IBM Tivoli Directory Integrator

Version 7.1.1, Fixpack 4

IBM Tivoli Directory Integrator

Version 7.1.1, Fixpack 4

Note

Before using this information and the product it supports, read the general information under "Notices" on page 17.

Edition notice

Note: This edition applies to version 7.1.1, fixpack 4 of *IBM Tivoli Directory Integrator* **licensed program (5724-K74) and to all subsequent releases and modifications until otherwise indicated in new editions.**

Contents

About this publication

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

IBM Tivoli Directory Integrator Version 7.1.1, Fixpack 4 documentation contains information about using the following connectors:

- QRadar Connector
- IBM Security Access Manager v2 Connector
- System for Cross-Domain Identity Management (SCIM) Connector

Access to publications and terminology

Read the descriptions of the IBM Tivoli Directory Integrator Version 7.1.1, Fixpack 4 library and the related publications that you can access online.

This section provides:

- Links to "Online publications."
- A link to the "IBM Terminology website" on page vi.

Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

IBM Tivoli Directory Integrator Library
The product documentation site (http://www-01.ibm.com/support/knowledgecenter/SSCQGF/welcome) displays the welcome page and navigation for this library.

IBM Publications Center
The IBM Publications Center site (http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss) offers customized search functions to help you find all the IBM publications you need.

Related information

Information related to IBM Tivoli Directory Integrator is available at the following locations:

- IBM Tivoli Directory Integrator uses the JNDI client from Oracle. For information about the JNDI client, see the *Java Naming and Directory Interface™ Specification* at http://download.oracle.com/javase/7/docs/technotes/guides/jndi/index.html .
- Information that might help to answer your questions related to IBM Tivoli Directory Integrator can be found at https://www-947.ibm.com/support/entry/myportal/over-accesspubsview/software/security_systems/tivoli_directory_integrator.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at http://www.ibm.com/software/globalization/terminology.

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.

Technical training

For technical training information, see the following IBM Education website at http://www.ibm.com/software/tivoli/education.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at http://www.ibm.com/software/support/probsub.html.

Troubleshooting provides details about:

- What information to collect before contacting IBM Support.
- The various methods for contacting IBM Support.
- How to use IBM Support Assistant.
- Instructions and problem-determination resources to isolate and fix the problem yourself.

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. QRadar Connector

You can use the IBM Tivoli Directory Integrator QRadar Connector to integrate unsupported event sources with QRadar.

QRadar is a next-generation security information and event management solution. It uses event information that comes from various log sources through its Device Support Modules (DSMs). The information must be in a format that is known as Log Event Extended Format (LEEF). The current version of LEEF is 1.0.

The QRadar connector accepts the following inputs:

- Events in LEEF format through Syslog input
- File imports through universal LEEF DSM

The QRadar Connector is designed to simplify the integration of unsupported event sources with QRadar. You can create valid LEEF event information by mapping from input data fields to the attributes of the LEEF V1.0 schema. You can create an IBM Tivoli Directory Integrator AssemblyLine with a connector that is configured to read or receive event data, followed by the QRadar Connector. The QRadar Connector produces the required LEEF output.

Before QRadar can use events that are created in this way, these events must be mapped in QRadar to allow for appropriate categorization. For more information, see the QRadar documentation.

QRadar Connector parameters

You can set the parameters on the **Connection** tab of the QRadar Connector to specify how to create the LEEF file.

To send LEEF-formatted syslog messages directly to QRadar, select the **Output to syslog** option.

To create a file in LEEF format, which you can later import into QRadar, clear the **Output to syslog** option. For the example in this section, it is assumed that you want to send these messages directly to syslog.

If you select the **Output to syslog** option, then the following parameters are available:

Hostname

Specifies the host name or IP address of the system where Syslog messages are sent.

This parameter is required.

Port

Specifies the port on which to send Syslog messages and on which QRadar listens.

Severity

Specifies the severity setting for the Syslog message.

The following values are available:

- alert
- critical
- debug
- emergency
- error
- informational
- notice
- warning

Facility

Specifies the facility name to use for the Syslog message.

The following values are available:

- kernel
- user
- mail
- system daemons
- security/authorization
- internal syslogs
- line printer subsystem
- network news subsystem
- UUCP subsystem
- clock daemon
- security/authorization messages
- FTP daemon
- NTP subsystem
- log audit (note 1)
- log alert (note 1)
- clock daemon (note 2)
- local0
- local1
- local2
- local3
- local4
- local5
- local6
- local7

Date format mask

Specifies the Java SimpleDateFormat mask that is applied to date values in mapped LEEF attributes, for example devTime.

The default value for this parameter is MMM dd yy HH:mm:ss, which creates a string like Oct 16 12 15:15:57.

Detailed Log

Indicates whether the connector displays Syslog messages in the log output for debugging purposes.

Comment

Stores textual information about this component.

If you clear the **Output to syslog** option, then the connector creates LEEF import files and the following parameters are available:

File path
Specifies the path to the file where the LEEF output is written. If the number of events that are written exceeds the value set in the **Maximum events per file** parameter, then a three-digit number is appended to all files. The number starts at 000 for the first file.

This parameter is required.

Date format mask
Specifies the Java SimpleDateFormat mask that is applied to date values in mapped LEEF attributes, for example, devTime.

The default value for this parameter is MMM dd yy HH:mm:ss, which creates a string like Oct 16 12 15:15:57.

Maximum events per file
Specifies whether to split the output split across multiple LEEF files.

Set the value to greater than zero (>0) to split the output. The files are named with the file name that is defined in the **File path** parameter and appended with a three-digit number that starts at 000 for the first file.

If you do not enter a value or the value is less than or equal to zero (<= 0), then all events are written to a single file. This file uses the name that is specified in the **File path** parameter.

By default, this parameter is not set and a single output file is created.

Detailed Log
Indicates whether the connector outputs debug information to the log.

Comment
Stores textual information about this component.

After you configure these parameters, click **Connect** in the Schema pane of either the input or output map of the connector. The list of standard LEEF fields is returned, which indicates the type of each field and whether it is required or optional.

Only four mandatory attributes must appear in an output map. They are part of the LEEF header that is written for an event and they must be mapped to create a LEEF output. Scroll down in the schema list to view the following mandatory attributes:

- LEEFHeader_EventID
- LEEFHeader_Product
- LEEFHeader_ProductVersion
- LEEFHeader_Vendor

You can ignore the [1..1] notation that follows the name of each required attribute.

Setting up the QRadar Connector

You can set up the AssemblyLine with QRadar Connector to parse an input file.

About this task

The QRadar Connector is available from IBM Tivoli Directory Integrator, Version 7.1.1, Fixpack 4 onwards. When you install IBM Tivoli Directory Integrator, the `QRadarConnector.jar` file is copied to the *`tdi_install`*`/jars/connectors` directory.

The following procedure assumes that you know how to create and configure AssemblyLines and Connectors in Configuration Editor. See Getting Started Guide and Users Guide in the IBM Tivoli Directory Integrator documentation.

Procedure

1. For this procedure, create or use a sample input file in the CSV format that uses semicolons (;) to delimit fields. Name the file `Alerts.csv`.

   ```
   SYSTEM;MANUFACTURER;MACADDRESS;SYSTEMVRS;PORT;HOSTNAME;IPSOURCE;WHEN;ALERTID;ACCOUNT
   StreamPort;TT Sys;1F:9D:A7:9B:29:78;1.5.12;2332;matrix.net;213.162.242.251;
        Fri Apr 27 13:04:09 GMT+1 2012;A00398988;WRST
   E112-B;Sun;64:C0:2A:7F:6A:5A;2.3.17;3566;matrix.net;195.89.246.157;
        Fri Apr 27 13:04:09 GMT+1 2012;ABN107441;SWCHW
   AccessGate;Oracle;87:F3:D2:33:A8:32;5.1.6;3962;abc.com;105.168.129.139;
        Fri Apr 27 13:04:09 GMT+1 2012;AL662162;GRCO
   StreamPort;IBM;1C:D8:B2:BD:29:DD;8.2.10;8597;ccrd.comgroup.eu;140.62.226.198;
        Fri Apr 27 13:04:09 GMT+1 2012;ABN861291;TEL5
   NetViewer;Elektron;65:70:22:50:FB:CB;5.7;1177;sil2.devops.crund.com;102.204.120.233;
        Fri Apr 27 13:04:09 GMT+1 2012;A00897609;FDDLR
   Auth Grid;HP;E0:C0:52:03:BE:ED;4.0.16;9957;fldrs.omnicom.net;94.23.123.47;
        Fri Apr 27 13:04:09 GMT+1 2012;ABN739017;GRMM
   Facilities Monitor;Cisco;EC:E0:CB:85:16:1F;2.1.18;3434;fldrs.omnicom.net;112.192.157.23;
        Fri Apr 27 13:04:09 GMT+1 2012;CRT852913;GRCO
   Omnisys;Cisco;09:1E:EA:54:B8:C7;2.3.17;6555;baynter.org;80.189.199.43;
        Fri Apr 27 13:04:09 GMT+1 2012;A00344678;ABCO
   ```

2. Create an **AssemblyLine** in the IBM Tivoli Directory Integrator Configuration Editor.
3. Add the **QRadar Connector** to the AssemblyLine by dragging it from the Navigator pane. For more information about how to add the connector to the AssemblyLine, see Connectors section in the IBM Tivoli Directory Integrator documentation. The **QRadarConnector** component in the AssemblyLine is displayed in blue, which indicates that it is inheriting its configuration from a connector in the library.
4. To read the CSV file, add a **FileSystem** Connector in iterator mode to the AssemblyLine.
5. To handle decoding of the file, select the **CSV Parser** in the File Connector.
6. Rename the connector. For example, rename it as `Read Alerts file`.
7. Place the `Read Alerts file` connector in the **Feed** section of the AssemblyLine. This iterator connector reads the entire file and passes parsed data to any components that you put in the **Data Flow** section for processing.
8. On the **Connection** tab, specify the **File Path** as the sample `Alerts.csv` file.
9. To discover the schema of the file, on the **Input Map** tab, click **Connect**.

   This action also helps you verify that you selected the correct parser. When you click **Connect**, the connector initializes the connection and queries the schema of the connected system. If you are working with an RDBMS, LDAP directory, or some other system that provided schema information, then you can view the list of available attributes.
10. Click **Next** to refresh the **Sample Value** column with the next entry that is parsed from the input file.

11. Browse through the values to verify that the connector can read and parse the file.
12. Set up the input map.

    These fields are not yet selected for processing in the AssemblyLine. You must create mapping rules that describe how data is passed from the connector into the AssemblyLine.

    Take one of the following actions:

    - Drag attributes from the schema area and drop them in the mapping area.
    - Click **Add** in the mapping area.

    For this example, you must bring all the schema attributes into the AssemblyLine for processing. Click **Add** and then specify the wildcard map (*) to **Map all attributes**.

    Now all the fields from each line of the CSV file are returned as attributes in the Work Entry. Each attribute retains the name of the field from which it gets its value.

What to do next

Configure the QRadar Connector parameters. For this example, configure the following settings:

- Select the **Output to Syslog** option.
- Specify the **Hostname** (example value: `localhost`).
- Specify the **Port** (example value: `514`).
- Specify the **Severity** (example value: `debug`).
- Specify the **Facility** (example value: `mail`).
- Select the **Detailed log** option.

Mapping input data to the LEEF schema

You can specify the values to write in the Syslog messages that are sent to QRadar by mapping input data to the LEEF schema.

Procedure

1. On the **Output Map** tab, click **Connect** in the Schema pane to discover the LEEF schema.
2. Map the mandatory attributes in the input fields to the attributes of the LEEF schema. Select the attributes from the schema area and drag them to the left to create mapping rules.
3. In addition to the mandatory attributes, map the following attributes in the Schema pane:

   `devTime`
   The device time, which is the raw event date and time that is generated from the host that provides the event log.

   `dst`
   The IP address of the event destination.

   `dstMAC`
   MAC address of the event destination in hexadecimal format.

   `dstPort`
   Destination port of the event.

4. Modify the mapping for these attributes by editing the mapping rules that you added to the QRadar Connector's **Output Map**.

   Each mapping rule consists of the target attribute name as it will appear after the mapping and the assignment of value for this attribute.

   In an **Output Map**, the assignment is shown on the left side of the mapping rule, while the target attribute name is on the right.

   For example, if you drag `LEEFHeader_EventID` attribute from the Schema pane to the **Output Map**, the target attribute name for the new rule is identical to the schema attribute that you selected:

   - **Assignment**: `work.LEEFHeader_EventID`
   - **Component Attribute name**: `LEEFHeader_EventID`
5. Correct the mapping rules.

   When you drag an attribute from the Schema pane into a map, a default assignment is defined. The assignment is defined as an attribute with the same name as the attribute that comes from the Work Entry.

   These default assignments must be modified so that they refer to the fields that are being read from the input file.

   a. Double-click an assignment value to open the script editor.

   b. Change the name of the work entry attribute to match the corresponding input field.

   The work entry is the data bucket that holds the values that are read by the iterator connector. It is available for scripting as the variable named *`work`*.

   Note: You can press `Ctrl+Space` key to view a list of input attributes. The same list is also displayed if you type `work.`

   The completed map for the example scenario that is described in the topic, "Setting up the QRadar Connector" on page 3 is shown here:

Table 1. Output map

Assignment	Component Attribute
work.ALERTID	LEEFHeader_EventID
work.SYSTEM	LEEFHeader_Product
work.SYSTEMVRS	LEEFHeader_ProductVersion
work.MANUFACTURER	LEEFHeader_Vendor
work.WHEN	devTime
work.IPSOURCE	dst
work.MACADDRESS	dstMAC
work.PORT	dstPort

What to do next

Set up a QRadar log source.

Setting up a QRadar log source

You must configure a dedicated log source, for QRadar to receive Syslog messages from a source.

About this task

Important: You must set the **Log Source Type** and **Protocol Configuration** parameters correctly. Otherwise, the Syslog events that you send are not received or parsed correctly. For more information, see the QRadar documentation.

Procedure

1. Log on to the QRadar SIEM console.
2. Click the **Admin** tab.
3. Under the **Data Sources > Events** section, click **Log Sources**.
4. Click **Add** to create a log source.
5. Set the following minimum parameters:

   Log Source Name
   Enter a title for the log source. This name appears in the log activity window.

   Log Source Description
   Enter a description for the log source.

   Log Source Type
   Identify the format of the events. Select the value `Universal LEEF`.

   If you do not select the value `Universal LEEF`, QRadar cannot parse the Syslog messages that you send through the QRadar Connector.

   Protocol Configuration
   Select the protocol for this log source. Select the value `Syslog`, which is the protocol that the QRadar Connector uses.

   Log Source Identifier
   Enter the IP address of your IBM Tivoli Directory Integrator server.

   Enabled
   Select this option to enable the log source.
6. Click **Save**.
7. On the **Admin** tab of the QRadar SIEM console, click **Deploy Changes** to activate your new log source.

What to do next

Test the IBM Tivoli Directory Integrator and QRadar integration solution. See "Verifying the solution."

Verifying the solution

After you complete the configuration steps for the QRadar Connector and set up the attribute maps, you can test the solution and verify that events are sent to QRadar.

Procedure

1. In the IBM Tivoli Directory Integrator Configuration Editor, open the AssemblyLine.
2. On the AssemblyLine Editor window, click **Run in console**. The AssemblyLine is started and the output that is being logged by the AssemblyLine is displayed.

3. Verify that the log output contains the metrics for the various operations that are carried out by the AssemblyLine Connectors. For example, the following sample output shows that eight lines were read from the input file and then written by the QRadar Connector.

```
[Read Alerts file] Get:8
[QRadarConnector] Add:8
```

4. To verify the events that were sent in QRadar, log on to the QRadar SIEM console.
5. Click the **Log Activity** tab.
6. Verify that the Syslog events appear in the table under **Log Activity**.

What to do next

Use the following information to troubleshoot when the log results are not as expected:

- In IBM Tivoli Directory Integrator Configuration Editor, on the QRadar Connector's **Connection** tab, ensure that the **Detailed Log** option is selected. If this option is not selected, QRadar does not get the log output of the actual LEEF events that are written.
- You must configure the mapping for incoming Syslog messages to QRadar events. If the mapping is not configured, in the QRadar **Log Activity** page, the events are displayed as `unknown` in the **Event Name** column.
- If no events appear in the **Log Activity** page, ensure that the display is not paused. From the **View** list, you can select `Real Time (streaming)` and remove any filters to ensure that you see the live feed. If you still do not see any events, confirm that you have the correct QRadar host name and Syslog port settings in your connector.
- If the events appear under **Log Activity** but the name of your log source is not displayed, the **`Log Source Identifier`** value might be wrong. If the IP address does not match the address of the Syslog packets, then they are handled by the Generic Log Source instead. In this case, no parsing is done and the Source IP and Destination IP columns default to the sender IP address of the packets that are received. You must specify this value in the **`Log Source Identifier`** parameter of your log source.
- The name of your log source might be displayed correctly under **Log Activity**, but the Source IP and Destination IP columns might still display the IBM Tivoli Directory Server's IP address. In that case, ensure that you select `Univeral LEEF` for the **`Log Source Type`**. Otherwise, parsing fails.

Chapter 2. IBM Security Access Manager v2 Connector

The IBM Security Access Manager v2 Connector enables you to provision and manage IBM Security Access Manager users and groups by using the IBM Security Access Manager Registry Direct API.

The IBM Security Access Manager Registry Direct API directly accesses the underlying Security Access Manager registry rather than through authorization servers or policy servers. It also provides access to most of the underlying registry user attributes and the attributes available through the traditional IBM Security Access Manager Java™ API. This API provides attribute read-only Global Sign On (Single Sign On resource credential) support. It does not create, enable, disable, or delete the users that are enabled for Global Sign On.

The IBM Security Access Manager v2 Connector uses the access method that is provided through the Registry Direct API.

This API:

- removes the dependency on the policy server, a single point of failure.
- provides access to more attributes.
- improves performance and scalability.

The IBM Security Access Manager v2 Connector supports managing users and groups in the following modes:

- Iterator
- AddOnly
- Update
- Lookup
- Delete

Note: The IBM Security Access Manager v2 Connector does not support adding, modifying, or deleting global sign-on users. These users can only be read by using Iterator or Lookup mode. To add, modify, or delete global sign-on users, use the Tivoli Access Manager (TAM) Connector.

Deploying the Registry Direct API

Before you configure the IBM Security Access Manager v2 Connector, you must deploy the IBM Security Access Manager Registry Direct API and configure its properties.

Before you begin

- Install IBM Tivoli Directory Integrator, Version 7.1.1, Fixpack 4, which contains `ISAMConnector.jar`.
- Install IBM Security Access Manager Version 6.1.1 or later and configure it for the user registry to integrate.
- IBM Security Access Manager authentication ID that is configured to allow stand-alone configuration.

Note: In stand-alone configuration, the LDAP identity that is used to access LDAP and do the administration updates must be manually created. Use access manager to create the LDAP identity. For example:

```
pdadmin sec_master> user create -no-password-policy
testapi cn=testapi,o=ibm,c=us testapi api passw0rd
( SecurityGroup ivacld-servers remote-acl-users )
```

For more information, see IBM Security Access Manager Registry Direct Java API documentation.

About this task

The `ISAMConnector.jar` file is in the *`tdi_install_dir`*`/jars/connectors` directory.

where

`tdi_install_dir` is the IBM Tivoli Directory Integrator installation directory. *`tdi_solution_dir`* is the IBM Tivoli Directory Integrator solution directory, which is selected during installation and is in *`tdi_install_dir`*`/bin/defaultSolDir` script.

The `com.tivoli.pd.rgy.jar` file contains the IBM Security Access Manager Registry Direct API library and the tool that creates API configuration file.

The following procedure assumes that the IBM Security Access Manager server is remote to the IBM Tivoli Directory Integrator Server.

Procedure

1. Make the IBM Security Access Manager Registry Direct API JAR file available to the IBM Tivoli Directory Integrator server. Choose one of the following methods:
   - Copy *`ISAM_install_dir`*`/java/export/rgy/com.tivoli.pd.rgy.jar` to the *`tdi_install_dir`*`/jars/3rdParty/IBM` directory.
   - Copy *`ISAM_install_dir`*`/java/export/rgy/com.tivoli.pd.rgy.jar` to the IBM Tivoli Directory Integrator directory that is specified by the **`com.ibm.di.loader.userjars`** property in `solution.properties`. The following setting shows the default:

     ```
     # com.ibm.di.loader.userjars=c:\myjars
     ```

     You must uncomment the line and create the directory name that is referenced.
2. Create the configuration file by using the IBM Security Access Manager configuration tool, `RgyConfig`.
   1. Change directory to *`tdi_install_dir`*`/jvm/jre` to use the IBMJava Runtime Environment.
   2. Run the following command:

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

      For more information about the configuration options for the Security Access Manager Registry Direct API, see Configuration options.

      Example

      Assumptions:

      - Current directory is *`tdi_install_dir`*`/jvm/jre`.

- You copied com.tivoli.pd.rgy.jar file to *tdi_install_dir*/jars/3rdParty/IBM.
- The valid DN for sec_master is cn=SecurityMaster,secAuthority=Default.

```
java.exe -cp tdi_install_dir/jars/3rdParty/IBM/com.tivoli.pd.rgy.jar
      com.tivoli.pd.rgy.util.RgyConfig sam4sdi.properties
      create Default Default "ldapSamServer:389:readwrite:5"
      "cn=SecurityMaster,secAuthority=Default" secret
```

The sam4sdi.properties file is created in the local directory.

3. Copy the newly created properties file to the *tdi_solution_dir* directory.
4. Restart IBM Tivoli Directory Integrator.

Configuration

After you install the IBM Security Access Manager v2 Connector, you can configure it by adding it to an AssemblyLine or the Connectors folder of your IBM Tivoli Directory Integrator project's resources.

The Delete, Lookup, and Update modes require link criteria, which you can create on the **Link Criteria** tab of the IBM Security Access Manager v2 Connector. You must use principalName for users and cn for groups.

Parameters

You can manage users and groups from IBM Security Access Manager with the IBM Security Access Manager v2 Connector parameters.

Use the following parameters on the **Connection** tab of the IBM Security Access Manager v2 Connector panel to configure the IBM Security Access Manager v2 Connector.

ISAM Domain
The name of the IBM Security Access Manager domain with which you are integrating.

Configuration file
The path to the IBM Security Access Manager API configuration file that is created with the **com.tivoli.pd.rgy.until.RgyConfig** tool.

Entry Type
The type of entry, either user or group.

Name Search Filter
The value that is used as the search filter against the **principalName** attribute for IBM Security Access Manager user accounts or the **cn** attribute for groups.

This parameter supports the wildcard character, asterisk (*). For example, ab* returns all entries that start with ab. This parameter is only available for Iterator mode.

Attribute maps

The IBM Security Access Manager v2 Connector schema depends on the entity type that you select.

Attributes for an IBM Security Access Manager user entity

The user entity type has the following schema attributes. Some attributes are written to the LDAP person entry that is associated with the user, while others are specific to the user account itself.

cn
Specifies the cn (common name) of the associated LDAP entry. This attribute is required.

description
Describes the associated LDAP person entry.

memberOf
Specifies that the user is a member of one or more groups.

This attribute must contain one or more group **cn** values or the **secDN** that references these values. Another approach to managing group membership is by using the **member** attribute of a group.

principalName
Uniquely identifies the user. Its unique value becomes the login credentials for this user. This attribute is required.

secAcctValid
Indicates whether an IBM Security Access Manager User account is valid or not. Its value can be either string or Boolean, for example `true` or `'true'`.

secDN
Specifies the DN (distinguished name) of the LDAP entry that is associated with this user. This attribute is required.

secPwdValid
Indicates whether the password for the user is valid.

For pass-through authentication (PTA) to work for the underlying IBM Tivoli Directory Server, set this Boolean flag to `true`.

Note: Changing the password automatically resets the value of **secPwdValid** to `true`. For example, if you set a value for **userPassword** in an AssemblyLine with update mode, the value of **secPwdValid** is set to `true`.

sn
Specifies the sn (surname) of the associated LDAP entry. This attribute is required.

userPassword
Writes the password for the user. The value must be in clear text.

This attribute is required if you create both the IBM Security Access Manager user and the LDAP person entry in the directory. It is required because the API applies policy checks to the entry that is created. However, if the person entry, which is to be added by the connector, already exists, then the user is imported instead of created. In this case, **userPassword** is not mandatory.

Attributes for an IBM Security Access Manager group entity

The group entity type has the following schema attributes. Only the **cn** and **secDN** attributes are specific to the group itself. The other attributes are for the associated LDAP group entry.

cn
Identifies an IBM Security Access Manager group and is also the cn (common name) of the associated LDAP group entry. This attribute is required.

description
Describes the associated LDAP group entry.

member
Contains one or more DN values that reference LDAP person or group entries or both. Another approach to managing group membership is by using the **memberOf** attribute of the individual users.

secDN
Specifies the DN of the LDAP entry that is associated with this group. This attribute is required.

Troubleshooting

You can use the explanations for common errors to troubleshoot the IBM Security Access Manager v2 Connector.

Unable to read in the configuration URL: file:/X:/TDI/LDAPSync/ISAM_API.properties.
The IBM Security Access Manager v2 Connector parameter that is labeled as Configuration File must contain the path and file name of the IBM Security Access Manager API properties file. This API properties file is generated with the **com.tivoli.pd.rgy.util.RgyConfig** tool.

The IBM Security Access Manager domain <*DomainName*> **does not exist.**
The domain name that is specified either in the IBM Security Access Manager v2 Connector Connection tab or in the API properties file is invalid.

The distinguished name does not map to an existing entry in the registry.
The **secDN** value does not map to an existing branch of the IBM Tivoli Directory Server directory tree. Ensure that your mapping of the attribute is correct.

The specified distinguished name (secDN) does not exist.
The **secDN** value does not map to an existing branch of the IBM Tivoli Directory Server directory tree. Ensure that your mapping of the attribute is correct.

An invalid group identification or Distinguished Name (DN) was specified.
The group identifier or DN value is invalid. For example, the **cn** attribute value that is used when you are writing groups is invalid. Ensure that your mapping of the attribute is correct.

There is no IBM Security Access Manager entity in the domain with ID <*id*>**.**
While you are writing groups, the **member** attribute must contain the IDs of existing IBM Security Access Manager user and group entities. Otherwise, these values are skipped and this error is logged.

Entry was not found.
The link criteria that is set up for the IBM Security Access Manager v2 Connector failed to locate an entry.

Group not found.
While you are writing IBM Security Access Manager users, the **memberOf** Attribute must contain the IDs of existing groups. Otherwise, these values are skipped and this error logged.

Connector gives null pointer exception when userPassword is missing in output map of the AddOnly mode
The userPassword attribute is required if you create both the IBM Security

Access Manager user and the LDAP person entry in the directory. It is required because the API applies policy checks to the entry that is created. However, if the person entry, which is to be added by the connector, already exists, then the user is imported instead of created. In this case, userPassword is not mandatory.

The `secPwdValid` password is written as `true` even when the value mapped to it was `false`.

The **`secValidPwd`** attribute for an IBM Security Access Manager user is set to `true` whenever the **`userPassword`** attribute is modified.

For more information, see the following links:

- IBM Security Access Manager documentation
- IBM Security Access Manager Registry Direct Java API documentation
- Tivoli Access Manager (TAM) Connector

Chapter 3. SCIM Connector

The System for Cross-Domain Identity Management (SCIM) protocol is an application-level, REST protocol for provisioning and managing identity data on the web. You can use the information provided here to know further about SCIM Connector.

The protocol supports creation, modification, retrieval, and discovery of core identity resources, which are users and groups, and also custom resource extensions.

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

Configuration

You can use the parameters provided here to configure the SCIM Connector.

The SCIM Connector uses the following parameters:

SCIM Server URL
Specifies the URL for the SCIM server. This parameter is required.

Resource Endpoint
Specifies the resource endpoint. You can select either `Users` or `Groups` from the core SCIM schema, or a user-defined resource endpoint.

User Name
Specifies the user name the connector uses for HTTP basic authentication with the SCIM server.

Password
Specifies the password for the specified user name.

The following parameters are available under the Advanced section:

Update Method
Specify the method to use when entries are updated in the SCIM server. You can select from the following options:

- `Patch with provided entry`: Sends the entry to the SCIM server with the PATCH method.
- `Replace entire entry`: Sends the entry to the SCIM server with the PUT method.

Attribute Filter
Specify a comma-separated list of attributes that the server must return. If you do not specify any values for this parameter, the default is no filter, which means that all resources are received.

Proxy Server
Specifies the host proxy server and port number (*`proxyhost:port`*), if you use a proxy server for connections. If you do not specify a value for this parameter, no proxy server is used.

Proxy Server User Name
Specifies the user name to authenticate to the proxy server, if the proxy server that you use requires authentication.

Proxy Server Password
Specifies the password for the proxy server user name that you specified.

Sort by
Specifies the attribute that is used to sort results, if the SCIM server implements sorting. If you do not specify a value for this parameter, the default is no sorting.

Sort order
Specifies the sort order as ascending or descending. This parameter is used only if you implement sorting. If you do not specify a value for this parameter, the results are sorted in ascending order.

Script
Controls how the SCIM Connector operates. Consider carefully before you modify the script because changing the script might produce unexpected results.

See Also

SCIM website at www.simplecloud.info.

Notices

This information was developed for products and services offered in the U.S.A. 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 give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :

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 states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might 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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

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

Licensees of this program who want 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 Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All 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 the names and addresses used by an actual business enterprise 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. 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 IBM's application programming interfaces.

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_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Index

Printed in USA