access Key ID
erawsiamsecretaccesskey2	Secret Access Key
erawsiamcreatedate1	Date Created
erawsiamlastused1	Date Last Used
erawsiamcreatedate2	Date Created

Table 7. Supported user attributes and descriptions (continued)	
Attribute	**Description**
erawsiamlastused	Date Last Used
erawsiamoptypeak1	Status
erawsiamoptypeak2	Status
erawsiamnewaccesskeyid	Create New Access Key ID

Adapter Configuration Properties

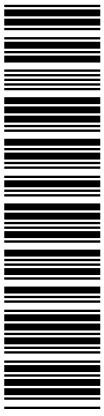
The following two logging hierarchies are available in the AWS SDK for Java. Set these two logging hierarchies as WARN in the TDI_HOME/timsol/log4j.properties.

- log4j.logger.com.amazonaws
- log4j.logger.org.apache.http.wire

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

Index

Part Number: 99F1234
Product Number: 1234-SS1



BA21-8475-00