IBM Security Directory Suite
8.0.1

Federated Directory Server Administration Guide

IBM

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

The client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBMproducts. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:
© (your company name) (year).
Portions of this code are derived from IBM Corp. Sample Programs.
© Copyright IBM Corp. _enter the year or years_.

Edition notice

Note: This edition applies to version 8.0.1.x of *IBM Security Directory Suite* (product number 5725-Y17) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

About this publication

IBM® Security Directory Integrator is an integrated development environment and runtime service for general-purpose, multi-format, multi-directional, real-time data movement, synchronization, and transformation.

Federated Directory Integrator Administration Guide contains information about using Federated Directory Server console to design, implement, and administer data integration solutions.

It also contains information about using the System for Cross-Domain Identity Management (SCIM) protocol and interface for identity management.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

For more information, see "Accessibility features for IBM Security Directory Suite" in the IBM Knowledge Center.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection, and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated, or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Chapter 1. Federated Directory Server administration

Federated Directory Server enables a collection of directories and other sources of data to be combined and treated as a single hierarchical directory. The Federated Directory Server console is a ready-to-use application that implements this directory integration.

Overview

The Federated Directory Server console provides synchronization services from one or more source systems, such as Active Directory or Sun Directory to the target directory. The IBM Security Directory Suite Directory Server is the default core centralized or target repository for Federated Directory Server.

The Federated Directory Server console has the following advantages:

- Requires less implementation time and effort than custom-built solutions because it is a ready-to-use, quality application.
- Easy to deploy and use.
- Enables integration across various data sources such as directories, databases, legacy data, and flat files, without affecting existing systems.
- Facilitates rapid deployment of identity and access management applications through a single point of access.
- Offers high speed, scalable performance, and superior security.

Features

Federated Directory Server has several features that help you quickly and easily implement directory integration solutions.

- Directory integration is possible without requiring changes to existing legacy data.
- It pulls data automatically into Directory Server.
- All relationships can contain advanced mapping and data transformation.
- Both users and groups can be integrated.
- Directory hierarchies can be maintained or flattened.
- Groups, including dynamic groups, can be created in a Federated Directory Server implementation that spans sources.
- Enriched data about people can be created from linked and augmented data from multiple sources.
- Federated Directory Server can be configured so that the user authentication goes directly to the existing backend local systems. Password replication, which is considered a major cost, is not required.
- Search is enabled across all content that is in the existing directory and data infrastructure.
- Users can log in to the enterprise directory by using a unique attribute like email or employee ID.
- Legacy data and the custom mapping of attributes can be managed through an interface that is easy to use.
- Write-back can be enabled to update the original sources.

Business scenarios

Federated Directory Server is a hybrid approach that addresses the security and collaboration requirements of directory services in various business scenarios.

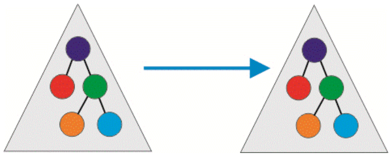
The following examples are some of the business needs that the features of Federated Directory Server can fulfil:

- You want to enable a central authentication service. However, you might want to leave passwords in place in the original source directory.
- You are required to manage groups across multiple directories to support services like enterprise messaging and access control.
- You want to augment your identity information so that the central LDAP directory can support the specific needs of applications and services.

By default, Directory Server is the centralized core back-end directory server. The administrator can choose the level of service that is required, for example pass-through authentication or write-back. Also, if required, a different system can be used as the central identity repository.

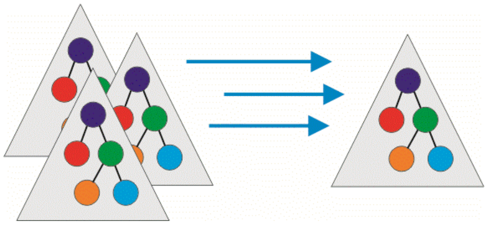
The specific needs of customers can be categorized into the following scenarios that are illustrated in the diagram.

Migrate directories or co-exist



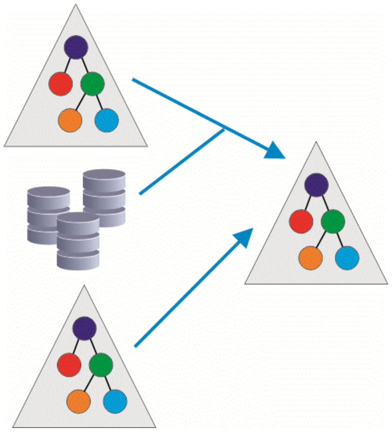
You can define the schemas and the amount of information that must be migrated. For example, you can provide more scalability and flexibility to data sources by migrating to Federated Directory Server without having to expand the schemas in the original data source.

Merge several data sources or directories



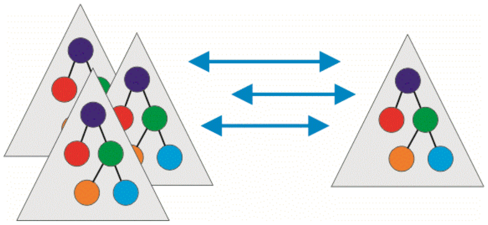
When you migrate or merge data from different data sources, the relationships can contain advanced mapping and data transformation. For example, you can integrate users and groups, maintain or flatten directory hierarchies, and create dynamic groups in Federated Directory Server that span data sources.

Enrich or augment with data from other sources



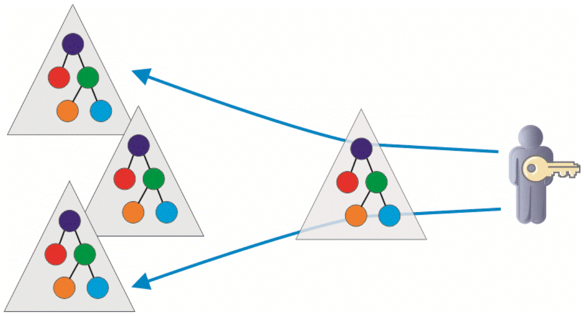
You can selectively add more data with a particular condition from another data source by setting up a join with the endpoint.

Selectively write back changes to the original source



If information is modified in the target directory server, it can be written back to the endpoint. However, the write-back is selective because some customers might want a barrier to preserve the original data in the endpoint.

Federate authentication back to the original source



Federated Directory Server can send the authentication request back to the endpoint where the credentials are stored so that the authentication process happens at the endpoint. The credentials are not required to be stored in the Federated Directory Server unless you choose to do so.

For example, you can combine the various capabilities of Federated Directory Server to create a custom solution that is specific to your requirements. Assume that you have an Active Directory that you want to use for single sign-on. You want to provide more scalability to it for more uses like social networking, but do not want to expand the schemas. You can migrate the data selectively, for example, only the email addresses of the users. Federated Directory Server also pulls the distinguished name (DN) from the source directory. You can then use the pass-through authentication capability of Federated Directory Server and retain the password credentials in the source directory itself without pulling it into the target directory. The user can log in to Directory Server by using a unique attribute, which is the email address in this case. The Directory Server does a bind with the DN to the Active Directory from where the user came. If a successful response is returned, then the user is authenticated.

Functional overview

Understand the key concepts, components, and architecture of Federated Directory Server.

The following diagram illustrates the various components of Federated Directory Server.

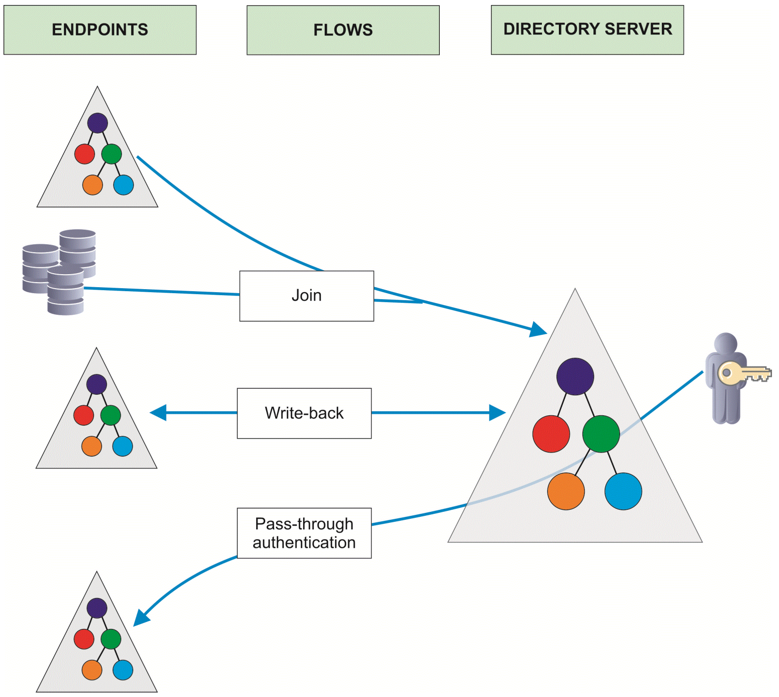


Figure 1. Federated Directory Server components

Directory Server
The IBM Security Directory Suite Directory Server, which is the target for all flows in the project.

Endpoint
A configured source system that can provide data in a flow. The endpoint types that are currently available are Active Directory, File, JDBC, LDAP, Directory Server, and Sun Directory.

Flow
A configuration that defines the relationship between the endpoints and the target Directory Server. You must create flows only after you configure the target Directory Server connection settings and add one or more endpoints.

Attribute maps
A map that is used to convert the attribute from the source schema to the corresponding attribute in the target schema. In Federated Directory Server you can apply one of the ready-to-use attribute maps or a customized attribute map to a flow operation.

Join
A configured source system that provides data that augments and enriches the data from the endpoint. If you configure a flow to specify a join with the endpoint, the entries are processed in the following manner:

1. An entry is read from the endpoint.
2. The flow looks it up on the join data source.
3. The entry is merged with the data from the endpoint.
4. The merged data is added to the target directory server.

Pass-through authentication
A feature of Directory Server where a user can be authenticated by delegating authentication to a different LDAP server. When you enable pass-through authentication for a flow, it configures Directory Server to use the credentials that are stored in the endpoint for authenticating users that originate from that flow.

Roadmap for getting started

Use the roadmap to understand the key tasks for setting up your Federated Directory Server configuration and to run synchronization operations.

Table 1. Roadmap for getting started with Federated Directory Server

Key steps	Optional or advanced tasks
Understand the key concepts, components, and architecture.	
Access the Federated Directory Server console.	Configure security settings for accessing the console.
Connect to the target directory server.	Define custom attribute mapping between source endpoint and target directory server. Specify the log settings for the directory server.
Add endpoints and configure them for one or more of the following data sources: • LDAP • Active Directory • Directory Server • Sun Directory • JDBC • File and file parsers	Configure pass-through authentication to delegate authentication back to the endpoint.
Create a flow to define the relationship between the endpoints and the target directory.	
Define flow settings.	Extend the custom attribute map for a specific flow. Configure a join to augment the data from another data source selectively. Enable write-back to propagate changes that are made in the target directory server back to the endpoint.
Verify the flow configuration by running a simulated synchronization operation.	
Run the initial synchronization to migrate data to the target directory.	
Schedule periodic incremental synchronizations.	Manually run a synchronization operation.
Enable and configure monitoring for flows	
Use logs and reports to troubleshoot the flow configuration and synchronization operations.	Check the known issues and limitations to resolve specific issues.

Accessing the Federated Directory Server console

You can access the web-based Federated Directory Server console application in your browser.

About this task

To access the Federated Directory Server console, you require IBM Security Directory Suite, Enterprise Edition.

Procedure

1. Log onto the IBM Security Directory Suite virtual appliance console. See Logging on to the virtual appliance console.
2. On the **Appliance Dashboard**, locate the **Server Control** widget. The Server Components column displays a list of all the servers.
3. Select **Federated Directory Server** from the list.
4. Click **Start** to start Federated Directory Server.
5. After the Federated Directory Server is started, on the **Appliance Dashboard**, locate the **Quick Links** widget.
6. Click **Federated Directory Server** to open the console.

What to do next

To use Federated Directory Server, complete the following steps:

1. Connect to a target directory server.
2. Configure one or more endpoints.
3. Define flow settings.

Note: As you configure the various features of Federated Directory Server in the console, by default, the changes are saved automatically. To modify the default autosave and refresh settings for the console:

1. On the Federated Directory Server console menu bar, click **Options**.
2. If you want to manually save the configuration changes that you make in the console, clear the **Enable auto-save** check box.
3. If you do not want to automatically reload the configuration changes, clear the **Automatically update FDS when configuration is saved** check box.
4. To create a snapshot of the current configuration, specify a **Snapshot description** and then click **Create snapshot**.
5. You can later roll back the changes to the level when you created a snapshot. Select the snapshot from the **Load snapshot** and then click **Load**.

Security settings

Access to the Federated Directory Server console is controlled by a set of properties that specify the security settings.

You must specify the security settings in the `solution.properties` file. These properties control the access to the Federated Directory Server console.

To modify the properties in the `solution.properties` file, take the following actions:

1. Log onto the IBM Security Directory Suite virtual appliance console. See Logging on to the virtual appliance console.
2. From the top-level menu of the virtual appliance console, select **Configure** > **Advanced Configuration** > **Update Property**.
3. On the Update Property page, click the **All Properties** tab.

4. In the left pane, click to expand **Federated Directory Server property files** section. Alternately, for Federated Directory Server with SCIM as target, expand the **SCIM Target property files** section.
5. Click **solution.properties**. The properties are displayed in the right pane.
6. Select a property.
7. Click **Edit**.
8. In the **Update Property** page, edit the **Property value**.
9. Click **Save Configuration**.

Local and remote users are distinguished by the client IP address in the incoming access request:

- If the IP address belongs to one of the network cards on the system where Federated Directory Server is running, it is considered a `localhost` user.
- All other IP addresses are considered as remote users.

Access permission for `localhost` users is built in with the following credentials:

User name: `admin`
Password: `admin`

To specify access control and permissions, you can set or modify the following authentication properties:

dashboard.auth=true

Indicates whether users are required to authenticate.

Valid values are `true` if users are required to authenticate or `false` if no authentication is required.

dashboard.auth.localhost

Indicates the type of authentication that connections from the `localhost` must use.

Valid values are:

- `properties` specifies that property-based authentication must be used.
- `none` specifies that authentication is not required.
- `deny` specifies that all connections from `localhost` are denied.
- `ldap` specifies that authentication is done by logging in to an LDAP server and optionally validating group membership.

dashboard.auth.remote

Indicates the type of authentication that remote connections must use.

Valid values are:

- `properties` specifies that property-based authentication must be used.
- `none` specifies that authentication is not required.
- `deny` specifies that all remote connections are denied access, that is, all connections that are not from the `localhost` are denied access.
- `ldap` specifies that authentication is done by logging in to an LDAP server and optionally validating group membership.

{protect}-dashboard.auth.user.*username=password*

Specifies the user credentials for remote access.

The default user name is `admin` with password `admin`:

```
{protect}-dashboard.auth.user.admin=admin
```

To specify multiple Federated Directory Server user login accounts, see the following example:

```
{protect}-dashboard.auth.user.admin=admin
{protect}-dashboard.auth.user.user1=user1passwd
{protect}-dashboard.auth.user.user2=user2passwd
```

dashboard.auth.ldap.url

Specifies the LDAP server address to use for authenticating the user. This property is used only if you specified `ldap` as the authentication mechanism.

Enter the LDAP host name, port number, and optionally a search base in the following format:

```
ldap://host:port [/search-base]
```

For example:

```
ldap://localhost:10389/ou=system
```

If the user provides an email address in the user name input field, Federated Directory Server first searches for a unique entry in the LDAP server from which it extracts the distinguished name (DN). Otherwise, it is expected that the value that is provided is acceptable to the LDAP server. After a DN is obtained for the user name and the password from the user, it does an LDAP basic authentication with the DN and password.

dashboard.auth.ldap.url.group

Specifies the LDAP server address to use for verifying group membership of the user after authentication. This property is used only if you specified `ldap` as the authentication mechanism.

Enter the LDAP host name, port number, and optionally a search base in the following format:

```
ldap://host:port [/search-base]
```

For example:

```
ldap://localhost:389/cn=group1,ou=groups,ou=system
```

If you specify this property, an additional authentication step is done after a user's credentials are authenticated against the LDAP repository. It checks that the authenticated user is also a member of the specified group before access is permitted.

Internet Explorer settings for remote access

Add the required configuration settings to access Federated Directory Server console from a remote system in an Internet Explorer browser, where Internet Explorer Enhanced Security Configuration (IE ESC) is enabled.

By default IE ESC blocks all scripts that are running on a web page. Federated Directory Server loads several scripts before it displays anything on the console. Hence, an IESC-enabled Internet Explorer browser shows a blank page when you open the console. To access the page, you must add sites that host the Federated Directory Server to the safe list of Internet Explorer.

1. From the **Internet Explorer** menu, click **Tools** > **Internet Options**.
2. Click **Security** tab.
3. Click **Trusted sites**.
4. Click **Sites**.
5. In the **Add this website to the zone** field, enter the URL of the Federated Directory Server console. For example: `https://myfds.com/fds/*`.
6. Click **Add**.
7. Click **Close** and then **OK** to close the page and save the settings.
8. Restart Internet Explorer browser.
9. Access the Federated Directory Server console in the Internet Explorer browser.

Connecting to Directory Server

The Directory Server is the default core centralized repository for Federated Directory Server. To use its synchronization services from one or more source systems to the target directory server, you must define the connection parameters for the target Directory Server in the Federated Directory Server console.

Procedure

1. In the Federated Directory Server console navigation pane, under **Directory Server**, click **Connection Settings**.
2. On the **Connection Settings** page, under **LDAP URL**, enter the **Host name** and **Port** of the target Directory Server.
3. For a secure connection, select **SSL**.
4. In the **User Login** and **Password** fields, enter the distinguished name and credentials for authentication to the Directory Server.
5. In the **Default Target Container** specify the container in the target Directory Server that is used to store the synchronized data. You can later specify a different target container for each scenario when you are creating flows.
6. In the next field, you can also specify a list of attributes that must be treated as binary attributes, for example, `jpegPhoto`. The format is one attribute name on each line.
7. Ensure that the connection is successful. Click **Test Connection**. A green tick mark displayed next to the name of the endpoint indicates that the connection is successful.
8. To see the entries in the target directory server, click **Browse Data**. You can use this feature to browse through the directory entries and add, delete, or modify them.

What to do next

See “Browsing the directory entries” on page 9.

Browsing the directory entries

Use the directory browser to view the directory hierarchy and the types of users, groups, and containers in the target Directory Server. You can also verify whether data was transferred correctly and add, modify, or delete entries.

Before you begin

Ensure that you can successfully connect to the target Directory Server from Federated Directory Server. A green tick mark displayed next to the **Connection Settings** link indicates that the connection is successful. If the connection is not successful, then the **Browse Directory** link is disabled.

Procedure

1. On the Federated Directory Server console, under **Directory Server**, click **Browse Directory**. You can also access the same browser from the directory server **Connection Settings** page.
2. Click **Search** to search an entry under the specified **Search base** for the **Search text** that you enter.
3. Click **Actions** and choose one of the following options:
   - To browse from the root of the directory server tree, click **Browse from root**.
   - To browse from the default target container that you specified with Connection Settings, click **Browse endpoint search base**.
4. Click an entry to view its attributes.

   Only attributes that are populated with values are displayed.
5. To display all attributes that are applicable to the object class for the entry, regardless of whether they have values, select **Show all attributes**.

   They are displayed in two sections, **Required Attributes** and **Optional Attributes**.

6. You can add, modify, or delete an entry.

   Add an entry

   Click **Actions** > **Add**.

   Select the entity type from the list that is displayed.

   Click **OK**.

   Modify the value of an attribute

   Click an entry in the directory tree navigation pane.

   In the attribute and value table that is displayed, double-click the value and edit it.

   Click **Save**. An `Entry modified` message appears on the header of the pane.

   Delete an entry

   Click an entry in the directory tree navigation pane.

   Click **Delete**.

   Click **OK**.

7. Optional: Test the access to the directory server.

   a) Click **Login test**.

   b) Enter the password to verify the credentials.

Enabling or disabling global write-back

Use the global write-back option to specify whether changes that are made in the target directory server must be propagated back to the source endpoint.

About this task

The global write-back option is a safety feature that you can disable to turn off write-back for all flows. However, if you want to selectively enable write-back for specific flows, you must leave this global write-back option enabled. Then, use the write-back option in each flow configuration to specify whether write-back is enabled or disabled for a particular flow. See "Enabling write-back for flows" on page 28.

Procedure

1. To enable the global write-back feature, under Directory Server, click **Write-back** and then select **Write-back enabled**. A green tick mark is displayed next to **Write-back**.

   A red cross mark indicates a problem with write-back. Hover your cursor over the red cross mark to see the tooltip about the error, and correct the problem.

2. Select **Ignore changes made by FDS** to indicate that you do not want the write-back operation to process entries that are modified by the user that is specified in the Directory Server connection settings.

   Example:

   `cn=root` is the user that is specified in connection settings.

   If you do not select **Ignore changes made by FDS**, then all changes that are made by the user `cn=root` are written-back to the source endpoint. It excludes changes that are made by Federated Directory Server flow operations.

Results

After a write-back operation, a summary of what was written back to the endpoint is displayed. The summary includes details such as the name of the flow, modified attributes, and the DNs of the directory server and endpoint. You can use the **Filter** field for searching the write-back summary.

Configuring pass-through authentication

Use pass-through authentication to delegate authentication back to the endpoint so that you do not have to migrate the credentials to the target Directory Server.

Before you begin

- Configure Directory Server for pass-through authentication. See Pass-through authentication in the IBM Security Directory Suite documentation.
- Verify the connection to the target Directory Server from Federated Directory Server. A green tick mark next to the **Connection Settings** link under **Directory Server** indicates that the connection is successful. If the connection is not successful, the **Pass-through Authentication** link is disabled.

About this task

Pass-through authentication is an optional feature of Directory Server, which delegates authentication of users to a different LDAP server. If you configure pass-through authentication, then Directory Server attempts to verify the credentials from an external LDAP directory server on behalf of the client.

Procedure

1. In the navigation pane, click **Pass-through Authentication** under **Directory Server**.
2. Click **Add** and specify a **Name** to identify the configuration.
3. In the **Target subtree** field, specify the Directory Server target subtree. Pass-through authentication is enabled only for the users in the containers of the target subtree.
   - Click **Select** to view the subtree and specify the container.
   - Click **Browse Data** to view, add, delete, or modify the entries in the target directory server.
4. Optional: Select **Enable password cache** to store the password in the target server during the first authentication. Subsequent authentications use the cached password.

   If a user changes the password on the endpoint, you must run a synchronization operation to update the password change in the target server.

   The password cache is supported for all the endpoint types that are supported by the Directory Server pass-through authentication feature.

   Limitation: If you enable the password cache feature and later disable it after a user authenticates, the user can still authenticate with the old password even after changing the password on the source.
5. Select an endpoint from **Select endpoint to copy connection details from**. The details are automatically filled in based on the connection parameters that you specified when you created the endpoint.
6. Optional: Edit the **Host name**, **Port**, **Search base**, **Username**, and **Password** fields, if necessary.
7. Click **Test Connection** to verify the connection settings for pass-through authentication.
8. Take one of the following actions:
   - Click **Save** to enable the pass-through authentication mechanism for the flows that are affected by this configuration.

     Affected flows are one or more flows whose target search base matches or is under the container hierarchy of the search base that you specified in the pass-through authentication configuration.
   - Click **Delete** if you do not want to enable pass-through authentication for affected flows.
9. Manually restart Directory Server for the changes to take effect and to enable pass-through authentication for affected flows.

Related tasks

"Browsing the directory entries" on page 9

Use the directory browser to view the directory hierarchy and the types of users, groups, and containers in the target Directory Server. You can also verify whether data was transferred correctly and add, modify, or delete entries.

Specifying the log settings

After you configure the connection settings for Directory Server, specify the path for the log file and log settings.

Procedure

1. In the navigation pane, under **Common Settings**, click **Log Settings**.
2. In the **Log Directory** field, specify the path for the log files. The default path is `LDAPSync/logs`.

   Note:

   - You can specify a path that is relative to the solution directory.
   - You can use forward slashes so that it is applicable to both Windows and UNIX systems.
3. In the **Log File History** field, specify the number of previous log files that must be retained. The default value is `20`.

What to do next

Configure one or more data resources as endpoints. See the following topics for the steps to configure the different types of endpoints.

Customizing attribute maps

When data is federated from multiple sources, the attributes must be mapped correctly when they are synchronized with the single target directory. You can specify how to convert attributes from the source endpoint schema to the target schema by defining custom maps for attributes.

About this task

The attribute mapping for standard schema such as Active Directory and Sun Directory is built in. Additionally, some ready-to-use custom maps are provided in Federated Directory Server. However, you might require to modify or extend these attribute maps or create new custom maps in some scenarios. For example, you might require custom maps if you use databases or files as your endpoint.

Procedure

1. In the navigation pane, under **Common Settings**, click **Attribute Maps**.

   The **Attribute Maps** page displays various attribute maps for person, group, and container objects. These maps are the ready-to-use map files in the *`sdi_solution_dir`*`/LDAPSync` directory.
2. Select the type of attribute map that you want to customize from the list.

   The attribute map table is displayed.
3. You can take any of the following actions:

   Create an attribute mapping

   a. Click **Add Attribute**.

   b. Select the attribute from the list of attributes in the target directory server. A new row is displayed with the selected attribute name under **Directory Server Attribute**.

      Note: If the **Add Attribute** window does not display the list of attributes from the target directory, take the following actions:

      i) Under **Directory Server** in the navigation pane, go to **Connection Settings**.

ii) Click **Test Connection**. Ensure that a green tick mark is displayed next to the name of the endpoint, which indicates that the connection is successful. This action also populates the fields that browse the target directory attributes.

Modify an attribute mapping

a. Under **Endpoint Attribute / Assignment**, double-click the default value to change the mapping and to specify more settings for the attribute mapping.

b. Select **Enabled** to use this attribute mapping for the endpoint.

c. Click **Simple Assignment** or **Scripted Assignment** to specify the type of mapping.

Note: If you select **Scripted Assignment**, you can define the assignment by writing JavaScript code in the text field or by calling a function in the `LDAPSync\customScript.js` file..

d. Under **Map when**, specify whether you want this mapping to be used for all operations, or only when either modifying an entry or creating an entry.

e. In the **Select Attribute** field, specify the attribute name in the source endpoint that must map to the target attribute.

Delete the mapping for a specific attribute

a. Select the check box beside the attribute.

b. Click **Remove Attribute**.

c. Click **OK**.

Duplicate a map to extend it with your custom attribute mapping.

a. Click **Duplicate Map**.

b. Enter a name for the new map file.

c. Click **OK**.

A new attribute map with all the attribute mapping entries of the source map is created.

Delete an attribute map and all its entries

a. Click **Delete Map**.

b. Click **OK**.

4. Click **Save**. Unless you save each map that you edited, the changes are lost.

Results

All attribute maps are stored in the *sdi_solution_dir*/`LDAPSync` directory.

What to do next

You can select this custom attribute map for flow operations when you define the flow specifications.

Configuring endpoints

You must specify endpoints for synchronization with the target Directory Server. You can configure multiple LDAP directories, databases, files, or even subtrees as endpoints in the Federated Directory Server console.

Before you begin

Ensure that you specify the connections settings for the target Directory Server. See "Connecting to Directory Server" on page 9.

Procedure

1. To specify a new endpoint, in the Endpoints section of the navigation pane, click **Add**.

The **Add Endpoint** window is displayed.

2. In the **Name** field, enter a name to identify the endpoint.
3. From the **Select endpoint type** list, select the appropriate type of endpoint.

   The following types of endpoints are available:

   - Active Directory
   - File
   - JDBC
   - LDAP
   - Sun Directory
   - Directory Server

   Note: After you create a configuration page for a specific type of endpoint, you cannot change it later. You must delete and create an endpoint again for the type of endpoint that you want to configure.

Results

The configuration page with endpoint parameters is displayed, which differs for each endpoint type.

In the navigation pane, a status icon is displayed next to each endpoint. You can click **Refresh** to see the latest status.

- A green dot is displayed soon after you create an endpoint and remains until you click **Test Connection** in the endpoint.
- After you test that the connection is successful, the green dot is replaced by a green tick mark.
- If the connection fails, a red cross mark is displayed.

What to do next

Configure the parameters for the endpoint. See the following topics for the different endpoint types.

If you want to delete an endpoint that you created and configured, follow these steps:

1. Under the **Endpoints** section of the navigation pane, right-click the name of the endpoint that you want to delete and then click **Delete**.
2. Click **OK** when the confirmation message appears.

Note: Flows that are based on an endpoint are also automatically deleted when you delete the endpoint.

Configuring an Active Directory endpoint

To configure an Active Directory as an endpoint, you must specify the LDAP URL, login name with credentials, the search base, and root suffix.

Before you begin

Ensure that you create an endpoint and specify the type as **Active Directory**. See “Configuring endpoints” on page 13.

Procedure

1. On the **Active Directory** endpoint configuration page, under **LDAP URL**, enter the **Host name** and **Port** of the Active Directory that you want to access. The default LDAP port number is 389. If you use SSL, the default LDAP port number is 636.

   For information about setting up SSL for Active Directory connections, see the IBM Security Directory Integrator documentation and search for *Microsoft Active Directory SSL configuration*.
2. For a secured connection, select **SSL**.

3. In the **User Login** and **Password** fields, enter the distinguished name and credentials for authentication to the service.

   For example: `cn=administrator,cn=users,dc=your_domain,dc=com`
4. In the **Include entries from the following container** field, enter the search base of the source directory under which entries are read for synchronization. Alternately, you can click **Contexts** and select from the **LDAP Search Base** list and then click **OK**.

   For example: `dc=your_domain,dc=com`

   Note: For Active Directory, this value must be set to the root suffix of the domain controller; otherwise, delete modifications are not detected.
5. To verify the Active Directory connection settings, click **Test Connection**.

   A green tick mark displayed next to the name of the endpoint indicates that the connection is successful. If the connection is successful, the attributes in the endpoint are displayed in a separate pane. You can use the **Filter** field to search the attributes.
6. After you configure the endpoint, to easily access the data in the directory, click **Browse Data**. You can use the LDAP browser to view the directory hierarchy and the types of users, groups, and containers. You can also add, modify, or delete entries in the directory.
7. Optional: You can also configure the following advanced parameters. Expand the **Advanced** section to view these parameters.

   Page Size
   Specify the number of entries per page that must be returned by the request. The default value is 500.

   Seconds Before Timeout
   Specify the maximum number of seconds to wait for the next changed Active Directory object. The default value is 0.

   Seconds Between Polling
   Specifies the number of seconds to sleep between successive polls. The default value is 60.

   Change State Key
   Specifies the name of the key or parameter that stores the change detection iterator state. The state key is used between runs to remember the last changed that was processed. If synchronization was stopped for any reason, when it is restarted, it can pick up from where it stopped.

   The value of this key must be unique for each endpoint. If you do not set this parameter, a value is computed automatically to ensure uniqueness.

   Binary Attributes
   Specify a list of attributes that must be interpreted as binary values instead of strings. When you enter the attribute names in this field, enter one attribute per line and do not use any separators.

What to do next

After you configure the endpoint, you can create a flow to define the relationship between the endpoint and the target directory server.

Related tasks

"Browsing the entries in an LDAP directory" on page 21
Use the directory browser to view the directory hierarchy and the types of users, groups, and containers in the endpoint. You can also verify whether data was transferred correctly and add, modify, or delete entries.

Configuring a file endpoint

To configure a file as an endpoint, you must specify the file path, type of entry, and the file parser.

Before you begin

Ensure that you create an endpoint and specify the type as **File**. See "Configuring endpoints" on page 13.

Procedure

1. On the **File** endpoint configuration page, in the **File Path** field, enter the path of the file that you want to access.
2. From the **Type of Entry** list, select `person`, `group`, or `container`.
3. To verify the file connection settings, click **Test Connection**.

   A green tick mark displayed next to the name of the endpoint indicates that the connection is successful. If the connection is successful, the attributes in the endpoint are displayed in a separate pane. You can use the **Filter** field to search the attributes.
4. Optional: You can also configure the following advanced parameters. Expand the **Advanced** section to view these parameters.

   Timeout (in seconds)

   Specify a positive number to indicate the number of seconds to wait between operations before timeout occurs.

   Specify 0 (zero) to wait forever.

   If you select the **Lock file** option, the **Timeout** value instead specifies how long to wait to acquire the lock.

   Lock file

   Select this option to indicate that an exclusive lock is acquired for writing to the file. This lock prevents the file from being opened for writing by another instance of Federated Directory Server or any other program until the lock is released.
5. From the **Parser** list, select the name of the parser that you require to access the file.

What to do next

After you configure the endpoint, you can create a flow to define the relationship between the endpoint and the target directory server.

Related concepts

“File parsers reference” on page 40

You can select and configure the appropriate file parser from the list that is provided in the file endpoint configuration page of the Federated Directory Server console.

Configuring a JDBC endpoint

To configure a JDBC connection as an endpoint, you must specify the JDBC URL, user name and password, schema, table name, and type of entry.

Before you begin

Ensure that you create an endpoint and specify the type as **JDBC**. See “Configuring endpoints” on page 13.

Procedure

1. On the JDBC endpoint configuration page, under **JDBC URL**, select the type of database from the **Type** list. You have the following options:
   - Choose a commonly used database.
     a. Select one of these databases from the list: DB2, Derby, `embedded Derby`, `solidDB`, `Microsoft SQL`, or `Oracle`.
     b. Specify the **Host name**, **Port**, and name of the **Database** wherever required.
   - Choose a generic database.
     a. Select `JDBC Details`.
     b. In the **JDBC URL** field, enter the JDBC connection URL for the database that you want to access. The following examples are some typical URLs for various JDBC providers:

Informix®
: jdbc:informix-sqli://*hostname*:*port*/*dbname*:informixserver=*Informix Server Name*

Sybase
: jdbc:sybase:Tds:*hostname*:*port*/

c. In the **JDBC Driver** field, enter the JDBC driver implementation class name. The following examples are some typical driver implementation class names for various JDBC providers:

Informix
: `com.informix.jdbc.IfxDriver`

Sybase
: `com.sybase.jdbc3.jdbc.SybDriver`

For more information about JDBC drivers, see the IBM Security Directory Integrator documentation and search for *Understanding JDBC Drivers*.

2. In the **Username** and **Password** fields, enter the login name and credentials to access the specified database.
3. From the **Table name** list, select the table or view for the operations. The list displays the tables in the specified database.
4. From the **Type of Entry** list, select `person`, `group`, or `container`.
5. To verify the JDBC connection settings, click **Test Connection**.

   A green tick mark displayed next to the name of the endpoint indicates that the connection is successful. If the connection is successful, the attributes in the endpoint are displayed in a separate pane. You can use this pane to browse through the records and **Filter** by attribute names.
6. Optional: You can also specify a custom SELECT statement to specify entries for operations.
   a) Expand the **Advanced** section.
   b) Enter the statement in the **Custom Select** field.
7. Optional: In the **Extra provider parameters** field, enter other parameters that are supported by the JDBC provider.
   a. Use the `name:value` format and enter one parameter on each line.
   b. Check your driver documentation for the supported parameters.
   c. For example, the following extra parameters are specific to DB2:

```
securityMechanism:KERBEROS_SECURITY
loginTimeout:20
readOnly:true
```

What to do next

After you configure the endpoint, you can create a flow to define the relationship between the endpoint and the target directory server.

Configuring an LDAP endpoint

To configure an LDAP directory as an endpoint, you must specify the LDAP URL, login name with credentials, the search base, and root suffix.

Before you begin

Ensure that you create an endpoint and specify the type as **LDAP**. See "Configuring endpoints" on page 13.

Procedure

1. On the LDAP endpoint configuration page, under **LDAP URL**, enter the **Host name** and **Port** of the LDAP directory that you want to access. The default LDAP port number is 389. If you use SSL, the default LDAP port number is 636.
2. For a secured connection, select **SSL**.
3. In the **User Login** and **Password** fields, enter the distinguished name and credentials for authentication to the service.

   For example: `cn=administrator,cn=users,dc=your_domain,dc=com`
4. In the **Include entries from the following container** field, enter the search base in the LDAP directory that is polled for changes. Alternately, you can click **Contexts** and select from the **LDAP Search Base** list and then click **OK**.

   For example: `dc=your_domain,dc=com`
5. To verify the LDAP directory connection settings, click **Test Connection**.

   A green tick mark displayed next to the name of the endpoint indicates that the connection is successful. If the connection is successful, the attributes in the endpoint are displayed in a separate pane. You can use the **Filter** field to search the attributes.
6. After you configure the endpoint, to easily access the data in the directory, click **Browse Data**. You can use the LDAP browser to view the directory hierarchy and the types of users, groups, and containers. You can also add, modify, or delete entries in the directory.
7. Optional: You can also configure the following advanced parameters. Expand the **Advanced** section to view these parameters.

   Binary Attributes

   Specify a list of attributes that must be interpreted as binary values instead of strings. When you enter the attribute names in this field, enter one attribute per line and do not use any separators.

   Page Size

   Specify the number of entries per page must be returned by the request. The default value is 500.

What to do next

After you configure the endpoint, you can create a flow to define the relationship between the endpoint and the target directory server.

Related tasks

"Browsing the entries in an LDAP directory" on page 21

Use the directory browser to view the directory hierarchy and the types of users, groups, and containers in the endpoint. You can also verify whether data was transferred correctly and add, modify, or delete entries.

Configuring a Sun Directory endpoint

To configure a Sun Directory as an endpoint, you must specify the LDAP URL, login name with credentials, the search base, and root suffix.

Before you begin

Ensure that you create an endpoint and specify the type as **Sun Directory**. See "Configuring endpoints" on page 13.

Procedure

1. On the Sun Directory endpoint configuration page, under **LDAP URL**, enter the **Host name** and **Port** of the Sun Directory service that you want to access. The default LDAP port number is 389. If you use SSL, the default LDAP port number is 636.
2. For a secured connection, select **SSL**.

3. In the **User Login** and **Password** fields, enter the distinguished name and credentials for authentication to the service.

   For example: `cn=administrator,cn=users,dc=your_domain,dc=com`
4. In the **Include entries from the following container** field, enter the search base in the Sun Directory that is polled for changes. Alternately, you can click **Contexts** and select from the **LDAP Search Base** list and then click **OK**.

   For example: `dc=your_domain,dc=com`
5. To verify the Sun Directory connection settings, click **Test Connection**.

   A green tick mark displayed next to the name of the endpoint indicates that the connection is successful. If the connection is successful, the attributes in the endpoint are displayed in a separate pane. You can use the **Filter** field to search the attributes.
6. After you configure the endpoint, to easily access the data in the directory, click **Browse Data**. You can use the LDAP browser to view the directory hierarchy and the types of users, groups, and containers. You can also add, modify, or delete entries in the directory.
7. Optional: You can also configure the following advanced parameters. Expand the **Advanced** section to view these parameters.

   Seconds Before Timeout
   Specify the maximum number of seconds to wait for the next changed Sun Directory object. The default value is 0.

   Seconds Between Polling
   Specifies the number of seconds the Connector sleeps between successive polls. The default value is 60.

   Change State Key
   Specifies the name of the key or parameter that stores the change detection iterator state. The state key is used between runs to remember the last changed that was processed. If synchronization was stopped for any reason, when it is restarted, it can pick up from where it stopped.

   The value of this key must be unique for each endpoint. If you do not set this parameter, a value is computed automatically to ensure uniqueness.

   Binary Attributes
   Specify a list of attributes that must be interpreted as binary values instead of strings. When you enter the attribute names in this field, enter one attribute per line and do not use any separators.

   Page Size
   Specify the number of entries per page that must be returned by the request.

What to do next

After you configure the endpoint, you can create a flow to define the relationship between the endpoint and the target directory server.

Related tasks

"Browsing the entries in an LDAP directory" on page 21
Use the directory browser to view the directory hierarchy and the types of users, groups, and containers in the endpoint. You can also verify whether data was transferred correctly and add, modify, or delete entries.

Configuring a Directory Server source endpoint

To configure a Directory Server as a endpoint, you must specify the LDAP URL, login name with credentials, the search base, and root suffix.

Before you begin

Ensure that you create an endpoint and specify the type as **Directory Server**. See "Configuring endpoints" on page 13.

Procedure

1. On the Directory Server source endpoint configuration page, under **LDAP URL**, enter the **Host name** and **Port** of the Directory Server that you want to access. The default LDAP port number is 389. If you use SSL, the default LDAP port number is 636.
2. For a secured connection, select **SSL**.
3. In the **User Login** and **Password** fields, enter the distinguished name and credentials for authentication to the server.

   For example: `cn=root`
4. In the **Include entries from the following container** field, enter the directory server search base that is polled for changes. Alternately, you can click **Contexts** and select from the **LDAP Search Base** list and then click **OK**.

   For example: `o=sample`
5. To verify the Directory Server connection settings, click **Test Connection**.

   A green tick mark displayed next to the name of the endpoint indicates that the connection is successful. If the connection is successful, the attributes in the endpoint are displayed in a separate pane. You can use the **Filter** field to search the attributes.
6. After you configure the endpoint, to easily access the data in the directory, click **Browse Data**. You can use the LDAP browser to view the directory hierarchy and the types of users, groups, and containers. You can also add, modify, or delete entries in the directory.
7. Optional: You can also configure the following advanced parameters. Expand the **Advanced** section to view these parameters.

   Seconds Before Timeout

   Specify the maximum number of seconds to wait for the next changed directory server object. The default value is 0.

   Seconds Between Polling

   Specifies the number of seconds to sleep between successive polls. The default value is 60.

   Change State Key

   Specifies the name of the key or parameter that stores the change detection iterator state. The state key is used between runs to remember the last changed that was processed. If synchronization was stopped for any reason, when it is restarted, it can pick up from where it stopped.

   The value of this key must be unique for each endpoint. If you do not set this parameter, a value is computed automatically to ensure uniqueness.

   Binary Attributes

   Specify a list of attributes that must be interpreted as binary values instead of strings. When you enter the attribute names in this field, enter one attribute per line and do not use any separators.

   Page Size

   Specify the number of entries per page that must be returned by the request.

What to do next

After you configure the endpoint, you can create a flow to define the relationship between the endpoint and the target directory server.

Related tasks

“Browsing the entries in an LDAP directory” on page 21

Use the directory browser to view the directory hierarchy and the types of users, groups, and containers in the endpoint. You can also verify whether data was transferred correctly and add, modify, or delete entries.

Browsing the entries in an LDAP directory

Use the directory browser to view the directory hierarchy and the types of users, groups, and containers in the endpoint. You can also verify whether data was transferred correctly and add, modify, or delete entries.

Before you begin

Ensure that you can successfully connect to the endpoint directory from Federated Directory Server. A green tick mark displayed next to the endpoint name under **Endpoints** indicates that the connection is successful. If the connection is not successful, then an error is displayed when you try to browse data.

About this task

This feature is available only for LDAP directories. The LDAP endpoints that you can configure in Federated Directory Server are Active Directory, LDAP, Sun Directory, and Directory Server.

Procedure

1. On the endpoint configuration screen, click **Browse Data**.
2. Click **Search** to search an entry under the specified **Search base** for the **Search text** that you enter.
3. Click **Actions** and choose one of the following options:
    - To browse from the root of the directory tree, click **Browse from root**.
    - To browse from the search base that you specified in the endpoint configuration, click **Browse endpoint search base**.
4. Click an entry to view its attributes.

    Only attributes that are populated with values are displayed.
5. To display all attributes that are applicable to the object class for the entry, regardless of whether they have values, select **Show all attributes**.

    They are displayed in two sections, **Required Attributes** and **Optional Attributes**.
6. You can add, modify, or delete an entry.

    Add an entry

    Click **Actions** > **Add**.

    Select the entity type from the list that is displayed.

    Click **OK**.

    Modify the value of an attribute

    Click an entry in the directory tree navigation pane.

    In the attribute and value table that is displayed, double-click the value and edit it.

    Click **Save**. An `Entry modified` message appears on the header of the pane.

    Delete an entry

    Click an entry in the directory tree navigation pane.

    Click **Delete**.

    Click **OK**.
7. Optional: Test the access to the directory server.

    a) Click **Login test**.

    b) Enter the password to verify the credentials.

Creating a flow

Create a flow that defines the relationship between the endpoints and the target Directory Server.

Before you begin

- Connect to a target directory server.
- Configure one or more endpoints.

Procedure

1. Click the **Flows** tab to view the **Flows** page.
2. On the **Flows** page, click **Add**.
3. In the **Add Flow** window, specify the **Name** for the flow.
4. From the **Select endpoint** list, select one of the configured endpoints to provide data for the flow.
5. Click **OK** to create the flow.

What to do next

Edit the flow to define the flow settings..

Defining flows

After you create a flow, you can edit the flow to define specific settings or use the default values that are provided for most settings.

Before you begin

Create a flow.

Procedure

1. To specify or modify the flow settings, on the **Flows** page, click the name of the flow and then click **Edit**.

   The configuration page for the selected flow is opened. You can view and edit the flow settings in the **Source** tab.
2. To change the endpoint, from the **Source** list, select one of the configured endpoints to provide data for the flow.
3. You can specify the flow settings that are grouped into the following categories:
   - General settings
   - User/Person settings
   - Group settings
   - Advanced settings

What to do next

If you want to delete a flow that is not required, close the configuration page for that flow. On the **Flows** page, click the name of the flow, and then click **Delete Flow**. Click **OK** when the confirmation message appears.

1. You can also configure the following enhancements for the flow:
   - Customize attribute maps
   - Define joins
   - Enable write-back

2. After you complete defining all of the flow settings, run the initial synchronization operation.
3. Then, either manually run incremental synchronization or schedule periodic synchronization.

Defining flow settings and filters

You must define flow settings to specify the target user and group containers and the container hierarchy. You can also specify filters to selectively process specific types of entries during migration and synchronization.

About this task

Flow settings are required. Filter settings are optional. If you do not specify any filters, all of the entries are processed during migration and synchronization.

Procedure

1. On the **Flows** page, click the name of the flow, and then click **Edit**.
2. On the **Source** tab, click **General Settings**.
3. Under **Types of Entries to Handle**, select the types of entries that you want to process for flow operations.

   By default, the options to **Handle Person entries** and **Handle Group entries** are both selected.
4. At **Mirror the source hierarchy into Directory Server** specify how you want to handle the hierarchy during synchronization.

   - Preserve the container hierarchy and copy the directory information tree structure from the endpoint to the target directory server during synchronization.

     a. Select the check box.

     b. In the **Target container in Directory Server** field, specify the search base in the target directory server, which is used as the root when mirroring the source hierarchy.
   - Flatten the hierarchy by pulling all entries from multiple containers in the endpoint into one specified container in the target directory.

     a. Clear the check box.

     b. In the **Target container for Users** field, specify the container under which you want to write the `Person` entries.

     c. In the **Target container for Groups** field, specify the container under which you want to write the `Group` entries.
5. Select **Debug log output** to generate detailed log messages with extra information, including errors about entries that are not processed or synchronized.
6. Optional: If you have LDAP endpoints, you can specify one or both of the following filtering criteria for entries during migration or synchronization.

   Enable filter based on group membership

   To migrate and synchronize only the members of specific groups, specify the groups under **User must be a group member of any of the following**.

   You can enter the group objects in the field or click **Add** to select from a list of available groups. The list contains all of the groups under the `OU` that is specified for the source endpoint.

   Enter each group on a separate line.

   Enable filter based on attribute values

   To migrate and synchronize only the entries that match a specific criteria, specify the attribute filters.

   a. Under **Attribute Filter**, select the attribute name from the list of available attributes.

   b. Select the operator from the list to specify the condition for applying the criteria, such as `equals`, `contains`, or `exists`.
   c. Enter the attribute value.

   You can specify a maximum of three attribute filters.

   By default, the AND logical condition ensures that the entry matches the criteria in all attribute filters because **Match any attribute filter** is cleared.

   To use the OR logical condition, where the entry matches any one of the criteria for attribute filters, select **Match any attribute filter**.

7. Optional: Specify further filtering details for entries that you want to include or exclude during synchronization.

   Enter one criteria on each line of the following fields. You can enter full DNs or partial texts.

   Include the following
   Specify the list of nodes in the endpoint that you want to synchronize.

   The values are used for substring searches in the returned entry DNs.

   Exclude the following
   Specify the list of nodes in the endpoint that you want to exclude when synchronizing.

Specifying user and group settings

Specify the source and target object classes and RDN attribute for `Person` and `Group` entries.

Procedure

User/Person settings

1. On the **Flows** page, click the name of the flow and then click **Edit**.
2. On the **Source** tab, click **User/Person settings**.
3. Typical default values are provided for the following settings, according to type of endpoint that you selected for the flow.

   Source Person Entry Object Class
   Specify the object class for `Person` entries in the endpoint.

   Target Person Entry Object Class
   Specify the entry that must be used for creating `Person` entries in the target directory.

   Source User RDN attribute
   Specify the attribute that is used as relative DN in the DN for the `Person` entries.

   Note: The attribute that is associated with this field cannot be customized in an attribute map. Use JavaScript in this field to manipulate the RDN.

   Target User RDN attribute
   The attribute to use as the RDN for entries that are written to Directory Server.

   Note: The attribute that is associated with this field cannot be customized in an attribute map. Use JavaScript in this field to manipulate the RDN.

Group settings

4. On the **Flows** page, click the name of the flow and then click **Edit**.
5. On the **Source** tab, click **Group settings**.
6. Typical default values are provided for the following settings, according to type of endpoint that you selected for the flow.

   Source Group Entry Object Class
   Specify the object class for `Group` entries in the endpoint.

   Target Group Entry Object Class
   Specify the entry that must be used for creating `Group` entries in the target directory.

Target Group Membership attribute

Specify the attribute for holding group membership in the target directory.

Configuring custom properties

You can specify custom properties to override the settings that are specified in the Federated Directory Server console.

About this task

You can use custom properties to override the settings that are specified in the Federated Directory Server console for endpoints, target directory server connections, or flows. You can also use custom properties to configure settings that are not available in the console.

Procedure

1. To specify custom properties, on the **Flows** page, click the name of the flow and then click **Edit**.
2. On the **Source** tab, click **Advanced Settings**.
3. In the **Custom properties** field, enter each custom property that you want to configure on a separate line.

   The following flow hooks, which are not available in the console, can be configured as custom properties:

   hook.onsuccess

   This hook is called when a flow completes successfully.

   hook.onfailure

   This hook is called when the flow stops due to an error.

   hook.onshutdownrequest

   This hook is called when a shutdown request is sent to the flow.

   hook.afterwrite

   The `afterwrite` hooks that you can configure through the console are only for successful write operation where the entry was modified. However, in custom properties, you can configure a non-qualified `afterwrite` hook, which is called when the write status succeeds, fails or is skipped. It can also be called when the operation results in an unchanged entry.

Example

The following examples show how you can use custom properties.

Specifying a custom property to override console settings

On the **General settings** page, you can enable **Debug log output** to generate detailed logs. To override this setting, enter the following custom property setting: `global.debug=true`.

Specifying a custom property that is not available in the console

The `onfailure` flow hook is not available in the Federated Directory Server console. You can use this flow hook to call an AssemblyLine when the flow stops due to an error. You can enable this flow hook by using the following custom properties:

```
hook.onfailure.AL=hookProject:/AssemblyLines/FlowFailure
hook.onfailure.enabled=true
```

Extending attribute maps for a flow

All flow relationships can contain advanced mapping and data transformation. When you set up a flow, you can specify the custom attribute maps that must be applied during the flow operations. You can choose from the attribute maps that you defined earlier for users and groups and extend those maps for a specific flow.

Before you begin

Customize attribute maps.

About this task

The custom attribute map is used to convert the attributes from the source endpoint schema to the corresponding attribute in the target schema.

Procedure

1. On the **Flows** tab, click the name of the flow and then click **Edit** to open the flow configuration page, if you did not already do so.
2. On the flow configuration page, click the **Attribute Maps** tab and then click **Person Objects** or **Group Objects** to view the custom mapping for users or groups.
3. From the **Select map for person objects** or **Select map for group objects** list, specify the map that you want to apply to the flow operations.

   The default is `person.map` for Person Objects and `group.map` for Group Objects.

   You can select another map from the list. The list includes both the ready-to-use custom attribute maps that are provided with Federated Directory Server and the maps that you customized earlier.
4. To extend the attribute mapping, take any of the following actions:

   Create an attribute mapping

   a. Click **Add Attribute**.

   b. Select the attribute from the list of attributes in the target directory server. A new row is displayed with the selected attribute name under **Directory Server Attribute**.

   Note: If the **Add Attribute** window does not display the list of attributes from the target directory, take the following actions:

   i) Under **Directory Server** in the navigation pane, go to **Connection Settings**.

   ii) Click **Test Connection**. Ensure that a green tick mark is displayed next to the name of the endpoint, which indicates that the connection is successful. This action also populates the fields that browse the target directory attributes.

   Modify an attribute mapping

   a. Under **Endpoint Attribute / Assignment**, double-click the default value to change the mapping and to specify more settings for the attribute mapping.

   b. Select **Enabled** to use this attribute mapping for the endpoint.

   c. Click **Simple Assignment** or **Scripted Assignment** to specify the type of mapping.

   Note: If you select **Scripted Assignment**, you can define the assignment by writing JavaScript code in the text field..

   Delete the mapping for a specific attribute

   a. Select the check box on the attribute row.

   b. Click **Remove Attribute**.

   c. Click **OK**.
5. Click **Save**. Unless you save each map that you edited, the changes are lost.

Results

As a precautionary measure, when you extend the custom attribute map, the changes are made in a copy of the original attribute map file. The new file is specific to this flow. It is named with the prefix `Flow_`*`flow_name`*. For example: `Flow_ADFlow_person.map`.

Configuring a join

To augment and enrich the data from the endpoint, you can configure the flow to specify a join from another data source selectively.

About this task

A flow can join data in one endpoint with data from another endpoint. For example, a database might contain information about people, which is not available in an LDAP directory. By joining the LDAP directory with the database, Federated Directory Server can show richer data about the people.

Whenever an entry comes in from the endpoint, the flow looks it up on the join data source, merges it with the data from the endpoint, and then adds to the target Directory Server.

Note: Only endpoints that support lookup can be used for a join. For example, endpoints like LDAP support lookup by using a certain criteria, hence they can be used for a join. File-based endpoints do not support lookup, hence cannot be used for join.

Procedure

1. On the **Flows** tab, click the name of the flow and then click **Edit** to open the flow configuration page, if you did not already do so.
2. Click the **Join** tab to view and edit the properties for the directory or data source for the join.
3. Select **Enabled** to apply the join to this flow.
4. From the **Select endpoint** list, select the endpoint that you want to use for the join. The **Select endpoint** list displays all the endpoints that you configured in Federated Directory Server. If you clear the **Enabled** check box, the **Select endpoint** field is disabled and the settings that you entered earlier are retained, but not applied during the flow operation.
5. Specify the action that must be taken when an error or failure occurs with an entry from the join during the flow operation. From the **On join failure** list, select one of the following options:

   - **Ignore error and continue** If you select this option, the error is ignored, the entry is added, modified, or deleted, and the flow operation continues with the next entry.
   - **Skip the current entry and continue** If you select this option, the entry that caused the error is skipped and the flow operation continues.
   - **Abort and terminate the flow** If you select this option, the flow operation is terminated at this entry.

   If you enabled **Debug log output** in **General Settings** on the **Source** tab, then you can view the details about the entries that caused errors.
6. You can choose to use a statement to specify simple criteria or a script for advanced criteria.

   - To specify simple criteria to find matching entries in the join, leave the **Scripted criteria** check box cleared and specify the criteria statement:
     - In the **Attribute** field, enter the attribute from the join endpoint.
     - From the **Operator** list, select the appropriate operator for the statement.
     - In the **Value** field, enter the corresponding attribute from the main endpoint.
   - To use a script to specify advanced criteria, select **Scripted criteria**. A field is provided where you can write the script for the criteria..
7. Under **Attribute Maps**, you can add, remove, or modify the attribute mapping for the join.

Create an attribute mapping

a. Click **Add Attribute**.
b. Select the attribute from the list of attributes in the target directory server. A new row is displayed with the selected attribute name under **Directory Server Attribute**.

   Note: If the **Add Attribute** window does not display the list of attributes from the target directory, take the following actions:

   i) Under **Directory Server** in the navigation pane, go to **Connection Settings**.
   ii) Click **Test Connection**. Ensure that a green tick mark is displayed next to the name of the endpoint, which indicates that the connection is successful. This action also populates the fields that browse the target directory attributes.

Modify an attribute mapping

a. Under **Endpoint Attribute / Assignment**, double-click the default value to change the mapping and to specify more settings for the attribute mapping.
b. Select **Enabled** to use this attribute mapping for the endpoint.
c. Click **Simple Assignment** or **Scripted Assignment** to specify the type of mapping.

   Note: If you select **Scripted Assignment**, you can define the assignment by writing JavaScript code in the text field or by calling a function in the `LDAPSync\customScript.js` file. For more information, see the IBM Security Directory Integrator documentation and search for *Scripting in IBM Security Directory Integrator*.
d. Under **Map when**, specify whether you want this mapping to be used for all operations, or only when either modifying an entry or creating an entry.
e. In the **Select Attribute** field, specify the attribute name in the source endpoint that must map to the target attribute.

Delete the mapping for a specific attribute

a. Select the check box on the attribute row.
b. Click **Remove Attribute**.
c. Click **OK**.

Enabling write-back for flows

Changes that are made in the target directory server can be propagated back to the endpoint by enabling write-back in a flow for selected attributes.

Before you begin

A global write-back option is provided as a safety feature, which you can use to turn off write-back for all flows. However, when you turn off the write-back feature globally, it prevents write-back for all flows, including the specific flows where you might want to enable write-back. Hence, you must first ensure that the write-back feature is enabled at a global level for all flows. See "Enabling or disabling global write-back" on page 10.

After you enable the global write-back feature, you must complete the steps in the following procedure to enable write-back for a specific flow.

About this task

Only the changes that are made to person entries that are targets of this flow are candidates for write-back operations.

Only the attributes that are selected as described in the following steps are handled by the write-back operations.

Procedure

1. To enable write-back for a specific flow, on the **Flows** tab, click the name of the flow and then click **Edit**.

   The configuration page for the flow is opened.
2. Click the **Write-back** tab.
3. Select **Enable** to enable the write-back option for this flow.
4. Specify the attributes in the directory server that must trigger a write-back operation and map it to the attribute in the endpoint.

   Create an attribute mapping

   a. Click **Add Attribute**.

   b. Select the attribute from the list of attributes in the target directory server. A new row is displayed with the selected attribute name under **Directory Server Attribute**.

      Note: If the **Add Attribute** window does not display the list of attributes from the target directory, take the following actions:

      i) Under **Directory Server** in the navigation pane, go to **Connection Settings**.

      ii) Click **Test Connection**. Ensure that a green tick mark is displayed next to the name of the endpoint, which indicates that the connection is successful. This action also populates the fields that browse the target directory attributes.

   Modify an attribute mapping

   a. Under **Endpoint Attribute / Assignment**, double-click the default value to change the mapping and to specify more settings for the attribute mapping.

   b. Select **Enabled** to use this attribute mapping for the endpoint.

   c. Click **Simple Assignment** or **Scripted Assignment** to specify the type of mapping.

      Note: If you select **Scripted Assignment**, you can define the assignment by writing JavaScript code in the text field or by calling a function in the `LDAPSync\customScript.js` file..

   Delete the mapping for a specific attribute

   a. Select the check box on the attribute row.

   b. Click **Remove Attribute**.

   c. Click **OK**.

Results

When a write-back operation happens, a summary of what was written back to the endpoint is displayed. The summary includes details such as the name of the flow, modified attributes, and the DNs of the directory server and endpoint is displayed. You can use the **Filter** field for searching the write-back summary.

Verifying the flow configuration

After you configure the flow and specify the criteria for the flow operations, you can run a simulated synchronization to verify the flow.

Before you begin

Ensure that you create and define a flow.

About this task

The simulated synchronization runs the same operations as an initial synchronization, but does not write anything to the directory server. This feature is helpful in the initial planning phase to verify that the flow is able to select the correct data subset in the endpoint.

Procedure

1. On the **Flows** page, click the name of the flow, and then click **Run Synchronization**.
2. In the **Run Synchronization** window, select **Simulate**.

Results

A complete synchronization from the source system is simulated according to the criteria specified for the flow.

A progress bar is displayed under the **Last Activity** column. The status and logs are displayed under the flow.

What to do next

If you want to stop the simulation operation that is in progress, click the name of the flow, and then click **Terminate**. Click **OK** when the confirmation message appears.

When the operation is completed, the details of the simulation such as date, operation, and modified attributes are displayed on a new tab. You can use the **Filter** field to search the table.

You can also check the status and logs to verify that the simulated synchronization was successful or to debug errors.

After you verify your flow by running a simulated synchronization, you can run the initial synchronization to migrate data to the directory server.

Synchronizing data on the target directory

After you define the flow settings you can synchronize data from the endpoint with the target Directory Server. You can do this either manually or set up a schedule for automated synchronization at regular intervals.

Running the initial synchronization

After you define the flow settings, you can run the initial synchronization to migrate data from the endpoint to the target Directory Server.

Before you begin

Ensure that you create and define a flow.

About this task

Initial synchronization is a one-time operation for a flow. It selects all entries in the endpoint that match the flow criteria and updates the directory server.

Procedure

1. On the **Flows** page, click the name of the flow, and then click **Run Synchronization**.
2. In the **Run Synchronization** window, select **Initial Synchronization**.

Results

A complete synchronization from the source system is started according to the criteria specified for the flow. Any current synchronization state data is reset.

A progress bar is displayed under the **Last Activity** column. The status and logs are displayed under the flow.

What to do next

If you want to stop a synchronization operation that is in progress, click the name of the flow, and then click **Terminate**. Click **OK** when the confirmation message appears. Terminating a flow operation leaves it in a partially synchronized state, so it must be used with caution.

When the operation is completed, you can check the status and logs to verify that the synchronization was successful or to debug errors.

After you ensure that the initial synchronization completed successfully, you can set up a schedule for synchronization at specific intervals.

Running incremental synchronization

After you run the initial synchronization, you can incrementally synchronize data on the target Directory Server based on the changes that are made in the endpoint. You can either run a manual synchronization or set up a schedule for automated synchronization at regular intervals.

Before you begin

- Create and define a flow.
- Run the initial synchronization for the flow.

Procedure

1. On the **Flows** page, click the name of the flow, and then click **Run Synchronization**.
2. In the **Run Synchronization** window, select **Incremental Synchronization**.

Results

The synchronization operation is started and a progress bar is displayed under the **Last Activity** column.

What to do next

If you want to stop a synchronization operation that is in progress, click the name of the flow, and then click **Terminate**. Click **OK** when the confirmation message appears. Terminating a flow operation leaves it in a partially synchronized state, so it must be used with caution.

When the operation is completed, you can check the status and logs to verify that the synchronization was successful or to debug errors.

To automatically run the synchronization at timed intervals, you can set up a schedule for synchronization at specific intervals.

Scheduling synchronization

You can specify a schedule to automatically run the incremental synchronization operation in a flow at timed intervals.

Before you begin

- Create and define a flow.
- Run the initial synchronization for the flow.

Procedure

1. To create a schedule for a flow operation for the first time, on the **Flows** page, under the name of the flow, click **No Schedule**. To edit a schedule that is already created, click the day and time of the next scheduled operation that is displayed under the flow.
2. In the **Schedule** window, click **Enabled** to activate the scheduler.

3. Select the type of schedule.
    - If you select **Timer**, the synchronization runs at the intervals specified in the schedule.
    - If you select **Keepalive**, the synchronization keeps running even if a timeout value is specified in the endpoint.
4. Select the frequency for the flow operation as either **Every Month** or **Selected Month(s)**. If you choose **Selected Month(s)**, the month names are displayed and you must select one or more months.
5. Select the days on which you want to run the flow operation from the following options: **Every Day**, **Weekdays** for specify days of the week, or **Selected day(s)** to specify the days of the month.
6. Under the **Hours/Minutes/Seconds** section, enter the time of the day when you want the flow operation to start. You can also enter the wildcard * (asterisk), a comma-separated list, or a range of numbers to specify hours, minutes, and seconds.

    For example:

    - To run the synchronization at the start of each hour, enter `*` in the **Hours** field, and then enter `0` in both the **Minutes** and **Seconds** fields.
    - To run the synchronization every 15 minutes in each hour, enter `*` in the **Hours** field, `0,15,30,45` in the **Minutes** field, and `0`, in the **Seconds** field.
7. Select **Enabled**.
8. If you anticipate that a flow operation might not complete before the next operation is scheduled to start, select **Don't start if already running**. This option is useful for operations that are of a longer duration because it prevents two instances of the same operation from running simultaneously.
9. If you want to stop the flow operation when it encounters a failure, select **Terminate schedule if assemblyline fails**.
    For example, you can enable this option to fix errors in the log file before a failed synchronization is automatically attempted repeatedly.
10. Click **Close** to save the schedule.

Results

The day and time of the next scheduled flow operation is displayed under the flow.

What to do next

If you do not want to use the scheduler in the future, you can clear the **Enabled** check box in the **Schedule** window.

Viewing logs and reports

After a synchronization activity is completed, you can view the logs to verify that it was successful.

About this task

On the **Flows** page, a summary of the flow operation is displayed under each flow with the following information:

- Number of users that were added, modified, and deleted
- Number of groups that were added, modified, and deleted
- The last activity that was run on this flow
- The total number of users and groups that were processed

When you define the general settings for the flow, if you selected the **Debug log output** option, then logs are generated with detailed information for debugging.

Procedure

1. To view the detailed logs, select the operation from the **Show logs from** list. The last operation is shown by default. You can select from any of the previous logs that are listed.

   Note: To change the number of historical log files that must be stored, see "Specifying the log settings" on page 12.

2. Click one of the following sections in the log to view a detailed report:

   Summary
   Displays the following summaries:

   - Number of Person, Group, and Container entries that were processed
   - Number of errors and warnings
   - Number of entries that were skipped and not successfully written to the target directory

   Error Log
   Displays all errors and warnings. You can use the details to troubleshoot any failures in the synchronization.

   Migration Log or Sync log
   If you are viewing the logs for the initial synchronization, the migration log is displayed, otherwise the log for synchronization operation is displayed. This log contains the details of the entire flow operation.

Monitoring

The Federated Directory Server console provides options to monitor the behavior and health of a flow.

The following options are available for monitoring:

- Security events can be sent to QRadar through Syslog. A security event is defined whenever an entry is added, modified, or deleted from the target directory server.
- Error events can be emitted as SNMP traps whenever an error occurs and is logged.
- If you enable custom monitoring, it is started immediately before the activation of any other hook, both standard and monitoring (QRadar and SNMP).

To configure the settings for monitoring, on Federated Directory Server navigation pane, under **Common Settings**, click **Monitoring**.

Configuring QRadar monitoring

Configure QRadar monitoring to track security events, which are when an entry is added, modified, or deleted in the target Directory Server.

Before you begin

Before you configure QRadar monitoring, you must ensure that the latest QRadar Direct Support Module (DSM) for Federated Directory Server is installed.

If you enabled **Auto Update** in your QRadar setup, QRadar automatically retrieves and installs new `rpm` files that are available when the system can access the internet. Hence, no action is required to obtain the Federated Directory Server DSM. See Configuring automatic update settings.

If the QRadar **Auto Update** feature is not enabled in your QRadar setup, you must obtain them the Federated Directory Server `rpm` files from IBM Fix Central and install it manually. Complete the following steps:

1. Download the following `rpm` files from IBM Fix Central:

   - `DSM-IBMFederatedDirectoryServer-`*`version`*`.noarch.rpm`
   - `DSM-IBMFederatedDirectoryServer-`*`version`*`.noarch.rpm`

For example:

- `DSM-IBMFederatedDirectoryServer-7.2-972015.noarch.rpm`
- `DSM-IBMFederatedDirectoryServer-7.1-972017.noarch.rpm`

2. Install the `rpm` files on your QRadar console.

   a. Log in to the system shell as `root`.

   b. Change directory to the directory to where you copied the `rpm` files.

   c. Run the command, `rpm -Uvh` *`rpm_filename`*.

   d. After the `rpm` files are installed, open the QRadar web user interface.

   e. Click the **Admin** tab.

   f. Click the **Deploy Changes**.

   The QRadar Direct Support Module (DSM) for Federated Directory Server is installed.

3. Configure the log source before events are received:

   a. Log in to QRadar.

   b. Click the **Admin** tab.

   c. In the navigation menu, click **Data Sources**.

   d. Click the **Log Sources** icon.

   e. Click **Add**. The **Add a log source** screen is displayed.

   f. Enter the log source configuration parameters.

   g. From the **Log Source Type** list, select `IBM Federated Directory Server`.

   h. From **Protocol Configuration** list, select `Syslog`.

   i. Enter the IP address or host name of the system that hosts Federated Directory Server, which appears in the syslog header of the events that are sent. If no header is being sent, use the IP address.

   j. Click **Save** to finish adding the log source.

   k. On the **Admin** tab, click **Deploy Changes** to deploy the new log source.

   Note: Auto-discovered log sources do not need to be deployed.

Procedure

1. In the Federated Directory Server console navigation pane, under **Common Settings**, click **Monitoring**.
2. On the **Monitoring** page, click the **QRadar** tab.
3. On the **QRadar** page, select **Enabled** to indicate that you want to monitor security events.
4. In the **Hostname** field, enter the host name or IP address of the QRadar server that must receive security events.
5. In the **Port** field, enter the port number on which the QRadar server must receive Syslog events.
6. From the **Severity** list, select the severity value for the Syslog event.
7. From the **Facility** field, select the facility value for the Syslog event.
8. In the **Map file** field, specify the path and file name of the map file sets up the various QRadar LEEF attributes for the event.
9. Click **Select...** to browse for the map file. The default value points to the `LDAPSync/QRadar.map` file.
10. Optional: In the **Date format mask** field, specify a standard Java `SimpleDateFormat` mask for date values that are written in mapped LEEF attributes.

This value controls both the value of the **`devTimeFormat`** attribute and the formatting of date values in the event. The default value is the ISO 8601 standard mask, `MMM dd yy HH:mm:ss`, which creates a string like `Oct 16 12 15:15:57`.

Configuring SNMP monitoring

Configure SNMP monitoring to track error events, which is whenever an error is logged during a flow operation.

Procedure

1. In the navigation pane, under **Common Settings**, click **Monitoring**.
2. On the **Monitoring** page, click the **SNMP** tab.
3. On the **SNMP** page, select **Enabled** to indicate that you want to monitor error events.
4. In the **Hostname** field, enter the host name or IP address of the SNMP monitor that must receive error events.
5. In the **Trap port** field, enter the port number on which the SNMP listens for traps.
6. In the **Community string** field, specify the community string that is used for the SNMP trap that is emitted.

   The SNMP community names serve as a weak form of authentication because devices that do not know the correct community name are precluded from SNMP operations. All messages that do not match this community string are discarded.

   If you leave it blank, then all community strings are accepted. The default value is `public`.
7. In the **Map file** field, specify the path and file name of the map file that sets up the various object identifiers (OIDs) that are passed in the emitted SNMP trap. The default value is `LDAPSync/SNMP.map`

Results

If enabled, the SNMP monitoring function passes the error message and the error level as `ERROR`, `WARN`, or `FATAL`.

What to do next

You can copy the `IBM-FDS-MIB.txt` from *`sdi_solution_dir`*`/LDAPSync` to your SNMP Server's MIB repository to enable SNMP server to correctly understand the SNMP messages that are sent by Federated Directory Server. Contact your SNMP Server administrator for help in configuring your SNMP device to use the Federated Directory Server MIB file.

Configuring custom monitoring

Use the custom monitoring option to do any number of actions at each active hook point during a flow operation.

About this task

If you configure custom monitoring, the specified AssemblyLine is called at all standard hook points in the flow operation. It is called before the actual flow hook's AssemblyLine is started, even if this hook is disabled.

Procedure

1. In the navigation pane, under **Common Settings**, click **Monitoring**.
2. On the **Monitoring** page, click the **Custom** tab.
3. On the **Custom** page, select **Enabled** to indicate that you want to monitor flow events by calling a custom AssemblyLine.

4. In the **Custom AssemblyLine** field, specify the AssemblyLine that you want to use for custom monitoring.

Results

Custom monitoring is started immediately before the activation of any other flow hook.

Configuring SCIM as the target

You can configure Federated Directory Server so that the central target repository is the System for Cross-Domain Identity Management (SCIM) instead of the default Directory Server.

About this task

To access the Federated Directory Server SCIM target console, you require IBM Security Directory Suite, Enterprise Edition.

Procedure

1. Log onto the IBM Security Directory Suite virtual appliance console. See Logging on to the virtual appliance console.
2. On the **Appliance Dashboard**, locate the **Server Control** widget. The Server Components column displays a list of all the servers.
3. Select **Federated Directory Server SCIM Target** from the list.
4. Click **Start** to start Federated Directory Server with SCIM as target.
5. After the Federated Directory Server SCIM Target is started, on the **Appliance Dashboard**, locate the **Quick Links** widget.
6. Click **Federated Directory Server SCIM Target** to open the console.

What to do next

Follow the Roadmap to use Federated Directory Server with SCIM as the target repository.

Known issues, limitations, and workarounds for Federated Directory Server

Use the problem descriptions and their solutions that are provided to resolve issues that you might encounter when you use Federated Directory Server.

Warning displayed when Active Directory is added as end point

When Active Directory is added as the end point in Federated Directory Server, the warning icon is sometimes displayed next to the Active Directory endpoint. The following warning message is displayed:

```
CTGDII886E Deleted objects cannot be read form the source.
```

This message is displayed because the Active Directory domain controller is not configured to allow deleted objects to be read. Refer to Microsoft documentation for the configuration steps that are needed to enable reading the `CN=Deleted Objects` branch of the Active Directory tree. The warning symbol is related to the setup of Active Directory domain controller or the authorization of the login that is being used when the end point is created in Federated Directory Server. For some Active Directory versions, the `CN=Deleted Objects` suffix needs to be explicitly made readable through LDAP.

Custom AssemblyLine cannot be used as endpoints or define joins in virtual appliance

In IBM Security Directory Suite virtual appliance, you cannot configure a custom AssemblyLine as an endpoint for Federated Directory Server.

AssemblyLines cannot be used to define the join operation in Federated Directory Server.

This limitation is a known limitation.

Quick Link for Federated Directory Server SCIM Target is not accessible

On the IBM Security Directory Suite virtual appliance console, in the **Quick Links** widget, at times the **Federated Directory Server SCIM Target** link is not accessible even though the service status is in the `started` state. To resolve this issue, you must restart the **Federated Directory Server SCIM Target** server in the **Server Control** widget.

In Federated Directory Server, the flows do not run as expected after migration

You might encounter issues when you run flows after you migrate Federated Directory Server with Directory Server as target by using the **`fdsmigr`** utility or Federated Directory Server with SCIM as target by using the **`fdsscimmigr`** utility. To avoid these issues, you must modify certain attributes in the respective `solution.properties` file, before you start the Federated Directory Server or Federated Directory Server SCIM Target.

For example, for Federated Directory Server with Directory Server as target, modify the following attributes in the `solution.properties` file:

1. `com.ibm.di.store.database=jdbc:derby://localhost:4527/$soldir$/TDISysStore;create=true`
2. `com.ibm.di.store.jdbc.urlprefix=jdbc:derby://localhost:4527/`
3. `com.ibm.di.store.port=4527`

The javax.net.debug property is not supported in IBM Security Directory Suite virtual appliance

If you set the **`javax.net.debug`** property to `true`, the java debug option is turned on. However, the **`javax.net.debug`** property is not supported in IBM Security Directory Suite virtual appliance. Hence, this property must not be set to `true` in any of the following `solution.properties` files:

- **Federated Directory Server property files** > **solution.properties**
- **SCIM Target property files** > **solution.properties**
- **SCIM Service property files** > **solution.properties**

If the **`javax.net.debug`** is set to `true`, the corresponding service does not run properly. This limitation is a known limitation.

Nested group membership might be lost during Initial synchronization

Problem

During initial synchronization, if a group is processed, which contains a member group that is not yet synchronized, then this member is treated as missing.

Solution

To ensure that all nested memberships are processed, rerun all groups that had missing members through the flow again after the initial synchronization. Also, defer any "Missing member" error messages until this final round of group handling.

Members from nested group are not migrated

If you specify a nested group in the **User must be a group member of any of the following** field, the entries from the nested group are not migrated during initial synchronization.

This issue is a known limitation and this scenario is not supported by Federated Directory Server.

Password cache allows authentication with old password

This issue is a known limitation with password cache for pass-through authentication in the following scenario:

1. You enable password cache.
2. A user authenticates and the password is stored on the target server.
3. You disable password cache.
4. The user changes the password on the source.

The user can still authenticate with the old password.

Initial synchronization fails after it retrieves Page Size values

Problem

On a Windows Server 2008 R2 system, the initial synchronization fails after it retrieves the values that are set by Page Size.

This problem is specific to operations that involve Active Directory.

Description

This problem occurs in the following scenario:

- The Active Directory on a Windows Server 2008 R2 system has many users and groups, for example, 10,000 users and 10,000 groups.
- The Page Size for the Active Directory endpoint is set to 500, which is the default value.
- A flow is defined to migrate these entries to Directory Server.

When you run the initial synchronization operation, 500 users are migrated and then an error occurs. Then, 500 groups are migrated and an error occurs. The operation is terminated with OperationNotSupportedException that is similar to the following error:

```
2013-06-12 16:37:31,250 ERROR [AssemblyLine.Flow_ADFlow1_ReadGroups_group.7]
     - [Flow_ADFlow1_ReadGroups_group/Read Groups/Default On Error]
     - [Flow_ADFlow1_ReadGroups_group/Read Groups/Default On Error]
     - javax.naming.OperationNotSupportedException: [LDAP: error code 12
     - 00002040: SvcErr: DSID-031401E7, problem 5010 (UNAVAIL_EXTENSION), data 0
]; remaining name 'ou=set1,dc=adsync,dc=tditest,dc=internal'
     - [LDAP: error code 12 - 00002040: SvcErr: DSID-031401E7,
     problem 5010 (UNAVAIL_EXTENSION), data 0
]
Stacktrace (for support):
javax.naming.OperationNotSupportedException: [LDAP: error code 12
     - 00002040: SvcErr: DSID-031401E7, problem 5010 (UNAVAIL_EXTENSION), data 0
]; remaining name 'ou=set1,dc=adsync,dc=tditest,dc=internal'
 at com.sun.jndi.ldap.LdapCtx.mapErrorCode(LdapCtx.java:3159)
 at com.sun.jndi.ldap.LdapCtx.processReturnCode(LdapCtx.java:3045)
 at com.sun.jndi.ldap.LdapCtx.processReturnCode(LdapCtx.java:2852)
 at com.sun.jndi.ldap.LdapCtx.searchAux(LdapCtx.java:1861)
 at com.sun.jndi.ldap.LdapCtx.c_search(LdapCtx.java:1784)
 at com.sun.jndi.toolkit.ctx.ComponentDirContext.p_search(ComponentDirContext.java:398)
 at com.sun.jndi.toolkit.ctx.PartialCompositeDirContext.search(PartialCompositeDirContext.java:368)
 at javax.naming.directory.InitialDirContext.search(InitialDirContext.java:287)
 at com.ibm.di.connector.LDAPConnector.getNextEntry(LDAPConnector.java:750)
 at com.ibm.di.server.AssemblyLineComponent.executeOperation(AssemblyLineComponent.java:3355)
 at com.ibm.di.server.AssemblyLineComponent.getnext(AssemblyLineComponent.java:932)
 at com.ibm.di.server.AssemblyLine.msGetNextIteratorEntry(AssemblyLine.java:3666)
 at com.ibm.di.server.AssemblyLine.executeMainStep(AssemblyLine.java:3375)
 at com.ibm.di.server.AssemblyLine.executeCycle(AssemblyLine.java:3151)
 at com.ibm.di.server.AssemblyLine.executeCycle(AssemblyLine.java:3091)
 at com.ibm.di.fc.AssemblyLineFC.executeCycle(AssemblyLineFC.java:451)
 at com.ibm.di.fc.AssemblyLineFC.perform(AssemblyLineFC.java:272)
 at sun.reflect.GeneratedMethodAccessor77.invoke(Unknown Source)
 at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:55)
 at java.lang.reflect.Method.invoke(Method.java:613)
 at com.ibm.jscript.types.JavaAccessObject.call(JavaAccessObject.java:321)
 at com.ibm.jscript.types.FBSObject.call(FBSObject.java:161)
 at com.ibm.jscript.ASTTree.ASTCall.interpret(ASTCall.java:175)
 at com.ibm.jscript.ASTTree.ASTAssign.interpret(ASTAssign.java:91)
 at com.ibm.jscript.ASTTree.ASTProgram.interpret(ASTProgram.java:119)
 at com.ibm.jscript.ASTTree.ASTProgram.interpretEx(ASTProgram.java:139)
 at com.ibm.jscript.JSExpression._interpretExpression(JSExpression.java:435)
 at com.ibm.jscript.JSExpression.interpretExpression(JSExpression.java:421)
 at com.ibm.jscript.JSExpression.evaluateValue(JSExpression.java:251)
 at com.ibm.jscript.JSExpression.evaluateValue(JSExpression.java:238)
 at com.ibm.jscript.JSExpression.evaluateValue(JSExpression.java:241)
 at com.ibm.jscript.JSInterpreter.interpret(JSInterpreter.java:57)
 at com.ibm.di.script.ScriptEngine.interpret(ScriptEngine.java:940)
 at com.ibm.di.script.ScriptEngine.interpret(ScriptEngine.java:925)
 at com.ibm.di.server.ScriptComponent.add1(ScriptComponent.java:244)
 at com.ibm.di.server.ScriptComponent.add(ScriptComponent.java:210)
 at com.ibm.di.server.AssemblyLine.msExecuteNextConnector(AssemblyLine.java:3759)
 at com.ibm.di.server.AssemblyLine.executeMainStep(AssemblyLine.java:3379)
 at com.ibm.di.server.AssemblyLine.executeMainLoop(AssemblyLine.java:2988)
 at com.ibm.di.server.AssemblyLine.executeMainLoop(AssemblyLine.java:2971)
 at com.ibm.di.server.AssemblyLine.executeAL(AssemblyLine.java:2940)
 at com.ibm.di.server.AssemblyLine.run(AssemblyLine.java:1319)

2013-06-12 16:37:31,250 ERROR [AssemblyLine.Flow_ADFlow1_ReadGroups_group.7]
     - [Flow_ADFlow1_ReadGroups_group/Read Groups/Default On Error]
     - Make sure that the search base is visible in the source system,
     for example from an LDAP browser.
Also ensure that the credentials defined for the Source connection are
     authorized to see entries in this container.
***** Start dumping: ERROR *****
                    class: 'javax.naming.OperationNotSupportedException'
            connectorname: 'Read Groups'
                exception: 'javax.naming.OperationNotSupportedException:
     [LDAP: error code 12 - 00002040: SvcErr: DSID-031401E7,
     problem 5010 (UNAVAIL_EXTENSION), data 0
]; remaining name 'ou=set1,dc=adsync,dc=tditest,dc=internal''
                  message: '[LDAP: error code 12 - 00002040: SvcErr: DSID-031401E7,
     problem 5010 (UNAVAIL_EXTENSION), data 0
]'
                operation: 'get'
                   status: 'fail'
***** End dumping: ERROR *****
***** Connector parameters: Read Groups *****
    ldapUrl: ldap://9.120.98.148:389
    ldapUsername: Administrator@adsync.tditest.internal
    ldapSearchBase: ou=set1,dc=adsync,dc=tditest,dc=internal
    ldapSearchFilter: objectClass=groupofuniquenames
    ldapSearchScope: subtree
    ldapSizeLimit: 0
    ldapPageSize: 500
    jndiExtraProviderParams: null
```

Solution

Complete the following steps to work around this issue:

1. On the Windows Server 2008 R2 Active Directory, apply the resolution in the Microsoft Knowledge Base website at http://support.microsoft.com/kb/977180.
2. Back up your Windows registry.
3. In the following registry setting, `HKLM\System\CurrentControlSet\Services\NTDS\Parameters`, add the string value `DSA Heuristics`.
4. Set the value to `000000000001`.
5. Restart the system.

Known issues and limitations with SCIM as target

The following known limitation exists when you deploy Federated Directory Server with SCIM as the target.

Entries with changes that are related to the DN are not processed correctly

This limitation exists in the following scenario:

The source endpoint is an LDAP server where there is no change log, for example, Active Directory. After you run the initial synchronization with SCIM as the target, changes related to the DN of an entry are made in the source endpoint. When you run an incremental synchronization, the `moddn` and `modrdn` operations do not work correctly. For example, if a user is moved to a container that is out of scope of the target, the changes are not processed correctly.

This issue does not occur when the source endpoint is a directory server that has change log.

File parsers reference

You can select and configure the appropriate file parser from the list that is provided in the file endpoint configuration page of the Federated Directory Server console.

CBE Parser for file endpoint

Use the CBE Parser to read XML from the input stream and convert this XML to a Common Base Event (CBE) object. When the CBE Parser reads from XML, it returns all standard CBE attributes and the CBE object as attribute of the Input Map.

To access the CBE Parser configuration parameters:

1. Add a File endpoint.
2. On the **File** endpoint configuration page, click **Parser** and select **CBE Parser** from the list.
3. Expand the **Parser** section to view the parameters.

Parameters

Comment
Use this field to add your comments. The comment is not considered while parsing data.

Detailed Log
Select this check box to generate detailed log messages with extra information.

You can also configure the following advanced parameters. Under the **Parser** section, expand **Advanced** to view these parameters.

Character Encoding
Specify the character encoding to use for reading or writing. The default value is `UTF-8`. When the parser reads from XML, this parameter is used only if the input source does not already have encoding defined.

The CBE Parser extends the XML Parser; therefore, the same character encoding rules apply. For more information, go to the IBM Security Directory Integrator documentation and search for *Character Encoding in the XML Parser*.

Validate XML
Select this check box to indicate that the parser must validate the XML with the XSD schema that is requested from the specification.

Omit XML Declaration
Select this check box to indicate that the parser must omit an XML declaration header in the output stream.

For detailed information about the CBE Parser and its input and output map attributes, go to the IBM Security Directory Integrator documentation and search for *CBE Parser*.

CSV Parser for file endpoint

Use the CSV Parser to read and write data in the comma-separated values (CSV) format.

To access the CSV Parser configuration parameters:

1. Add a File endpoint.
2. On the **File** endpoint configuration page, click **Parser** and select **CSV Parser** from the list.
3. Expand the **Parser** section to view the parameters.

Parameters

Field Separator
Specify the character that is used to separate each column, which is typically a comma or semicolon. The default value is a semi-colon (`;`).

Sort fields
Select this check box to write header fields in alphabetical (ascending) order. The default value is `false`.

Comment
Use this field to add your comments. The comment is not considered while parsing data.

Detailed Log
Select this check box to generate detailed log messages with extra information.

You can also configure the following advanced parameters. Under the **Parser** section, expand **Advanced** to view these parameters.

Field Names
Specify the name for each column to which the parser must read or write. You can use the **Field Separator** between the field names, or specify each name on a separate line.

The order in which you specify the column names controls the order in which the columns are written to the output file.

Enable Quoting
Select this check box to output with quotation marks during a write operation. This option is selected by default.

If you clear this check box, the field is output as is, which can cause problems. When reading, quotation marks around the field are stripped if the **Enable Quoting** check box is selected. The parser is able to read quoted attributes that contain the column separator. If **Enable Quoting** check box is cleared, the parser returns unexpected values when the input contains fields that are delimited by quotation marks.

Quote all fields
Select this check box to output all fields independently with quotation marks, if they contain quotation mark, separator, or a new line.

Write header
Select this check box to output all the field names that are separated by the column separate on the first line. This option is selected by default.

Write BOM
Select this check box to write Byte Order Marker (BOM) to the file. You must also select **Write header** for this option to take effect.

Log long lines
Specify a maximum number of bytes for a line. The line numbers of lines that are longer than this maximum number are logged.

Combine remainder in last field
Select this check box to combine all extra fields from lines that exceed the number of defined fields into a new **`Remainder`** field. The fields, and implicitly, the number of fields, are defined by **Field Names**, or its absence, the first line of the file.

Character Encoding
Specify the character encoding to use for reading or writing.

For more information, go to the IBM Security Directory Integrator documentation and search for *Character Encoding conversion*.

For detailed information about the CSV Parser and its schema, go to the IBM Security Directory Integrator documentation and search for *CSV Parser*.

DSMLv1 Parser for file endpoint

Use the DSMLv1 Parser to read and write XML documents. Directory Services Markup Language v1.0 (DSMLv1) enables the representation of directory structural information as an XML document. The Parser silently ignores schema entries.

To access the DSMLv1 Parser configuration parameters:

1. Add a File endpoint.
2. On the **File** endpoint configuration page, click **Parser** and select **DSMLv1 Parser** from the list.
3. Expand the **Parser** section to view the parameters.

Parameters

Comment
Use this field to add your comments. The comment is not considered while parsing data.

Detailed Log
Select this check box to generate log messages with detailed debug information.

You can also configure the following advanced parameters. Under the **Parser** section, expand **Advanced** to view these parameters.

DN Attribute
Specify the attribute that is used for the distinguished name DSML attribute. The default value is $dn.

DSML prefix
Specify the prefix that is used on XML elements to indicate that they belong to the DSML namespace. The default value is `dsml`.

DSML namespace URI
Specify the URI that identifies this namespace. The default value is `http://www.dsml.org/DSML`.

Omit XML Declaration
Select this check box to indicate that the parser must omit an XML declaration header in the output stream.

Document Validation
Select this check box to request file validation that is based on the specified DTD or schema.

Namespace Aware
Select this check box to indicate the parser must request a namespace-aware parser.

Character Encoding
Specify the character encoding to use for reading or writing. The default value is `UTF-8`.

The DSMLv1 Parser extends the Simple XML Parser; therefore, the same character encoding rules apply. For more information, go to the IBM Security Directory Integrator documentation and search for *Character Encoding in the Simple XML Parser*.

For detailed information about the DSMLv1 Parser and examples of its usage, go to the IBM Security Directory Integrator documentation and search for *DSMLv1 Parser*.

DSMLv2 Parser for file endpoint

Use the DSMLv2 Parser to parse and create DSMLv2 request and response messages. Directory Services Markup Language v2.0 (DSMLv2) provides a method for expressing directory queries and updates and the results of these operations as XML documents.

To access the DSMLv2 Parser configuration parameters:

1. Add a File endpoint.
2. On the **File** endpoint configuration page, click **Parser** and select **DSMLv2 Parser** from the list.
3. Expand the **Parser** section to view the parameters.

Parameters

Mode
Specify whether the parser operates in `Server` or in `Client` mode. In `Server` mode, requests are read and responses are written. In `Client` mode, requests are written and responses are read.

Comment
Use this field to add your comments. The comment is not considered while parsing data.

Detailed Log
Select this check box to generate detailed log messages with extra information.

You can also configure the following advanced parameters. Under the **Parser** section, expand **Advanced** to view these parameters.

Character Encoding
Specify the character encoding to use for reading or writing. The default value is `UTF-8`.

The DSMLv2 Parser extends the Simple XML Parser; therefore, the same character encoding rules apply. For more information, go to the IBM Security Directory Integrator documentation and search for *Character Encoding in the Simple XML Parser*.

Binary Attributes
Specify a comma delimited list of attributes that must be treated by the parser as binary attributes. A list of attributes are provided by default, which you can modify.

On Error
Specify how the server responds to failures while processing batch request elements. The valid values are `exit` and `resume`. The default value is `exit`.

Processing
Specify the value of the **`processing`** DSML attribute for batch requests. The valid values are `sequential` and `parallel`. The default value is `sequential`.

Response Order
Specify how the server orders individual responses within the batch response. The valid values are `sequential` and `unordered`. The default value is `sequential`. If you select `sequential`, the server must return a batch response in which the individual responses maintain a positional correspondence with the individual requests.

Omit XML Declaration
Select this check box to indicate that the parser must omit an XML declaration header in the output stream.

Indent Output
Select this check box to indent the output according to the depth of the statement lines. The result is cosmetic only; it has no bearing upon the semantic content of the output file.

Soap Binding
Select this check box to create SOAP DSML message. Otherwise, the DSML messages are not wrapped in SOAP.

For detailed information about the DSMLv2 Parser, its operations, attributes, and examples, go to the IBM Security Directory Integrator documentation and search for *DSMLv2 Parser*.

Fixed Record Parser for file endpoint

Use the Fixed Record Parser to read and write fixed-length text records.

To access the Fixed Record Parser configuration parameters:

1. Add a File endpoint.
2. On the **File** endpoint configuration page, click **Parser** and select **Fixed Record Parser** from the list.
3. Expand the **Parser** section to view the parameters.

Parameters

Column Description
Specify each column description as the field name, the offset, and length, which are separated by commas. This field is a multi-line field where you must specify one column description per line.

For example:

```
field1, 1, 12
field2, 13, 4
field3, 17, 3
```

Field names are displayed during schema discovery. The offsets start at 1; invalid values such as 0 might cause an exception.

Comment

Use this field to add your comments. The comment is not considered while parsing data.

Detailed Log

Select this check box to generate detailed log messages with extra information.

You can also configure the following advanced parameters. Under the **Parser** section, expand **Advanced** to view these parameters.

Trim values

Select this check box to remove leading and trailing spaces from fields during read operations.

Character Encoding

Specify the character encoding to use for reading or writing.

For more information, go to the IBM Security Directory Integrator documentation and search for *Character Encoding conversion*.

HTTP Parser for file endpoint

Use the HTTP Parser to interpret a byte stream according to the HTTP specification.

To access the HTTP Parser configuration parameters:

1. Add a File endpoint.
2. On the **File** endpoint configuration page, click **Parser** and select **HTTP Parser** from the list.
3. Expand the **Parser** section to view the parameters.

Parameters

Client Mode

Select this check box to indicate that the parser must operate in client HTTP response mode. If the **Client Mode** check box is cleared, the parser operates in server mode. This option is useful only if the parser is writing an output stream.

Comment

Use this field to add your comments. The comment is not considered while parsing data.

Detailed Log

Select this check box to generate detailed log messages with extra information.

You can also configure the following advanced parameters. Under the **Parser** section, expand **Advanced** to view these parameters.

Headers as Properties

Select this check box to retrieve and set the header values as properties. If this check box is cleared, the header values are read as attributes and returned as attributes.

Character Encoding

Specify the character encoding to use for reading or writing.

For more information, go to the IBM Security Directory Integrator documentation and search for *Character sets/Encoding*.

For detailed information about the HTTP Parser, its schema, and header fields, go to the IBM Security Directory Integrator documentation and search for *HTTP Parser*.

IdML Parser for file endpoint

Use the IdML Parser to parse the contents of an IdML (Identity Markup Language) file. It can be used for only reading IdML documents. It relies on the XML Parser for handling the IdML files and snippets.

To access the IdML Parser configuration parameters:

1. Add a File endpoint.
2. On the **File** endpoint configuration page, click **Parser** and select **IdML Parser** from the list.
3. Expand the **Parser** section to view the parameters.

Parameters

Comment
Use this field to add your comments. The comment is not considered while parsing data.

Detailed Log
Select this check box to generate log messages with detailed debug information.

You can also configure the following advanced parameters. Under the **Parser** section, expand **Advanced** to view these parameters.

Character Encoding
Specify the character encoding to use for reading or writing.

For detailed information about the IdML Parser and its schema, go to the IBM Security Directory Integrator documentation and search for *IdML Parser*.

JSON Parser for file endpoint

Use the JSON Parser to read and write entries in the JavaScript Object Notation (JSON) format. JSON is a lightweight data-interchange format and a subset of JavaScript programming language. JSON is built with the following two structures: an ordered list of values (array) and a collection of name-value pairs (object).

To access the JSON Parser configuration parameters:

1. Add a File endpoint.
2. On the **File** endpoint configuration page, click **Parser** and select **JSON Parser** from the list.
3. Expand the **Parser** section to view the parameters.

Parameters

Compact Output
Select this check box to display data in compact mode. Compact mode writes JSON data on a single unformatted line and is the default mode.

Character Encoding
Specify the character encoding to be used for reading or writing data.

Comment
Use this field to add your comments. The comment is not considered while parsing data.

Detailed Log
Select this check box to generate log messages with detailed debug information.

For detailed information about the JSON Parser, its objects and attributes, and examples of its usage, go to the IBM Security Directory Integrator documentation and search for *JSON Parser*.

LDIF Parser for file endpoint

Use the LDIF Parser to read and write data that is in the LDAP Data Interchange Format (LDIF). The LDIF format is used to specify a set of directory entries or a set of changes to be applied to directory entries, but not both. An LDIF file consists of a series of records that are separated by line separators.

To access the LDIF Parser configuration parameters:

1. Add a File endpoint.
2. On the **File** endpoint configuration page, click **Parser** and select **LDIF Parser** from the list.
3. Expand the **Parser** section to view the parameters.

Parameters

DN Attribute Name
Specify the attribute name to use for an LDIF dn line. The default value is $dn.

Version Number
Select this check box to display a version attribute in the beginning of the output (required by RFC2849). This check box is selected by default.

Comment
Use this field to add your comments. The comment is not considered while parsing data.

Detailed Log
Select this check box to generate log messages with detailed debug information.

You can also configure the following advanced parameters. Under the **Parser** section, expand **Advanced** to view these parameters.

Binary Attributes
Specify a comma delimited list of attributes that must be treated by the parser as binary attributes.

Character Encoding
Specify the character encoding to use for reading or writing. The default value is `UTF-8`.

For more information, go to the IBM Security Directory Integrator documentation and search for *Character Encoding conversion*.

Note: A conforming LDIF file must always have **Character Encoding** set to `UTF-8`. **Character Encoding** is also applied for encoding or decoding BASE64 encoded strings. BASE64 encoding looks like garbled text if you do not know how to decode it.

Only Descriptive Records
Select this check box to write only descriptive records. An LDIF file might contain change records or descriptive records. A change record describes a change that is needed for an entry. It can be identified by a `changetype` line, which is the second line immediately after the dn line. A descriptive record describes an entry. A correct LDIF file contains either only change records or only descriptive records.

By default, this check box is not selected.

Support language tags
Select this box if you want the parser to support language tags. When information is represented in multiple languages, the server associates language tags with attribute values.

For detailed information about the LDIF Parser, go to the IBM Security Directory Integrator documentation and search for *LDIF Parser*.

Line Reader Parser for file endpoint

Use the Line Reader Parser to read single lines of data from a file. The line that is read is returned in a single attribute. The attribute named `linenumber` contains the line number, starting with `1`.

Use the Line Reader Parser for reading text files only and not for binary files. If you want to copy a binary file, you can use the scriptable FTP object. For more information and examples of the FTP object, go to the IBM Security Directory Integrator documentation and search for *The FTP object*.

To access the Line Reader Parser configuration parameters:

1. Add a File endpoint.
2. On the **File** endpoint configuration page, click **Parser** and select **Line Reader Parser** from the list.
3. Expand the **Parser** section to view the parameters.

Parameters

Attribute Name
Specify the name of the attribute that contains the line of text either read or about to be written. The default value is `line`.

Comment
Use this field to add your comments. The comment is not considered while parsing data.

Detailed Log
Select this check box to generate log messages with detailed debug information.

You can also configure the following advanced parameters. Under the **Parser** section, expand **Advanced** to view these parameters.

Character Encoding
Specify the character encoding to use for reading or writing.

For more information, go to the IBM Security Directory Integrator documentation and search for *Character Encoding conversion*.

Script Parser for file endpoint

Use the Script Parser to write your own parser by using JavaScript.

To access the Script Parser configuration parameters:

1. Add a File endpoint.
2. On the **File** endpoint configuration page, click **Parser** and select **Script Parser** from the list.
3. Expand the **Parser** section to view the parameters.

Parameters

Script
Use this field to write the user-defined script to be run. A sample script is provided by default. For more information about the objects and functions that you can use in the script, go to the IBM Security Directory Integrator documentation and search for *Script Parser*.

You can also configure the following advanced parameters. Under the **Parser** section, expand **Advanced** to view these parameters.

External Files
If you want to include external script files at run time, specify them here, one file on each line. These files are run before your script.

Include Global Scripts
Select to include scripts from the Script Library.

Character Encoding
Specify the character encoding to use for reading or writing.

For more information, go to the IBM Security Directory Integrator documentation and search for *Character Encoding conversion*.

Comment
Use this field to add your comments. The comment is not considered while parsing data.

Detailed Log
Select this check box to generate log messages with detailed debug information.

For detailed information about the Script Parser, its objects, methods, and schema, go to the IBM Security Directory Integrator documentation and search for *Script Parser*.

Simple Parser for file endpoint

Use the Simple Parser to read and write entries that consist of attribute name and value pairs.

The entries are in the following format:

- Each line has one `attributename:value` pair.
- Multi-valued attributes use multiple lines.
- Lines with a single period mark the end of an entry.
- **`\r`** and **`\n`** in the value is an encoding of CR and LF line breaks.

To access the Simple Parser configuration parameters:

1. Add a File endpoint.
2. On the **File** endpoint configuration page, click **Parser** and select **Simple Parser** from the list.
3. Expand the **Parser** section to view the parameters.

Parameters

Comment
Use this field to add your comments. The comment is not considered while parsing data.

Detailed Log
Select this check box to generate log messages with detailed debug information.

You can also configure the following advanced parameters. Under the **Parser** section, expand **Advanced** to view these parameters.

Character Encoding
Specify the character encoding to use for reading or writing.

For more information, go to the IBM Security Directory Integrator documentation and search for *Character Encoding conversion*.

Simple XML Parser for file endpoint

Use the Simple XML Parser to read and write XML documents. It deals with XML data that is not more than two levels deep.

The Simple XML Parser uses the Apache Xerces and Xalan libraries. The parser gives access to the XML document through a script object called `xmldom`. The `xmldom` object is an instance of the `org.w3c.dom.Document` interface.

Note: The “XML Parser for file endpoint” on page 51 is the improved and enhanced XML Parser.

To access the Simple XML Parser configuration parameters:

1. Add a File endpoint.
2. On the **File** endpoint configuration page, click **Parser** and select **Simple XML Parser** from the list.
3. Expand the **Parser** section to view the parameters.

Parameters

Root Tag
Specify the root tag that encloses entries. The default value is `DocRoot`.

Entry Tag
Specify the name of the element for entries that are passed to the parser. The default value is `Entry`.

Value Tag
Specify the name of the element for attribute values that are passed to the parser. The default value is `ValueTag`.

Comment
Use this field to add your comments. The comment is not considered while parsing data.

Detailed Log
Select this check box to generate log messages with detailed debug information.

You can also configure the following advanced parameters. Under the **Parser** section, expand **Advanced** to view these parameters.

Omit XML Declaration
Select this check box to indicate that the parser must omit an XML declaration header in the output stream.

Document Validation
Select this check box to request file validation that is based on the specified DTD or schema.

Namespace Aware
Select this check box to indicate the parser must request a namespace-aware parser.

Character Encoding
Specify the character encoding to use for reading or writing. The default value is `UTF-8`.

For more information, go to the IBM Security Directory Integrator documentation and search for *Character Encoding in the Simple XML Parser*.

Indent Output
Select this check box to indent the output according to the depth of the statement lines. The result is cosmetic only; it has no bearing upon the semantic content of the output file.

For detailed information about the Simple XML Parser and examples of its usage, go to the IBM Security Directory Integrator documentation and search for *Simple XML Parser*.

Related information

W3C documentation at http://www.w3schools.com
Oracle Java API documentation at http://docs.oracle.com

SOAP Parser for file endpoint

Use the SOAP Parser to read and write SOAP XML documents.

The SOAP Parser converts SOAP XML documents to or from entry objects in the following manner:

- When the parser writes to the XML document, it uses attributes from the entry to build the document. The **SOAP_CALL** attribute is expected to contain the value for the SOAP call.
- When the parser reads from the XML document, the **SOAP_CALL** attribute is set to reflect the first tag that follows the `SOAP-ENV:Body` tag. For each attribute in the entry, a tag with that name and value is created. Each tag under the `SOAP_CALL` tag translates into an attribute in the entry object.

To access the SOAP Parser configuration parameters:

1. Add a File endpoint.
2. On the **File** endpoint configuration page, click **Parser** and select **SOAP Parser** from the list.
3. Expand the **Parser** section to view the parameters.

Parameters

Comment
Use this field to add your comments. The comment is not considered while parsing data.

Detailed Log
Select this check box to generate log messages with detailed debug information.

You can also configure the following advanced parameters. Under the **Parser** section, expand **Advanced** to view these parameters.

Omit XML Declaration
Select this check box to indicate that the parser must omit an XML declaration header in the output stream.

Document Validation
Select this check box to request file validation that is based on the specified DTD or schema.

Namespace Aware
Select this check box to indicate the parser must request a namespace-aware parser.

Character Encoding
Specify the character encoding to use for reading or writing. The default value is UTF-8.

For more information, go to the IBM Security Directory Integrator documentation and search for *Character Encoding conversion*.

For detailed information about the SOAP Parser and examples of its usage, go to the IBM Security Directory Integrator documentation and search for *SOAP Parser*.

SPMLv2 Parser for file endpoint

Use the SPMLv2 Parser to parse or write SPML Version 2 (SPMLv2) messages, which are individual SPMLv2 requests and responses.

SPMLv2 defines a core protocol over which different data models can be used to define the actual provisioning data. The combination of a data model with the SPML core specification is referred to as a profile. The use of SPML requires that a specific profile is used. This SPMLv2 Parser that is provided with Federated Directory Server console supports the SPMLv2 DSMLv2 profile.

To access the SPMLv2 Parser configuration parameters:

1. Add a File endpoint.
2. On the **File** endpoint configuration page, click **Parser** and select **SPMLv2 Parser** from the list.
3. Expand the **Parser** section to view the parameters.

Parameters

Comment
Use this field to add your comments. The comment is not considered while parsing data.

Detailed Log
Select this check box to generate log messages with detailed debug information.

You can also configure the following advanced parameters. Under the **Parser** section, expand **Advanced** to view these parameters.

Binary Attributes
Specify a comma delimited list of attributes that must be treated by the parser as binary attributes. A list of attributes are provided by default, which you can modify.

Character Encoding
Specify the character encoding to use for reading or writing. The default value is UTF-8.

The SPMLv2 Parser extends the XML Parser; therefore, the same character encoding rules apply. For more information, go to the IBM Security Directory Integrator documentation and search for *Character Encoding in the XML Parser*.

For detailed information about the SPMLv2 Parser, its operations and attributes, and examples of its usage, go to the IBM Security Directory Integrator documentation and search for *SPMLv2 Parser*.

XML Parser for file endpoint

Use the XML Parser to read and write XML documents. The XML Parser uses the XLXP implementation of the StAX (JSR-173) specification. StAX is a cursor-based XML Parser that can both read from and write to XML.

This XML Parser is much faster than the traditional DOM-based Simple XML Parser because it does not need to load the whole XML structure in memory like DOM does.

To access the XML Parser configuration parameters:

1. Add a File endpoint.
2. On the **File** endpoint configuration page, click **Parser** and select **XML Parser** from the list.
3. Expand the **Parser** section to view the parameters.

Parameters

Simple XPath

Specify the value that is used (an expression similar to XPath) to discover elements to interpret them as entries. This parameter is also used to display the structure of the XML document to be written.

Entry Tag

Specify the name of the element that holds each entry that is passed to the XML Parser.

Value Tag

Specify the name of the element that holds each attribute value that is passed to the XML Parser.

Comment

Use this field to add your comments. The comment is not considered while parsing data.

Detailed Log

Select this check box to generate log messages with detailed debug information.

You can also configure the following advanced parameters. Under the **Parser** section, expand **Advanced** to view these parameters.

Prefix to Namespace map

Specify the list of mappings between the prefix and namespace in the following format: *prefix=namespace*.

Separate each mapping with a vertical bar (|).

If the prefix starts with $, it is considered as a default namespace declaration.

The default value is `prefix=namespace`.

XSD Schema Location

Specify the schema location, which is used for display purposes only.

Character Encoding

Specify the character encoding to use for reading or writing. The default value is `UTF-8`.

For more information, go to the IBM Security Directory Integrator documentation and search for *Character Encoding in the XML Parser*.

Static Attribute Declarations

Specify the declarations for attributes and prefixes. They are written with the static elements that are specified in the **Simple XPath** field.

The following text is provided in this field by default:

```
<!-- this is an example for statically declared XML attributes/namespaces -->
<!-- DocRoot xmlns="defaultNS" attr1="val2">
<Entry xmlns:p1="p1NS" p1:attr2="val2" />
</DocRoot-->
```

Ignore repeating XML declarations while reading
Select this check box to always acknowledge the first XML declaration and to ignore the subsequent declarations.

Coalescing
Select this check box to coalesce adjacent character data sections.

Omit XML declaration when writing
Select this check box to suppress writing an XML declaration to the output. This option is useful for appending to an existing XML file.

Multi-rooted Document
Select this check box to output each entry as a stand-alone element, which creates a multi-rooted document.

Indent Output
Select this check box to indent the output according to the depth of the statement lines. The result is cosmetic only; it has no bearing upon the semantic content of the output file.

Permit invalid XML characters when writing
Select this check box to include the invalid XML characters in the XML tags. If this check box is not selected, an exception occurs during write operations on the XML document.

For detailed information about the XML Parser and examples of its usage, go to the IBM Security Directory Integrator documentation and search for *XML Parser*.

XML SAX Parser for file endpoint

Use the XML SAX Parser to read large XML documents that the DOM-based XML Parser cannot handle because of memory constraints. The XML SAX Parser is based on the Apache Xerces library.

The XML SAX Parser extracts data that is enclosed within the **Group tag** that you specify in the configuration. It creates an entry with the attributes that are present in the data.

To access the XML SAX Parser configuration parameters:

1. Add a File endpoint.
2. On the **File** endpoint configuration page, click **Parser** and select **XML SAX Parser** from the list.
3. Expand the **Parser** section to view the parameters.

Parameters

Group Tag
Specify the names of one or more XML group tags that enclose the entries. You can specify multiple tags by separating each tag name with a comma. If you do not specify a value, the root tag is used and the entire XML document is returned as a single entry.

Comment
Use this field to add your comments. The comment is not considered while parsing data.

Detailed Log
Select this check box to generate log messages with detailed debug information.

You can also configure the following advanced parameters. Under the **Parser** section, expand **Advanced** to view these parameters.

Remove prefix
Specify the prefix that you want to remove from the attribute names.

Ignore Attributes
Select this check box to ignore the attributes of the group tag and its child attributes.

Character Encoding
Specify the character encoding to use for reading or writing. The default value is `UTF-8`.

Document Validation
Select this check box to request file validation that is based on the specified DTD or schema.

Use XSD Validation
Select this check box to use XSD instead of DTD to validate the XML file.

Namespace Aware
Select this check box to indicate the parser must request a namespace-aware parser.

Read Timeout
Specify the number of seconds after which the parser stops if no data is received.

For detailed information about the XML SAX Parser and examples of its usage, go to the IBM Security Directory Integrator documentation and search for *XML SAX Parser*.

XSL-Based XML Parser for file endpoint

Use the XSL-Based XML Parser to parse XML documents in any format by using the XSL that you specify. The XML documents are parsed into attribute-value pairs and stored in the entry object.

To access the XSL-Based XML Parser configuration parameters:

1. Add a File endpoint.
2. On the **File** endpoint configuration page, click **Parser** and select **XSL-Based XML Parser** from the list.
3. Expand the **Parser** section to view the parameters.

Parameters

Comment
Use this field to add your comments. The comment is not considered while parsing data.

Detailed Log
Select this check box to generate log messages with detailed debug information.

You can also configure the following advanced parameters. Under the **Parser** section, expand **Advanced** to view these parameters.

Character Encoding
Specify the character encoding to use for reading or writing. The default value is UTF-8.

The XSL-Based XML Parser extends the Simple XML Parser; therefore, the same character encoding rules apply. For more information, go to the IBM Security Directory Integrator documentation and search for *Character Encoding in the Simple XML Parser*.

Indent Output
Select this check box to indent the output according to the depth of the statement lines. The result is cosmetic only; it has no bearing upon the semantic content of the output file.

Omit XML Declaration
Select this check box to indicate that the parser must omit an XML declaration header in the output stream.

Document Validation
Select this check box to request file validation that is based on the specified DTD or schema.

Namespace Aware
Select this check box to indicate the parser must request a namespace-aware parser.

To configure the input parameters, under the **Parser** section, expand **Input**.

Use Input XSL file
Select this check box to use an input XSL file. If you select this check box, the contents of the **Input XSL** field are ignored.

Input XSL File Name
Specify the path and file name of the input XSL file that contains the matching rules for transforming the user XML to the Federated Directory Server internal format.

Input XSL
Use this editable area to enter or paste the entire input XSL.

To configure the output parameters, under the **Parser** section, expand **Output**.

Use output XSL file
Select this check box to use an output XSL file. If you select this check box, the contents of the **Output XSL** field are ignored.

Output XSL File Name
Specify the path and file name of the output XSL file that has matching rules for transforming the Federated Directory Server internal format back to user XML.

Output XSL
Use this editable area to enter or paste the entire output XSL.

For detailed information about the XSL-Based XML Parser and examples of its usage, go to the IBM Security Directory Integrator documentation and search for *XSL based XML Parser*.

Federated Directory Server plug-in for IBM Security Access Manager

Configure this plug-in to use one or more directories as authentication sources for IBM Security Access Manager. For example, you can use Active Directory and Sun Directory Server as authentication sources, leaving the user administration and passwords in place in the respective identity stores.

The plug-in is based on the synchronization service that is provided by Federated Directory Server and the pass-through authentication feature of Directory Server. Federated Directory Server provides a ready-to-use browser interface to configure the synchronization of several identity stores with a central Directory Server instance. You can also use the Federated Directory Server browser console to configure pass-through authentication in Directory Server.

Federated Directory Server handles synchronization from a specific directory through a flow. You can configure a flow to do a callout after each entry is processed and written to Directory Server. At this post-operation feature, the Federated Directory Server plug-in for IBM Security Access Manager is attached to the required flows. Whenever a person or group entry is added, modified, or deleted in the target directory, the plug-in is called.

When the plug-in is called, the configuration parameters that are set in the Federated Directory Server console are passed to it. It then propagates the changes to identity information to IBM Security Access Manager as part of the flow operation.

IBM Security Directory Integrator is the system that powers the server-side functions of Federated Directory Server. Though previous experience with IBM Security Directory Integrator is not required, understanding this tool might make it easier to deploy and manage the Federated Directory Server solution. It helps you to use the hooks in Federated Directory Server to attach your own business logic with the various background federation processes that are running.

Note: The Federated Directory Server plug-in for IBM Security Access Manager is supported only for LDAP endpoints. Non-LDAP endpoints are not supported.

Roadmap for setting up the plug-in

To set up the plug-in, you must configure the required settings in the IBM Security Access Manager API, Directory Server, and Federated Directory Server.

The Federated Directory Server provides an identity federation service by keeping one or more identity stores synchronized with a central Directory Server instance.

Directory Server provides a pass-through authentication feature that you can configure through Federated Directory Server.

The Federated Directory Server plug-in for IBM Security Access Manager extends this solution by synchronizing user accounts and groups with IBM Security Access Manager.

The following roadmap specifies the steps in an end-to-end scenario for setting up the plug-in.

Table 2. Roadmap to set up Federated Directory Server plug-in for IBM Security Access Manager

Key steps	**More information**
Install the plug-in package.	"Installing the plug-in" on page 55
Generate the IBM Security Access Manager API properties file and specify values for the properties.	"Plug-in API properties file" on page 57
Log on to the Federated Directory Server console.	"Accessing the Federated Directory Server console" on page 6
Connect to Directory Server from Federated Directory Server.	"Connecting to Directory Server" on page 9
Configure a source endpoint for synchronizing with Directory Server. **Note:** The Federated Directory Server plug-in for IBM Security Access Manager is supported only for LDAP endpoints. Non-LDAP endpoints are not supported.	"Configuring endpoints" on page 13
Enable pass-through authentication in Directory Server.	Pass-through authentication
Configure pass-through authentication in Federated Directory Server.	"Configuring pass-through authentication" on page 11
Create a flow and define flow settings in Federated Directory Server.	"Creating a flow" on page 22 "Defining flows" on page 22
Attach the plug-in to a flow in Federated Directory Server and configure the plug-in properties.	"Configuring the plug-in properties" on page 58
Map the source endpoint attributes to the IBM Security Access Manager user and group entries.	"Mapping the attributes" on page 59
Run a simulated synchronization to test the flow.	"Verifying the flow configuration" on page 29
Run an initial synchronization to migrate data from the endpoint to the target Directory Server.	"Running the initial synchronization" on page 30
Test that the IBM Security Access Manager authentication works as required.	"Verifying the plug-in setup" on page 61
Create a schedule to automatically run incremental synchronization at timed intervals.	"Scheduling synchronization" on page 31

Installing the plug-in

You must make the IBM Security Access Manager API available to IBM Security Directory Integrator.

Before you begin

Install IBM Security Access Manager Version 6.1.1 or later.

Also, ensure that the Federated Directory Server target directory and the directory that is used by IBM Security Access Manager is the same Directory Server instance. Otherwise, manual configuration of Directory Server is required. If you added extended attributes to the IBM Security Access Manager schema in Directory Server, then you must add assignments to the `FDS_ISAM_Plugin.map` mapping file.

About this task

`sdi_solution_dir` is the IBM Security Directory Integrator Solution Directory, which is selected during installation and is in *`tdi_install_dir`*`/bin/defaultSolDir` script.

`tdi_install_dir` is the Directory Server installation directory.

Procedure

Make the IBM Security Access Manager API available to IBM Security Directory Integrator with either one of the following methods:

With IBM Security Access Manager	**Steps**
Virtual appliance	a. Download the `com.tivoli.pd.rgy.jar` file. On the IBM Security Access Manager appliance, log in to the local management interface. Go to **Custom File Management**. Under the `ISAM` folder, download `pdjrte-<version>.zip` file. After extracting this compressed file, browse to `pdjrte/java/export/rgy` folder and locate the `com.tivoli.pd.rgy.jar` file. b. Upload `com.tivoli.pd.rgy.jar` to the IBM Security Directory Suite virtual appliance by using one of the following methods. **Local management interface** i) Log in and go to **Configure Directory Suite** > **Advanced Configuration** > **Custom File Management**. ii) Select `CustomIn` directory. iii) Select the option to upload the `com.tivoli.pd.rgy.jar` file. **Command line interface** - Log in and enter the following command: *`sdsva.example.com>`*` sds client_tools idsgetfile -h` *`someothermachine.example.com`*` -u root` `-f <`*`SOME_BASE_PATH_TO_GET_JAR_FILE`*`/com.tivoli.pd.rgy.jar` The file is uploaded to the `CustomIn` directory on the virtual appliance. c. Modify the Federated Directory Server `solution.properties` file on the IBM Security Directory Suite virtual appliance. i) Log in and go to **Configure Directory Suite** > **Advanced Configuration** > **Update Property**. ii) From **Federated Directory Server Property Files** area, select `solution.properties`. iii) Click **New**. iv) Add the property name **`com.ibm.di.userjars`** and property value as `/userdata/directory/CustomIn/`. v) Click **Save Configuration**. d. Restart the Federated Directory Server from the local management interface dashboard server control panel.
On-premise software	- From the *`ISAM_install_dir`*`/java/export/rgy` directory, copy the `com.tivoli.pd.rgy.jar` file to the *`tdi_install_dir`*`/jars` directory.

With IBM Security Access Manager	Steps
	- Add *ISAM_install_dir*/java/export/rgy to the **com.ibm.di.userjars** property in the *sdi_solution_dir*/ solution.properties file.

What to do next

You must generate the configuration file that contains connection details for the IBM Security Access Manager API. See "Plug-in API properties file" on page 57.

Plug-in API properties file

Run the **com.tivoli.pd.rgy.until.RgyConfig** tool to create and set up the API properties file for the plug-in with the IBM Java runtime environment.

Note: An IBM Java runtime environment is in the *tdi_install_dir*/jvm/jre/bin folder.

Syntax

```
java -cp jars/com.tivoli.pd.rgy.jar
     com.tivoli.pd.rgy.util.RgyConfig properties_file_destination
     create Default Default "ldaphostname:389:readwrite:5"
     "DN" DN_password
```

Parameters

properties_file_destination

Specifies the full path to the file that is created when you run this command.

The default value is the following relative path: LDAPSync/ISAM_API.properties.

ldaphostname*:*port*:*settings

Specifies the following details:

- Host name of the LDAP server with which IBM Security Access Manager is configured. The LDAP server host name is specified in the IBM Security Access Manager runtime configuration file.
- Port number of the LDAP server. The default value is 389. You can change this value.
- The setting, which is :readwrite:5.

Enclose the entire value, *ldaphostname*:*port*:*settings*, in double quotation marks.

DN

Specifies the LDAP Distinguished Name (DN) for authenticating to IBM Security Access Manager. Enclose the value in double quotation marks.

DN_password

Specifies the corresponding password for the DN.

Example

```
java -cp jars/com.tivoli.pd.rgy.jar
     com.tivoli.pd.rgy.util.RgyConfig
     sdi_solution_dir/LDAPSync/ISAM_API.properties
     create Default Default "ldapSamServer:389:readwrite:5"  "cn=root" cnrootpassword
```

Default in the command statement corresponds to the IBM Security Access Manager domain with which it is to be integrated and the value that is set in the IBM Security Access Manager plug-in AssemblyLine parameters.

The result looks similar to the following properties file, where the property settings reflect the values that were specified when the **RgyConfig** tool was run.

```
#IBM IBM Security
Access Manager
#Mon Dec 03 10:40:06 MHT 2013
ldap.ssl-enable=false
ldap.bind-pwd={obf2}dwTRqM+riTiJyfwSscdYIsiAAb2aAXkqmJrtiJm2Hp4\=
ldap.bind-dn=cn\=root
ldap.mgmt-version=6.1.1
ldap.svrs=ldapSamServer \1:389\:readwrite\:5;
local_domain=Default
ldap.mgmt=true
mgmt_domain=Default
delFromRegistry=true
```

Complete the following for the configuration to take effect:

1. Copy the newly created `ISAM_API.properties` under the `CustomIn` folder by using the virtual appliance console.
2. On the Federated Directory Server console, when you configure the flow in the **Source** > **Flow Hooks** panel, specify the value for **isam.api.properties.filepath** as `/userdata/directory/CustomIn/ISAM_API.properties.`
3. On the virtual appliance console, restart Federated Directory Server in the **Server Control** widget.

Configuring the plug-in properties

Attach the plug-in to a flow in Federated Directory Server and specify values for the plug-in configuration properties.

Before you begin

Complete steps 1 - 8 in "Roadmap for setting up the plug-in" on page 54.

Procedure

1. In the Federated Directory Server console, on the **Flows** page, click the name of the flow and click **Edit**.
2. On the **Source** tab, click **Flow Hooks**.
3. Select **Enabled** to enable the feature for attaching AssemblyLines to flows.
4. Expand **User add/mod/delete** and select **Enabled** to indicate that this specific flow hook must call the AssemblyLine after each user is added, modified, or deleted.
5. Click **Browse** beside **AssemblyLine**.
6. In the browse menu, expand `FDS_ISAM_Plugin`, select `ProvisionISAM`, and click **OK**.
7. Specify the following properties to configure the plug-in:

   isam.api.properties.filepath

   Specify the path to the IBM Security Access Manager API properties file.

   The default value is `LDAPSync/ISAM_API.properties`.

   isam.domain

   Specify the IBM Security Access Manager domain that is to be integrated.

   This domain name must be the same as the domain used to create the IBM Security Access Manager API properties file.

   The default value is `Default`.

   isam.map.principalName

   Specify the mapping instruction for the `principalName` of the IBM Security Access Manager entry that corresponds to the current Person being synchronized.

   You can use one of the following special values:

- `targetRDN` specifies the target Person RDN.
- `sourceRDN` specifies the source Person RDN.

Otherwise, the value of this property must be the name of an attribute that is in the entry that is read from the source endpoint.

The default value is `targetRDN`.

Note: The setup for this solution requires that Federated Directory Server and IBM Security Access Manager share the same Directory Server instance. In this scenario, you must specify `targetRDN` as the value.

isam.map.secDN

Specify the mapping instruction for the `secDN` of the IBM Security Access Manager entry that corresponds to the current Person being synchronized.

You can use one of the following special values:

- `targetDN` specifies the target Person DN.
- `sourceDN` specifies the source Person DN.
- `mapFile` specifies that the map file handles secDN.

Otherwise, the value of this property must be the name of an attribute that is available in the entry that is read from the source endpoint.

The default value is `targetRDN`.

Note: The setup for this solution requires that Federated Directory Server and IBM Security Access Manager share the same Directory Server instance. In this scenario, you must specify `targetRDN` as the value.

isam.mapFile

Optional property that specifies the path and file name of the map file to be used.

As the Solution Directory is always the current working directory for IBM Security Directory Integrator, you can use a relative path such as `LDAPSync/FDS_ISAM_Plugin.map`.

The default value is `LDAPSync/FDS_ISAM_Plugin.map`.

Mapping the attributes

Map the source endpoint attributes to the IBM Security Access Manager user and group entries.

About this task

In the Federated Directory Server console, the flow configuration has an option to map attributes. However, if you try to modify the `FDS_ISAM_Plugin.map` on the **Attribute Map** tab of the flow configuration, the results might not be what you require. The changes that you make are not saved in the `FDS_ISAM_Plugin.map` file. Instead, the changes are saved in a copy of the `FDS_ISAM_Plugin.map` with a different file name that corresponds to the name of the flow. It might conflict with the configuration in the **Flow Hooks** page for the **`isam.mapFile`** property's value, which is usually `FDS_ISAM_Plugin.map`.

Procedure

1. In the Federated Directory Server console, under **Common Settings**, click **Attribute Maps**.

   The attribute maps in the *`sdi_solution_dir`*`/LDAPSync` directory are listed.
2. Select **FDS_ISAM_Plugin.map**. The attribute mapping table for the plug-in is displayed with default mapping.
3. Configure the attribute mapping for `FDS_ISAM_Plugin.map`. Follow the instructions in "Customizing attribute maps" on page 12. The minimum mapping that is required is the source `Person` attribute to be used for the `principalName` of its corresponding IBM Security Access Manager user. By default,

this value is set to the `UID` value from the source entry. The plug-in uses the `sAMAccountName` if `UID` is not found in the source entry, followed by `employeeCode`.

The following attributes are present in the default `FDS_ISAM_Plugin.map`:

cn
The common name of the user or group.

description
The description of the user or group.

secAcctValid
User entry flag that enables or disables the IBM Security Access Manager user account.

- `true` specifies that the account is disabled. The default value is `true`. This value must be `true` for pass-through authentication to work for provisioned IBM Security Access Manager user accounts.
- `false` specifies that the account is not disabled.

secPwdValid
User entry flag to indicate whether the **`userPassword`** attribute of the IBM Security Access Manager user is valid.

- `true` specifies that the account is disabled. The default value is `true`. This value must be `true` for pass-through authentication to work for provisioned IBM Security Access Manager user accounts.
- `false` specifies that the account is not disabled.

sn
The surname of the user.

All of the attributes might not be in the default `FDS_ISAM_Plugin.map` file. For example, **`userPassword`** is not required as passwords are not synchronized. Instead, authentication requests from IBM Security Access Manager are passed through to source endpoints by the pass-through authentication feature of the Directory Server. Some attributes are described in the following list:

secDN
The DN of the entry in the IBM Security Access Manager directory for both user and group entries. The **`isam.map.secDN`** property describes how this attribute is mapped. The map file entry is only used when the value of this property is set to `mapFile`.

member
uniqueMember
Attribute for user entries to specify an optional list of either principal names of IBM Security Access Manager users or their `secDN` values. These users are added to the IBM Security Access Manager security group if they exist as user entries.

If a value is determined to be a `secDN` value, the RDN of the DN is assumed to be the principal name of the user. If delta operation tags are set, any value that is tagged as `delete` is removed from group membership.

memberOf
Attribute for group entries to specify an optional list of IBM Security Access Manager security group names of which the user entry is a member.

This feature is provided for convenience. However, group membership is typically handled by mapping the `member` attribute of a user entry.

userPassword
Optional password for the IBM Security Access Manager user.

Results

The attribute mapping is saved to the `FDS_ISAM_Plugin.map` file in *`sdi_solution_dir`*`/LDAPSync` directory.

Verifying the plug-in setup

To test that the plug-in is working properly, you must verify the synchronized entries in the target Directory Server.

About this task

In the Federated Directory Server console, you can use the LDAP browser to verify entries in the target Directory Server. For more information, see "Browsing the directory entries" on page 9.

Procedure

1. Verify that the IBM Security Access Manager users were added by the plug-in. These user entries must appear under `SECAUTHORITY=instance name,cn=Users` container of Directory Server.
2. If you used `Default` as the IBM Security Access Manager instance, check under `cn=Users,SECAUTHORITY=DEFAULT` search base and search with `principalname=*` as the filter. Verify that each LDAP person entry that is synchronized to Directory Server is also represented as an IBM Security Access Manager user. The user's secDN must be pointing to the corresponding LDAP entry.
3. Use the credentials of a user that was synchronized to Directory Server, but where the original password for that user exists in the source directory. If the login works, then pass-through authentication is also functioning successfully.

Troubleshooting

Understanding the limitations, log files, and explanations for common errors can help you troubleshoot the Federated Directory Server plug-in for IBM Security Access Manager.

Known limitations

This solution uses the IBM Security Access Manager Registry Direct API. It does not support adding, modifying, or deleting Global Sign On (GSO) users.

Log files

You can view the log files on the Federated Directory Server console. On the **Flows** tab, click the *flow name* and select **View Logs**.

The IBM Security Access Manager synchronization process creates the following log file: `*flow*-ProvisionISAM.log`, where *`flow`* is the name of the synchronization flow that calls the plug-in to provision IBM Security Access Manager. A history of 50 older logs is also maintained. This log usually contains more details about the problem, including the `principalName` and `secDN` for the entry that is being synchronized.

The errors that are reported by the IBM Security Access Manager provisioning process are displayed in Federated Directory Server. The logs typically contain the text *afterwrite* or *post-write* in the logged message. The logged messages usually consist of two parts, with the Federated Directory Server error printed first and followed by a second message that indicates the root cause of the error.

For example, the following error might occur after write operations:

```
CTGDII761E Error invoking afterwrite Hook
```

Sometimes, the initial message also contains the Config and AssemblyLine name, which by default is `FDS_ISAM_Plugin:/AssemblyLines/ProvisionISAM`.

The last part of each error report provides insights to correct the problem.

Mandatory attribute is missing from output map
: The error message also includes the name of an attribute that is required by IBM Security Access Manager. You must update the map file to ensure that this value is returned.

CTGDIS047W Entry is not found

This error occurs only during incremental synchronization when a user is to be deleted from IBM Security Access Manager. It indicates that this user was not found in the IBM Security Access Manager registry.

CTGDKD262E Could not start Config Instance

This error occurs when the configuration XML file that contains the IBM Security Access Manager Provisioning AssemblyLine is not found in the `*sdi_solution_dir*/configs` folder. By default, this file is `FDS_ISAM_Plugin.xml`. Ensure that the configuration file is copied to this folder and try again.

HPDAA0321E The Distinguished Name does not map to an existing entry in the registry.
HPDAA0320E The Distinguished Name that is provided has incorrect syntax.

These error indicates that the `secDN` attribute value is invalid.

If you set the **`isam.map.secDN`** property to `compute`, then check the value of the **`isam.user.container`** property. This property contains the DN of an existing container in the IBM Security Access Manager directory where user entries are written. Also, ensure that the **`isam.map.secDN.type`** property is set to either `CN` or `UID`.

If **`isam.map.secDN`** property is set to `mapFile`, then ensure that the map file contains the `secDN` attribute. The mapping assignment must produce a syntactically correct DN value. Also, the suffix of the DN must refer to an existing container in the IBM Security Access Manager directory.

Chapter 2. System for Cross-Domain Identity Management administration

The System for Cross-Domain Identity Management (SCIM) is a standard that defines schema and protocol for identity management. You can use the SCIM service that is provided in IBM Security Directory Integrator with Directory Server as the backend directory. You can also use the SCIM connector to allow IBM Security Directory Integrator solutions to read and write to servers that support the SCIM protocol.

Overview

SCIM is emerging as a standard for user and group management and is often used instead of the traditional LDAP protocol. SCIM provides the flexibility that is required for HTTP REST, cross-enterprise, and cloud application deployments. As many cloud services do not offer an LDAP interface, you can use SCIM independent of the underlying protocols.

The SCIM protocol is an application-level, REST protocol for provisioning and managing identity data on the web. The protocol supports creation, modification, retrieval, and discovery of the core identity resources, which are users and groups, and also custom resource extensions.

Features

The SCIM specification is designed to make managing user identities in cloud-based applications and services easy, fast, and inexpensive.

SCIM provides the following features:

- It builds upon experience with existing schemas and deployments.
- It places emphasis on simplicity of development and integration.
- It applies existing authentication, authorization, and privacy models.

It aims to reduce the cost and complexity of user management operations by providing a common user schema and extension model. It also binds documents to provide patterns for exchanging this schema by using standard protocols.

For more information, see the SCIM website at http://www.simplecloud.info/.

Business scenarios

The SCIM protocol is often adopted for user and group management on non-LDAP systems. New applications, both inside the enterprise and in cloud-related scenarios, can use HTTP REST to abstract away the underlying technology.

SCIM can be used successfully in the following scenarios:

- Internal deployment of new identity services with SCIM as a provisioning protocol for long-term future use.
- Internal or external cloud where LDAP is unacceptable as protocol.
- Provisioning to SaaS applications that have SCIM as the user management interface.

For more information, see the SCIM website at http://www.simplecloud.info/ and search for *SCIM scenarios*.

SCIM service in IBM Security Directory Suite

The SCIM service in IBM Security Directory Suite provides a SCIM interface to the Directory Server and a SCIM connector for servers that use the SCIM protocol.

The backend to the SCIM server must be a Directory Server that contains the identity data. The SCIM server receives the SCIM requests and internally connects to the Directory Server to access the data to serve the requests.

The SCIM connector implements the SCIM protocol by using JavaScript and an HTTP Client Connector.

Supported software

The SCIM service adheres to the SCIM 1.1 specification. For more information, see the SCIM website at http://www.simplecloud.info/ and search for *specifications*.

Supported features

The SCIM service supports most of operation of SCIM version 1.1 with appropriate attention to changes in version 2.0.

The following features are supported in the current version of the SCIM service:

- Management of users and groups with Directory Server as the backend directory
- Schema: Enterprise user schema extension
- JSON data type
- GET/PUT/POST/DELETE requests
- PATCH: Modifying with PATCH (HTTP) request helps consumers to send only the attributes that require modification
- Pagination
- Authentication scheme: HTTP Basic
- Filtering enables consumers to use the **`filter`** query parameter to request a subset of resources.
- Partial resources enable consumers to use the **`attributes`** query parameter to specify the attributes that must be returned in resource representations
- Sorting allows consumers to specify the order in which the resources are returned.

The current version of the SCIM server does not support:

- OAuth authentication
- Bulk updates
- Automatic limitation of number of resources returned.

Note: To get the SCIM parameter **`active`** to work as intended, the password policy must be turned on in the Directory Server. To turn on the password policy, set **`ibm-pwdPolicy`** to `true` under `cn=pwdpolicy,cn=ibmpolicies`. This setting allows SCIM to read the **`ibm-pwdAccountLocked`** setting from Directory Server. For more information about setting the password policy, see the IBM Security Directory Suite documentationand search for *Setting password policy*.

Configuration files

Before you deploy the SCIM service, you must modify the configuration files to specify connection settings, user and group mapping, and schemas.

To modify the properties in the `SCIM.properties` file, take the following actions:

1. Log onto the IBM Security Directory Suite virtual appliance console. See Logging on to the virtual appliance console.

2. From the top-level menu of the virtual appliance console, select **Configure** > **Advanced Configuration** > **Update Property**.
3. On the Update Property page, click the **All Properties** tab.
4. In the left pane, click to expand **SCIM Service property files** section.
5. Click **SCIM/SCIM.properties**. The properties are displayed in the right pane.
6. Select a property.
7. Click **Edit**.
8. In the **Update Property** page, edit the **Property value**.
9. Click **Save Configuration**.

You can download the property files with default properties and values from IBM Security Directory Suite property files. These files include the properties that are listed in the following section, but might not be available for modification through the virtual appliance **Update Property** page.

SCIM.properties

The `SCIM.properties` file contains the following server system-specific properties, including details of the backend Directory Server.

Location
The externally accessible URL of the SCIM service. It affects only the location headers in SCIM replies.

httpPort
The port that the SCIM Service uses for listening. The SCIM Service always uses SSL.

LDAP.LookupLimit
uThe maximum number of resources that can be found by the SCIM Service. The default value is only 20000, to avoid memory overflow.

LDAPServer
The URL for the Directory Server that stores the user data.

LDAPServer.1
The URL for the first failover server. If more than one failover server is required, you can add **`LDAPServer.2`**, and so on.

userSearchBase
The Search Base for users in the Directory Server.

groupSearchBase
The Search Base for groups in the Directory Server.

userObjectClass
The list of object classes that are used when a user is created in the Directory Server.

groupObjectClass
The list of object classes that are used when a group is created in the Directory Server.

userSearchFilter
Used to find all users in the userSearchBase.

groupSearchFilter
Used to find all groups in the groupSearchBase.

dummyGroupMember
When new groups are created, if **`dummyGroupMember`** has a value and there are no members in the group, this value is added to avoid object violation error.

audit.log
Set this parameter to `true` to create audit logs.

audit.logFile
The name of the audit log file.

audit.logFileDatePattern
The date pattern specifies how often the log file is rolled over to a backup file. It also specifies how the date is appended to the log file name for the backup files that store previous logs.

audit.syslog
Indicates whether syslogging to QRadar® is enabled. Set the value to `true` to enable.

audit.QRadarHost
The host where QRadar is located.

audit.QRadarPort
The port number for QRadar.

audit.facility
The facility for the audit messages.

audit.eventID
The event ID to use in audit logs.

audit.devTimeFormat
The date format to use in audit logs.

mapTenantNames
Set this property to `true` to change the way that SCIM authentication is done. For more information and a list of properties that you can use if this property is `true`, see "Authentication of SCIM requests" on page 80.

TenantBase
The base DN to which containers are added in the LDAP server when a new tenant is added.

alltenants
Set this property to `true` to enable the `alltenants` endpoint.

usePasswordPolicy
If this property is det to `true`, it enables you to set and get password policy attributes for a tenant.

AuthenticationRealm
The realm that is presented to the user when asked for authentication.

authenticationEndpoint
If this property is set to `true`, it enables the authentication endpoint. The default value is `false`.

UserMapping.json and GroupMapping.json

The `UserMapping.json` and `GroupMapping.json` files specify the mapping between SCIM attributes and Directory Server user or group attributes. Each entry in these files contains an SCIM attribute name and an LDAP attribute name. The entry might also contain the following extra attributes.

ReadOnly
Specifies that the value is mapped only from LDAP to SCIM and not the other way.

WriteOnly
Specifies that the value is mapped only from SCIM to LDAP and not the other way. This entry must be used for password.

CreateDN
Specifies that the value is also used to create a distinguished name (DN) in the Directory Server, by appending the userSearchBase to the value. To be able to create new resources, there must be one entry with the **`CreateDN`** attribute, which uses a SCIM attribute name that is always provided.

Type
Provides the canonical type for a multi-valued attribute.

Conversion
Specifies a conversion of the attribute value. The conversion attribute can have one of the following values:

- **`DateTime`** converts the value from LDAP date format to SCIM date format.
- **`Group`** converts the value from an LDAP group to a SCIM group.

- **NewLines** converts the new lines in SCIM values to $ in LDAP values and vice versa.
- **IsActive** computes the active status for a user based on several operational attributes.
- **Boolean** converts from SCIM boolean to LDAP TRUE or FALSE.
- **InverseBoolean** converts from SCIM boolean to LDAP TRUE or FALSE, but TRUE maps to FALSE and vice versa.
- **MultiValued** indicates a multi-valued attribute with no canonical type.

Note:

- There must be only one map entry for each SCIM name, unless the entries have a unique **Type**.
- There must be only one entry for each LDAP name, unless the entries are **ReadOnly**.

UserSchema.json and GroupSchema.json

The `UserSchema.json` and `GroupSchema.json` files provide the schema definition of users or groups as per the SCIM specification. The attributes that are specified must match the attributes that are defined in the `UserMapping.json` and `GroupMapping.json` files.

ServiceProviderConfig.json
Defines the specification compliance, supported data models, authentication schemes, and so forth.

SCIM.xml
The configuration file that implements the SCIM service.

QRadarLogging.map

The `QRadarLogging.map` file specifies the values for attributes that are sent to the QRadar system when QRadar syslogging is enabled.

For more information, see the `Readme.txt` file in the `SCIM` folder in the *`sdi_solution_dir`* of IBM Security Directory Integrator installation.

Starting the SCIM service

Use the **Server Control** widget on the virtual appliance console to start the SCIM service.

Procedure

1. Log onto the IBM Security Directory Suite virtual appliance console. See Logging on to the virtual appliance console.
2. On the **Appliance Dashboard**, locate the **Server Control** widget. The Server Components column displays a list of all the servers.
3. Select **SCIM Service** from the list.
4. Click **Start** to start Federated Directory Server.

Logging and tracing

The logging and tracing feature of SCIM can help you to help find the cause of issues and resolve them.

You can set the **debug** parameter in the `SCIM.properties` file to `true` to increase the amount of data that is logged in the log files.

To configure audit logging, you can set the following properties in the `SCIM.properties` file.

audit.log
Indicates whether logging is turned on. Set the value to `true` to turn on the logging.

auditLogFile
Specifies the file name where the daily logging is done.

audit.logFileDatePattern
Specifies how often the log file must be rolled over to a new file. The default value is daily. The rollover happens only when the first message is logged in the new day. The logging is done by using a log4j DailyRollingFileAppender.

The logging is done in JSON format, where each line is one JSON object as shown in the following example:

```
{"url":"\/Users", "date":"2013-08-03 14:19:25,234","host":"127.0.0.1",
     "method":"POST","user":"cn=root",
     "resourceID":"cn=John Doe,ou=People,DC=EXAMPLE,DC=COM",
     "date":"2013-08-03 14:19:25,296","user":"cn=root","status":"201 Created"}
```

The JSON objects have the following attributes:

user
The user name that authorizes the request.

date
The date and time when the request was received.

remoteHost
The IP address of the host from which the request was received.

remotePort
The port from which the request came.

localHost
The local IP address.

localPort
The local port.

method
The method in the request.

url
The URL in the request.

userAgent
Name of the browser from which the request came, if available.

resourceID
The resource ID that was created or returned by the request.

status
The HTTP status that was returned.

Computation of active status of a user

You can compute the active status of a user based on several operational attributes.

In `UserMapping.json`, the conversion **`IsActive`** enables this computation.

The attribute **`accountLockedCode`** is included in the return body. This attribute is set if the active status is `false` and is a comma-separated list that contains the reasons why the account is locked. The following reasons are possible:

ibm-pwdAccountLocked
If the value of this attribute is `true`, it means that the account was administratively locked.

pwdAccountLockedTime
This attribute indicates that the account was locked for some reason and when the account was locked. For example, the account might be locked due to excessive login failures.

pwdChangedTime
This attribute indicates that the password expired and specifies when the password was last changed.

pwdFailureTime
: This attribute indicates too many failed login attempts and specifies the times that the failures occurred. It can be a temporary lock, which depends on the password policy.

SCIM object model

SCIM is built on an object model where a *Resource* is the common denominator and all SCIM objects are derived from it.

SCIM currently has three objects that directly inherit from the Resource object. The `ServiceProviderConfiguration` and Schema are used for discovery and contain no user information. The `CoreResource` object contains the user and group data within its two child resources, User and Group.

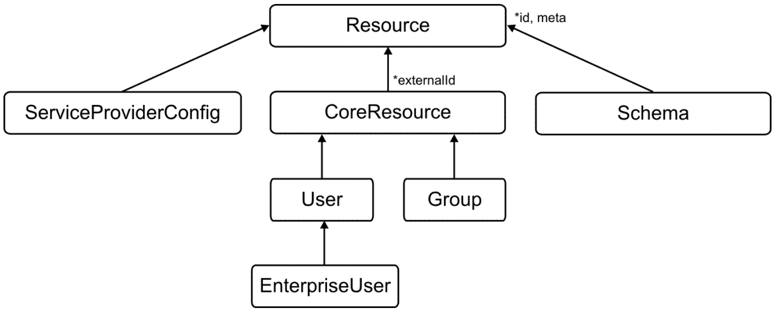


Figure 2. SCIM object model

Operations

SCIM provides a REST API with a rich but simple set of operations that you can use to manage resources.

The SCIM operations support everything from patching a specific attribute on a specific user to doing massive bulk updates.

Create
: `POST https://example.com/{v}/{resource}`

Read
: `GET https://example.com/{v}/{resource}/{id}`

Replace
: `PUT https://example.com/{v}/{resource}/{id}`

Delete
: `DELETE https://example.com/{v}/{resource}/{id}`

Update
: `PATCH https://example.com/{v}/{resource}/{id}`

Search

```
GET https://example.com/{v}/{resource}?filter={attribute}{op}{value}
    &sortBy={attributeName}&sortOrder={ascending|descending}
```

Bulk
: `POST https://example.com/{v}/Bulk`

Discovery operations

To simplify interoperability, SCIM provides two end points to discover supported features and specific attribute details.

`GET /ServiceProviderConfigs`
: Discovers specification compliance, authentication schemes, data models.

GET /Schemas

- GET /Schemas/User
- GET /Schemas/Group
- GET /Schemas/policy
- GET /Schemas/tenant

Introspects resources and attribute extensions.

Examples of SCIM operations

You can use the SCIM operations to search, create, modify, or delete users and groups in various scenarios.

Example 1

To get a list of all users, send the following request:

```
GET /users
```

Example 2

The following example shows how to get a list of all users but include only the **displayName** and **id** attributes. It also limits the result to the users from numbers 11 - 20.

Request:

```
GET /users?attributes=displayName,id&count=10&startIndex=11
```

Results:

```
{
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]
,
  "Resources":  [
        {
      "id":"7b401115-35f2-4a74-8384-a684cb4f31a1",
      "displayName":"Alexander Shelton"
    }
,
        {
      "id":"44216fbe-36a1-4215-b6f7-032775bc5e07",
      "displayName":"Andy Walker"
    }
,
        {
      "id":"c5292b7e-ffeb-4855-a086-7289d3445bd6",
      "displayName":"Alan White"
    }
,
        {
      "id":"5ad2d53c-9844-48ca-8460-c0d80fec5972",
      "displayName":"Alan Worrell"
    }
,
        {
      "id":"2b62e6a0-a698-4ffb-a107-1078b2d56437",
      "displayName":"Barbara Francis"
    }
,
        {
      "id":"3904d440-3f54-46cf-b63a-aacab03ac767",
      "displayName":"Bjorn Free"
    }
,
        {
      "id":"abb9526e-dfa8-452a-9d88-9eff3d79da90",
      "displayName":"Barbara Hall"
    }
,
        {
      "id":"d7df93df-d0bd-4c60-ad52-ec2bf8917fbc",
      "displayName":"Benjamin Hall"
    }
,
        {
      "id":"f98c9470-d7fe-490f-ab71-e84c9d3e9448",
      "displayName":"Barbara Jablonski"
    }
,
        {
      "id":"87fd1385-7d13-4423-851a-fb1d047bc2f0",
      "displayName":"Bjorn Jensen"
    }

  ]
,
  "totalResults":"163",
  "startIndex":"11",
  "itemsPerPage":"10"
}
```

Example 3

The following example gets a list of all users where the **`familyName`** starts with k.

Request:

```
GET /users?filter=name.familyName sw “k”
```

Results:

```
{
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]
,
  "Resources":  [
        {
      "id":"6f0fa17b-d988-4f95-98c0-095a545cc44e",
      "externalID":"aknutson",
      "meta":      {
        "created":"2013-04-16T09:14:02Z",
        "modified":"2013-04-16T09:14:02Z"
      }
,
      "userName":"uid=aknutson,ou=People,DC=EXAMPLE,DC=COM",
      "displayName":"Ashley Knutson",
      "name":      {
        "givenName":"Ashley",
        "familyName":"Knutson"
      }
,
      "phoneNumbers":      [
                {
          "type":"work",
          "value":"+1 408 555 2169"
        }
,
                {
          "type":"fax",
          "value":"+1 408 555 4774"
        }

      ]
,
      "emails":      [
                {
          "type":"work",
          "value":"aknutson@example.com"
        }

      ]

    }
,
        {
```

```
      "id":"6f7a3e28-db6c-4846-ae78-2346f39f65ee",
      "externalID":"ekohler",
      "meta":      {
        "created":"2013-04-16T09:14:02Z",
        "modified":"2013-04-16T09:14:02Z"
      }
,
      "userName":"uid=ekohler,ou=People,DC=EXAMPLE,DC=COM",
      "displayName":"Elba Kohler",
      "name":      {
        "givenName":"Elba",
        "familyName":"Kohler"
      }
,
      "phoneNumbers":      [
                {
          "type":"work",
          "value":"+1 408 555 1926"
        }
,
                {
          "type":"fax",
          "value":"+1 408 555 9332"
        }

      ]
,
      "emails":      [
                {
          "type":"work",
          "value":"ekohler@example.com"
        }

      ]

    }
,
        {
      "id":"e5318e13-1534-4eb9-9237-e1367a2744e1",
      "externalID":"skellehe",
      "meta":      {
        "created":"2013-04-16T09:14:02Z",
        "modified":"2013-04-16T09:14:02Z"
      }
,
      "userName":"uid=skellehe,ou=People,DC=EXAMPLE,DC=COM",
      "displayName":"Sue Kelleher",
      "name":      {
        "givenName":"Sue",
        "familyName":"Kelleher"
      }
,
      "phoneNumbers":      [
                {
          "type":"work",
          "value":"+1 408 555 3480"
        }
,
                {
          "type":"fax",
          "value":"+1 408 555 8721"
        }

      ]
,
      "emails":      [
                {
          "type":"work",
          "value":"skellehe@example.com"
        }

      ]

    }
,
        {
      "id":"3bac3d16-33ee-4a39-a6d1-063c5537530a",
      "externalID":"tkelly",
      "meta":      {
        "created":"2013-04-16T09:14:02Z",
        "modified":"2013-04-16T09:14:02Z"
      }
```

```
,
      "userName":"uid=tkelly,ou=People,DC=EXAMPLE,DC=COM",
      "displayName":"Timothy Kelly",
      "name":      {
        "givenName":"Timothy",
        "familyName":"Kelly"
      }
,
      "phoneNumbers":      [
                {
          "type":"work",
          "value":"+1 408 555 4295"
        }
,
                {
          "type":"fax",
          "value":"+1 408 555 1992"
        }

      ]
,
      "emails":      [
                {
          "type":"work",
          "value":"tkelly@example.com"
        }

      ]

    }

  ]
,
  "totalResults":"4"
}
```

Example 4

The following example shows how to search for the user with the **id** 2064f364-260b-4c29-8c28-b12583486ca3.

Request:

```
GET /users/2064f364-260b-4c29-8c28-b12583486ca3
```

Results:

```
{
  "id":"2064f364-260b-4c29-8c28-b12583486ca3",
  "externalID":"abergin",
  "meta":  {
    "created":"2013-04-16T09:14:02Z",
    "modified":"2013-04-16T09:14:02Z"
  }
,
  "userName":"uid=abergin,ou=People,DC=EXAMPLE,DC=COM",
  "displayName":"Andy Bergin",
  "name":  {
    "givenName":"Andy",
    "familyName":"Bergin"
  }
,
  "phoneNumbers":  [
        {
      "type":"work",
      "value":"+1 408 555 8585"
    }
,
        {
      "type":"fax",
      "value":"+1 408 555 7472"
    }

  ]
,
  "emails":  [
        {
```

```
      "type":"work",
      "value":"abergin@example.com"
    }

  ]
,
  "groups":  [
        {
      "value":"57a96228-48a6-4f29-a8ad-345828fccd6a",
      "display":"QA Managers"
    }

  ]
,
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]

}
```

Example 5

The following example shows how to get a list of all users created after a specified date.

Request:

```
    GET /users?filter=meta.created gt “2013-05-17T00:00:00Z”
```

Results:

```
{
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]
,
  "Resources":  [
        {
      "id":"78a13de7-0ef9-42ae-ba7c-b9c64a2050aa",
      "externalID":"wlutz2",
      "meta":      {
        "created":"2013-05-21T11:39:48Z",
        "modified":"2013-05-21T11:53:30Z"
      }
,
      "userName":"uid=wlutz2,ou=People,DC=EXAMPLE,DC=COM",
      "displayName":"Wendy Lutz",
      "name":      {
        "givenName":"Wendy",
        "familyName":"Lutz"
      }
,
      "phoneNumbers":      [
                {
          "type":"work",
          "value":"+1 408 555 3358"
        }
,
                {
          "type":"fax",
          "value":"+1 408 555 9332"
        }

      ]
,
      "emails":      [
                {
          "type":"work",
          "value":"wlutz@example.com"
        }

      ]

    }
,
        {
      "id":"a4cc7512-1530-4adc-952b-cd752aa79828",
      "externalID":"wlutz4",
      "meta":      {
        "created":"2013-05-21T11:54:12Z",
        "modified":"2013-05-21T11:54:12Z"
      }
,
      "userName":"uid=wlutz4,ou=People,DC=EXAMPLE,DC=COM",
      "displayName":"Wendy Lutz",
      "name":      {
        "givenName":"Wendy",
        "familyName":"Lutz"
      }
,
      "phoneNumbers":      [
                {
          "type":"work",
          "value":"+1 408 555 3358"
        }
,
                {
          "type":"fax",
          "value":"+1 408 555 9332"
        }

      ]
,
      "emails":      [
                {
          "type":"work",
          "value":"wlutz@example.com"
        }

      ]

    }
,
        {
      "id":"9be8c033-cf93-448e-a96b-d1290ff6d445",
      "externalID":"abergin2",
      "meta":      {
        "created":"2013-05-24T11:29:51Z",
        "modified":"2013-05-24T11:51:09Z"
      }
,
      "userName":"uid=abergin2,ou=People,DC=EXAMPLE,DC=COM",
      "displayName":"Andy Bergin Jr",
      "name":      {
        "givenName":"Andy",
        "familyName":"Bergin"
      }
,
      "phoneNumbers":      [
                {
          "type":"work",
          "value":"+1 408 555 8585"
        }
,
                {
          "type":"fax",
          "value":"+1 408 555 7472"
        }

      ]
,
      "emails":      [
                {
          "type":"work",
          "value":"abergin@example.com"
        }

      ]

    }

  ]
,
  "totalResults":"3"
}
```

Example 6

To create a user, send the following request:

```
    POST /users
```

The body must contain information about the new user in JSON format as shown in the following example:

```
{
      "externalID":"abergin2",
      "displayName":"Andy Bergin",
      "name":      {
        "givenName":"Andy",
        "familyName":"Bergin"
      }
,
      "phoneNumbers":      [
                {
          "type":"work",
          "value":"+1 408 555 8585"
        }
,
                {
          "type":"fax",
          "value":"+1 408 555 7472"
        }

      ]
,
      "emails":      [
                {
          "type":"work",
          "value":"abergin@example.com"
        }

      ]
}
```

Results:

```
200 OK
{
  "id":"9be8c033-cf93-448e-a96b-d1290ff6d445",
  "externalID":"abergin2",
  "meta":  {
    "created":"2013-05-24T11:29:51Z",
    "modified":"2013-05-24T11:51:09Z"
  }
,
  "userName":"uid=abergin2,ou=People,DC=EXAMPLE,DC=COM",
  "displayName":"Andy Bergin",
  "name":  {
    "givenName":"Andy",
    "familyName":"Bergin"
  }
,
  "phoneNumbers":  [
        {
      "type":"work",
      "value":"+1 408 555 8585"
    }
,
        {
      "type":"fax",
      "value":"+1 408 555 7472"
    }

  ]
,
  "emails":  [
        {
      "type":"work",
      "value":"abergin@example.com"
    }

  ]
,
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]

}
```

Example 7

The following example shows how to modify a user. It changes only the **`displayName`** of the user that was created in the previous example with id b9be8c033-cf93-448e-a96b-d1290ff6d445.

Request:

```
    PATCH /users/b9be8c033-cf93-448e-a96b-d1290ff6d445
```

The HTTP body must contain the following information:

```
    {
        "displayName":"Andy Bergin Jr"
    }
```

Results:

```
{
  "id":"9be8c033-cf93-448e-a96b-d1290ff6d445",
  "externalID":"abergin2",
  "meta":  {
    "created":"2013-05-24T11:29:51Z",
    "modified":"2013-05-24T11:51:09Z"
  }
,
  "userName":"uid=abergin2,ou=People,DC=EXAMPLE,DC=COM",
  "displayName":"Andy Bergin Jr",
  "name":  {
    "givenName":"Andy",
    "familyName":"Bergin"
  }
,
  "phoneNumbers":  [
        {
      "type":"work",
      "value":"+1 408 555 8585"
    }
,
        {
      "type":"fax",
      "value":"+1 408 555 7472"
    }

  ]
,
  "emails":  [
        {
      "type":"work",
      "value":"abergin@example.com"
    }

  ]
,
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]

}
```

Note: To test the operations with a browser that does not have a **PATCH** command, you can set the value of the HTTP header X-HTTP-Method-Override to PATCH. You can also use this setting to work around firewalls that block certain HTTP methods.

Example 8

The following example shows how to delete the user with **`id`** 2064f364-260b-4c29-8c28-b12583486ca3.

Request:

```
    DELETE /users/2064f364-260b-4c29-8c28-b12583486ca3
```

Results:

```
200 OK
```

Example 9

To get a list of all groups, use the following request:

```
    GET /groups
```

Example 10

The following example shows how to search for a specific group by its **`id`**.

Request:

```
    GET /groups/5653c887-1d5a-42cf-a470-6a2fe2608730
```

Results:

```
{
  "id":"5653c887-1d5a-42cf-a470-6a2fe2608730",
  "externalID":"Accounting Managers",
  "meta":  {
    "created":"2013-04-16T09:10:45Z",
    "modified":"2013-04-16T09:10:45Z"
  }
,
  "displayName":"Accounting Managers",
  "members":  [
        {
      "value":"71e064d4-3791-4ac8-b7c6-62686ce710cd",
      "display":"Sam Carter"
    }
,
        {
      "value":"6ba0ff5b-98b4-41c8-be28-331b99d94bde",
      "display":"Ted Morris"
    }

  ]
,
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]

}
```

Example 11

The following example shows how to search for a group by its **`displayName`**.

Request:

```
    GET /groups?filter=displayName eq “Accounting Managers”
```

Results:

```
{
  "id":"5653c887-1d5a-42cf-a470-6a2fe2608730",
  "externalID":"Accounting Managers",
  "meta":  {
        "created":"2013-04-16T09:10:45Z",
    "modified":"2013-04-16T09:10:45Z"
  }
,
  "displayName":"Accounting Managers",
  "members":  [
        {
      "value":"71e064d4-3791-4ac8-b7c6-62686ce710cd",
      "display":"Sam Carter"
    }
,
        {
      "value":"6ba0ff5b-98b4-41c8-be28-331b99d94bde",
      "display":"Ted Morris"
    }

  ]
,
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]

}
```

Example 12

The following example shows how to create a group.

Request:

```
POST /groups
```

The body must contain the information about the new group:

```
{
       "externalID":"Test Group",
       "displayName":"Test Group",
      "members":      [
     "5156d423-3c74-415b-844f-606a2aabafcc",
     "900faa78-d7c6-421c-9181-313134d17dd0"
      ]
    }
```

Results:

```
201 Created
{
  "id":"7e15ce9e-2fe7-4624-b5d5-adedc242e07a",
  "externalID":"Test Group",
  "meta":  {
    "created":"2013-05-27T02:37:38Z",
    "modified":"2013-05-27T02:37:38Z"
  }
,
  "displayName":"Test Group",
  "members":  [
        {
      "value":"5156d423-3c74-415b-844f-606a2aabafcc",
      "display":"Kirsten Vaughan"
    }
,
        {
      "value":"900faa78-d7c6-421c-9181-313134d17dd0",
      "display":"Robert Daugherty"
    }

  ]
,
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]

}
```

Authentication of SCIM requests

The SCIM authentication service extends the SCIM standard to enable authentication calls and user and group management.

All SCIM requests must be authenticated, unless they are a request for a `Schema` or `ServiceProviderConfig` object. If the request is not authenticated, a `401 Unauthorized` message is returned.

The authentication uses the typical HTTP basic authorization header, which contains a base64 encoding of a user name and password. This mechanism is the same as the process used by most browsers.

There are two scenarios for the authentication of credentials:

- In the `SCIM.properties` file, you do not specify the value of the property **`mapTenantNames`** as `true`. In this case, the user name must be an LDAP name that is known to the LDAP server that is a back-end server for the SCIM Services AssemblyLine. The user name and its corresponding password are sent to the LDAP server for verification.
- In the `SCIM.properties` file, you specify the value of the property **`mapTenantNames`** as `true`. In this case, you must specify some more properties that define this user name in the `SCIM.properties` file. For example, if the user name is `domain`, you can specify `domain.ldapName=cn=root`. It indicates that requests that come from the HTTP user name `domain` bind to the LDAP server with the user name `cn=root`. If this property is not specified, and the property **`tenantBase`** has a value, a HTTP user name is constructed with the pattern, `cn=Administrator,ou=domain, tenantBase`. For the password, if you specify `domain.password=Secret` and `domain.ldapPassword=VerySecret`, then the HTTP request password must be `Secret`, otherwise the authentication fails. The password that is sent to the LDAP server is `VerySecret`. If these two properties do not exist, then the password is sent to the LDAP server directly.

A request might also fail to be authorized if there are access limitations for the user `domain`. If the property **`domain.access`** does not exist or does not match the resource and method, then the request is not authorized. If you set **`mapTenantNames`** to `true`, this setting also enables you to use the access property for all users.

Access verification

If you set the **`mapTenantNames`** property to `true`, then all requests also verify the access rights of the user. For a request to be authorized, you must specify the **`domain.access`** property with a value that matches the requested resource and method. The **`domin.access`** property value must be comma-separated string of keywords. The default is no access. You can use the following keywords:

all
: All access is allowed.

createUser
: POST a user.

createGroup
: POST a group.

modifyUser
: PATCH or PUT a user.

modifyGroup
: PATCH or PUT a group.

deleteUser
: DELETE a user.

deleteGroup
: DELETE a group.

readUser
: GET on one or more users.

readGroup
GET on one or more groups.

auth
Authenticate a user with the non-standard endpoint or authentication.

superuser
Access to manipulate an new tenant endpoint. For more information, see the section, "SCIM superuser" on page 81.

For security reasons, the access control also verifies that the LDAP DN of the requested resource matches the LDAP search base.

The authentication endpoint

If you set the property `authenticationEndpoint=true` in the `SCIM.properties` file, a local extension to the SCIM protocol is enabled and user names can be authenticated.

Even the use of the authentication endpoint must be authorized. The `Authorization` header must contain a user name and password like any other SCIM request. This user name and password is described in the previous section. The authorization credentials are not directly related to the user that is to be authenticated. Specify the user to be authenticated with a filter, for example, `userName sw "Je"`, where `sw` means `starts with`. The authentication service looks up this user with the help of the authorization credentials. Exactly one user must match the filter criteria. Then, the service uses the DN from this user with a password that is specified in an `Authentication-Password` header to try to bind to the LDAP server. The attempt results in one of the following outcomes:

- If the bind succeeds, a `204 No Content` reply is returned.
- If the authentication fails because the user does not exist or the password does not match, a `403 Forbidden` reply is returned.
- If the `Authentication-Password` header is not present, a `403 No Password` reply is returned.

Access the authentication endpoint with the endpoint name `authentication` as shown in the following example request:

```
GET /authentication?filter=userName eq "Some User"
Authorization: Basic  QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Authentication-Password: secret
```

SCIM superuser

If you specify the keyword `superuser` for a tenant using the SCIM service, that tenant has superuser access. A value of `all` does not give superuser access.

A superuser is allowed to manipulate a new tenant endpoint, including the following operations:

POST

Add a new tenant.

The new **`tenantName`** is given in the JSON payload.

The **`tenantName`** and the **`password`** may be used in the basic authentication header in subsequent SCIM calls to log in as the tenant.

The payload must also include the **`password`**. For example:

```
{
    "tenantName": "someName",
    "password": "secret"
}
```

If the operation is successful, the status returned is `201 Created`, or else an error status is returned. The return body contains the tenant information in the same format as the GET tenant operation.

DELETE

Delete a tenant.

The tenant name must be given in the URL. For example:

```
DELETE /Tenant/someName
```

If the operation is successful, the status returned is `200 OK`, or else an error status is returned. The return body is similar to the following example:

```
{ "result": "OK" }
```

.

GET

Check whether a tenant exists.

The tenant name must be given in the URL. For example:

```
GET /Tenant/test2
```

If the tenant exists, the status returned is `200 OK`. The reply body is similar to the following example:

```
{
  "tenantName":"test2",
  "enabled":true,
  "baseDn":"ou=test2,o=sample",
     "tenantAdminDn":"cn=Administrator,ou=test2,o=sample",
     "passwordPolicyDn":"cn=test2,cn=ibmPolicies"
}
```

The verification of the superuser follows the usual rules. You can specify the password in `SCIM.properties`. In that case, the given password is verified against the password specified in `SCIM.properties`. If the password is not specified in `SCIM.properties`, the LDAP server verifies the password.

The superuser can also pretend to be another tenant for purpose of user administration. Specify a value for the HTTP header `TenantName`. When the superuser pretends to be another tenant, access is granted according to the access rights of that tenant.

`AddTenant` adds the following containers in the LDAP server:

```
ou=tenantName, base
ou=users, ou=tenantName, base
ou=groups, ou=tenantName, base
```

Where,

base is specified by the property **`TenantBase`** in `SCIM.properties`. The base must be an existing container in the LDAP server. The name of the first of these containers is returned in the **`baseDn`** attribute.

`AddTenant` also add a person to the LDAP server with the specified password:

```
cn=Administrator, ou=tenantName, base
```

This person is also set to be the owner of the `ou=tenantName,` *`base`* container, with **`ownerpropagate`** set to `true`.

Also, this is the person who is used in the bind operation to the LDAP server, so that the tenant operations are done with the access rights of this user.

If the property **`usePasswordPolicy`** is set to `true`, **`AddTenant`** also adds a password policy to the LDAP server. For example:

```
cn=tenantName,cn=ibmPolicies
```

The policy initially contains only the required attribute **pwdAttribute**. A new group is also created. For example:

```
cn=allUsers, ou=tenantName, base
```

This group has **ibm-pwdGroupPolicyDN** that points to the password policy. All new users for this tenant are added to this group. In this way, all the users have this password policy applied to them.

Note: The properties **ldapName** and **ldapPassword** must be defined in the SCIM.properties file. These properties are the credentials that are used for tenants, unless some tenants have specified other values for these properties. The superuser might use different LDAP credentials, with a relatively higher ACL.

Enabling or disabling tenants

The LDAP attribute **ibm-pwdAccountLocked** is used to mark a tenant as disabled.

Use the PATCH method on the tenant endpoint. For example:

```
PATCH /tenant/tenantName
```

Use the following body with this operation:

```
{ "enabled": false }
```

If the operation is successful, the status returned is 200 OK and the body becomes the new tenant information.

Password policy for tenants

To be able to set and get password policy attributes for a tenant, the following property must be set in SCIM.properties:

```
usePasswordPolicy=true
```

Also, in the LDAP server, the **ibm-pwdGroupAndIndividualEnabled** and **ibm-pwdPolicy** attributes must be set to true in the global password policy.

When a tenant is created, a default or empty password policy is created for that tenant and a tenant specific group is set up with **ibm-pwdGroupPolicyDN** pointing to that policy. All the users of the tenant are created as members of that group, so that the password policy is applied to them.

The following three methods are applicable to the tenant endpoint:

GET

```
GET /policy/tenantName
```

If the operation is successful, the status returned is 200 OK, and the body becomes the password policy for that tenant.

PATCH

```
PATCH /policy/tenantName
```

This operation modifies the password policy for a tenant. The body must contain the new values for the policy attributes that need to be changed.

If the operation is successful, the status returned is 200 OK, and the body becomes the modified password policy for that tenant.

PUT

```
PUT /policy/tenantName
```

This operation replaces the password policy for a tenant. The body must contain all the new values for the policy attributes that need to be changed. Existing attributes that are not present in the body are deleted.

If the operation is successful, the status returned is `200 OK`, and the body becomes the modified password policy for that tenant.

Schemas

The following schemas are used for tenant and tenant password policy.

- `GET /Schemas/tenant` gets the schema for a tenant.
- `GET /Schemas/policy` gets the schema for a tenant password policy.

The `alltenants` endpoint

To enable the `alltenants` endpoint, you must set `alltenants=true` in `SCIM.properties`.

Superuser access is required to use this endpoint.

This endpoint supports the following methods.

GET

```
GET /alltenants
```

This operation returns all tenants in the same format as `GET /users`.

There is a `Resources` array inside the JSON body, which contains all the tenant objects.

Pagination can also be used in the same way as for users.

DELETE

```
DELETE /alltenants
```

This operation deletes all tenants and all their information.

⚠ **CAUTION:** There is no undo, so be careful when you use this command.

The return body is similar to the `GET /alltenants`, except that every tenant also has a **`deleted`** attribute, which is set to `true` if the tenant was successfully deleted. If the deletion was not successful, it contains an error string.

There is no pagination for this command. The command might take a long time to complete, up to many hours if the tenants have thousands of users.

The `apiusers` endpoint

Use the `apiusers` endpoint to create users who can use the API for user administration.

This endpoint supports the following methods.

GET

```
GET /APIusers
```

This operation returns all API users in the same format as `GET /users`.

There are two attributes for each API user:

name
The name that is used to log in to SCIM.

DN
An LDAP DN that can be used in LDAP.

```
GET /apiuser/name
```

This operation returns the api user with the specified name.

POST

```
POST /APIusers
```

This operation adds an API user.

The body must contain two attributes, **name** and **password**.

```
{
  "name":"someName",
  "password":"secret:"
}
```

This name and password is used by the new API user later to log in to SCIM.

The body might contain more attributes, such as `API key`, `role`, or `access`.

PATCH

```
PATCH /APIuser/username
```

This operation modifies the API user.

The body must contain the attributes that need to be changed, for example, the `password`.

DELETE

```
DELETE /APIusers/username
```

Deletes the specified API user.

In SCIM, when the API users log in to SCIM, they must provide their name and password in the usual HTTP Basic Authentication header. They must also provide an HTTP Header `TenantName` containing the tenant name for the SCIM Service to know which tenant they represent. An API user can do everything that a user can do, except administer API users.

In LDAP, the new API users are person objects that are stored in a container that is named `ou=API,ou=<tenantname>,<tenantBase>`. To give the new API users the correct access rights in LDAP, an **`aclEntry`** attribute is added to the user and group container for each tenant, with the following value:

```
group:groupName:normal:rwsc:system:rsc:restricted:rsc:object:ad:at.userpassword:rwsc
```

Where, `groupName` is a new group that contains all the API users for that tenant.

HTTP response codes

The HTTP response codes that are returned for successful operations and errors are described here.

Successful operations

200 OK
The operation was completed successfully.

201 Created
The user or group was created successfully.

204 No Content
An authentication request was successful.

Errors

400 Bad Request

The path portion is missing in the URL.

Change of a constant endpoint was attempted, for example, the schema.

The endpoint is unknown.

A POST request (create user or group) with no external ID was provided.

ID was not provided in a modify (PUT, PATCH, or DELETE) request.

An exception occurred during an attempt to parse the request.

No HTTP body was included in a modify (PUT or PATCH) request.

The HTTP body could not be parsed as JSON in a modify (PUT or PATCH) request.

An ID provided in a group member attribute could not be converted to an LDAP DN.

A search filter could not be parsed successfully.

401 Unauthorized

No credential was provided.

The credentials (user name or password) were not correct.

An attempt was made to modify a user that is outside the scope for this user name.

This user has no access rights.

This user is not allowed to do the attempted operation.

403 Forbidden

An attempt was made to authenticate a user that does not exist.

The password that was provided for authentication of a user was not correct.

403 No Password

An attempt was made to authenticate a user, but the password was not provided in the "Authentication-Password" HTTP header.

404 Not Found

Request was made for unknown schema.

An attempt was made to modify (PUT, PATCH, or DELETE) a user or group that could not be found.

An attempt was made to look up (GET) a user or group that could not be found.

409 Conflict

An attempt was made to create a user or group that exists.

409 Duplicate

At least two users matched the filter in an AUTHENTICATE request.

500 Internal server error

The user or group could not be found after it was created.

An exception occurred during an attempt was made to process the request.

A schema file could not be found.

The user or group mapping file could not be found.

Unable to parse the user or group mapping file.

The user or group mapping did not contain a way to create a DN.

501 Not Implemented

An attempt was made to send or receive XML encoded information.

An HTML operation was not recognized.

503 Service Unavailable

Unable to connect to the backend LDAP server.

High availability

The SCIM services can switch to another LDAP server if required.

Note:

- The information that is stored on the LDAP servers must be kept synchronized by some other means. The synchronization is not within the scope of the SCIM Service.
- All servers that are involved must be set up in the same way, with the same containers and user credentials.

Add the **`LDAPServer.1`** property to `SCIM.properties` to specify the URL for the first failover server. If more than one failover server is required, you can add **`LDAPServer.2`**, and so on.

The SCIM Service fails over in the following way:

- When AssemblyLines are started, the SCIM Service attempts an anonymous bind to the LDAP servers.
- When it gets an answer, that LDAP server is set as the current server.
- When a request comes in, the current server is first queried.
- If a communication error occurs while a request is being processed, the AssemblyLine again tries an anonymous bind to all LDAP servers.
- If a server answers, the processing of the request restarts by using the new LDAP server.
- If no servers reply, or a communication error occurs three times during the processing of a single request, an error is returned as before.

For more information, see the topics about Directory Server Replication.

Note

Before using this information and the product it supports, read the general information under "Notices" on page 0 .

Index