IBM Security Verify Governance Identity Manager

Guardium GDAP Adapter Installation and Configuration Guide

BA21-8475-00

Contents

Figures

Tables

Chapter 1. Overview

An adapter is an interface between a managed resource and an IBM Security Identity server. The Guardium GDPR adapter enables communication between Guardium and the IBM Security Identity and Governance Intelligence server.

Features of the adapter

The Guardium GDPR adapter supports the following operations on a Guardium appliance that is configured with a DB2 datasource only.

The Guardium GDPR adapter monitors databases that is configured with it. The database user and access information is collected in the form of pre-generated reports.

You can perform following operations on this data that is generated by Guardium.

- Reconciling users
- Reconciling support data (Tables).
- Test connection from Verify Governance Identity Manager server to Guardium resource.

Architecture of the adapter

The Guardium GDPR Adapter communicates to Guardium resource to fetch users and table access information that is collected in the form of pre-generated reports.

The Security Directory Integrator httpClient connector is used for reconciling data from Guardium reports.

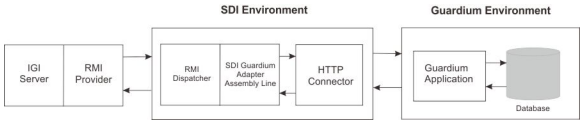


Figure 1. The architecture of the Guardium GDPR Adapter

Chapter 2. Planning

Plan and prepare to install and configure the adapter by understanding and completing the following tasks.

Prerequisites

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

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

Table 1. Prerequisites to install the adapter

Prerequisite	Description
Directory Integrator	• IBM Security Directory Integrator Version 7.1.1 + 7.1.1-TIV-TDI-FP0004 + 7.2.0-ISS-SDI-LA0008 • IBM® Security Directory Integrator Version 7.2 + FP3 or later **Note:** • Earlier versions of IBM Security Directory Integrator that are still supported might function properly. However, to resolve any communication errors, you must upgrade your Directory Integrator release to the versions that the adapter officially supports. • The adapter supports IBM Security Directory Integrator 7.2, which is available only to customers who have the correct entitlement. Contact your IBM representative to find out whether you have the entitlement to download IBM Security Directory Integrator 7.2.
Identity server	IBM Security Identity Governance and Intelligence server Version 5.2.3
Guardium specific requirements	Guardium Version 10.1.3. Guardium database entitlement reports must be pre-generated on the Guardium Appliance. Generally, the Admin user is needed to build and generate reports. Guardium GDPR adapter requires a `client id` and corresponding `client secret` to be configured with Guardium resource. Guardium User Guide is available at https://www.ibm.com/support/knowledgecenter/en/SSMPHH_10.0.0/com.ibm.guardium.doc/g100_welcome.html.

Table 1. Prerequisites to install the adapter (continued)	
Prerequisite	**Description**
Create Guardium reports	The adapter requires the following two reports to perform reconciliation: • User Data Reconciliation: Entitlement report for user to permission mapping • Support Data Reconciliation: Entitlement report for permission to taxonomy criteria mapping For more information, see Chapter 6, "GDPR reports overview," on page 19.
Network Connectivity	Install the adapter on a workstation that can communicate with the service through the TCP/IP network.
System Administrator authority	To complete the adapter installation procedure, you must have system administrator authority.
Security Directory Integrator adapters solution directory	A Security Directory Integrator adapters solution directory is a Security Directory Integrator work directory for IBM Security Verify Adapters. For more information, see the *Dispatcher Installation and Configuration Guide*.

Installation worksheet

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

Table 2. Required information to install the adapter

Required information	Description	Value

Security Directory Integrator Home Directory	The *ITDI_HOME* directory contains the jars/connectors subdirectory that contains adapter JAR files. For example, the `jars/connectors` subdirectory contains the JAR file for the UNIX adapter.	If Security Directory Integrator is automatically installed with your Identity server product, the default directory path for Security Directory Integrator is as follows:
		Windows:
		• For Directory Integrator version 7.1.1:
		drive`\Program Files\IBM\TDI\V7.1.1`
		• For Directory Integrator version 7.2:
		drive`\Program Files\IBM\TDI\V7.2`
		UNIX:
		• For Directory Integrator version 7.1.1:
		`/opt/IBM/TDI/V7.1.1`
		• For Directory Integrator version 7.2:
		`/opt/IBM/TDI/V7.2`

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

Required information	Description	Value

Adapters solution directory	When you install the dispatcher, the installer prompts you to specify a file path for the solution directory. For more information about the solution directory, see the *Dispatcher Installation and Configuration Guide*.	The default solution directory is at:
		Windows:
		• For Directory Integrator version 7.1.1:
		`drive\Program Files\IBM\TDI\V7.1.1\isimsoln`
		• For Directory Integrator version 7.2:
		`drive\Program Files\IBM\TDI\V7.2\isimsoln`
		UNIX:
		• For Directory Integrator version 7.1.1:
		`/opt/IBM/TDI/V7.1.1/isimsoln`
		• For Directory Integrator version 7.2:
		`/opt/IBM/TDI/V7.2/isimsoln`

Chapter 3. Installing

All IBM Security Directory Integrator-based adapters require the Dispatcher for the adapters to function correctly. Download the Dispatcher installer from the IBM Passport Advantage website. For more information about the installation, see the Dispatcher Installation and Configuration Guide.

If the Dispatcher is installed from a previous installation, do not reinstall it unless the Dispatcher is upgraded.

Importing the adapter profile

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

Before you begin

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

About this task

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

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

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

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

Procedure

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

A message indicates that you successfully imported a profile.

7. Click **Close**.

   The new profile is displayed in the list of profiles.

Results

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

What to do next

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

- Import the attribute mapping file. See “Importing attribute mapping file” on page 8.
- Create a connector that uses the target profile. See “Adding a connector” on page 8.

Importing attribute mapping file

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

About this task

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

Procedure

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

      A message indicates that you successfully imported the file.
7. Click **Close**.

Adding a connector

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

About this task

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

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

Procedure

To add a connector, complete these steps.

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Connectors**.
   A list of connectors is displayed on the **Connectors** tab.
4. Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Click **Actions** > **Add**.
   The **Connector Details** pane is enabled for your input.
7. On the **Connector Details** tab, complete these steps:
   a) Assign a name and description for the connector.
   b) Select the target profile type as `Identity Brokerage` and its corresponding target profile.
   c) Select the entity, such as **Account** or **User**.
      Depending on the connector type, this field might be preselected.
   d) Optional: Select **Trace ON** and the corresponding **Trace Level** to enable trace logs.
      The available trace levels are DEBUG, INFO, and ERROR.
   e) Optional: Select **History ON** to save and track the connector usage.
   f) Click **Save**.
      The fields for enabling the channels for sending and receiving data are now visible.
   g) Select and set the connector properties in the **Global Config** accordion pane.
      For information about the global configuration properties, see Global Config accordion pane.
   h) Click **Save**. The fields for enabling the channels for sending and receiving data are now visible.

Results

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

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

What to do next

Enable the channel modes to synchronize the data between the target systems and Verify Governance Identity Manager. For more information, see “Enabling connectors” on page 10.

Configuring the SSL connection between the IBM Security Directory Integrator and Guardium server

This topic describes the procedures to configure the SSL connection between the IBM Security Directory Integrator and the Guardium server.

About this task

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

Procedure

1. On a web browser, navigate to your instance URL. For example, `https://<Guardium_Host><Port_Number>`.
2. View the certificate.
   a) Click the SSL lock icon on the browser.
   b) Click **View Certificates**.
3. Select **Guardium Certificate**.
4. Click **Export to file**.
5. Select `X.509 (.CER)` format and click **Save**.
6. Perform one of the following actions:
   - If the RMI Dispatcher already has a configured keystore, use the `keytool.exe` program to import the Guardium certificate.
   - If the keystore is not yet configured, create it by running the following command from a command prompt. Ensure that the command is run in a single line.

     ```
     keytool -import -alias guardium -file c:\guardium.cer -keystore truststore.jks -storepass passw0rd
     ```
7. Edit `IDI_HOME/timsol/solution.properties` file to specify the truststore and keystore information.

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

   - Keystore file information for the server authentication
   - It is used to verify the server public key. For example,
     - `javax.net.ssl.trustStore=truststore.jks`
     - `javax.net.ssl.trustStorePassword=passw0rd`
     - `javax.net.ssl.trustStoreType=jks`

   If these key properties are not configured, you can set truststore to the same that contains the Guardium certificate. Otherwise, you must import the Guardium certificate to the truststore specified in `javax.net.ssl.trustStore` .
8. After you modify the `solution.properties` file, restart the Dispatcher. For more information, see the *Dispatcher Installation and Configuration Guide*.

Enabling connectors

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

Before you begin

Table 3. Prerequisites for enabling a connector

Prerequisite	Find more information
A connector must exist in Verify Governance Identity Manager.	“Adding a connector” on page 8.
Ensure that you enabled the appropriate channel modes for the connector.	“Reviewing and setting channel modes for each new connector” on page 11.

Procedure

To enable a connector, complete these steps:

1. Log in to the Verify Governance Identity Manager Administration Console.

2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Connectors**.

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

   Enable write-to channel
   Propagates every change in the Access Governance Core repository into the target system.

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

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

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

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

Results

The connector is enabled.

What to do next

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

Reviewing and setting channel modes for each new connector

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

About this task

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

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

Procedure

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

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

   A list of connectors is displayed on the **Connectors** tab.

4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Optional: To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Select the connector that you want to enable.
7. On the **Connector Details** tab, complete these steps:
   a) Select the channel modes that you want to enable, and then click **Save**. Depending on the channels that you enable, the corresponding **Channel** tabs are displayed, in which you can do more configuration, such as mapping attributes and setting up rules.

      Enable write-to channel
      Propagates every change in the Access Governance Core repository into the target system.

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

      Enable reconciliation
      Synchronizes the modified data between the Access Governance Core repository and the target system.
8. Select **Monitor** > **Change Log Sync Status**.
   A list of connectors is displayed.
9. On the **Change Log Sync Status** tab, complete these steps:
   a) Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
   b) Select a connector, and click **Actions** > **Sync Now**.
      The synchronization process begins.
   c) Optional: To view the status of the synchronization request, select **Sync History** in the right pane.
      Information about the synchronization is displayed in the **Sync History** tab.
10. Set the change log synchronization schedule for each new connector that you migrated.
11. When the connector configuration is complete, enable the connector by completing these steps:
    a) Select **Manage** > **Connectors**.
    b) Select the connector that you want to enable, and then select the **Enable** check box in the **Connector Details** tab.
    c) Click **Save**.
       For more information, see "Enabling connectors" on page 10.

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

       For Identity Brokerage HR feed connectors, only the check box for enabling the read-from channel is available.
12. Start the connector by selecting **Monitor** > **Connector Status**. Select the connector that you want to start, and then select **Actions** > **Start**.

Attribute Mapping

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

About this task

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

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

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

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

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

Note:

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

Procedure

1. Open the mapping definition file by using any text editor.
2. Edit the mapping.
3. If the target attribute has a list of predefined values, use the following syntax to convert its values to the corresponding Verify Governance Identity Manager attribute values.
   a) `[conversion].`*`<target_attribute>.<IGI_attribute>`* `=`
   `[`*`<target_attribute_value1>=<IGI_attribute_value1>;...;`*
   b) *`<target_attribute_valuen>=<IGI_attribute_valuen>`*
4. For attributes that contains date and time, use the following syntax to convert its values.
   For example,
   a) `[conversion.date].erbirthDate.BIRTHDAY=[yyyyMMdd=dd/MM/yyyy HH:mm:ss]`
   b) `[conversion.date].ACCOUNT_EXPIRY_DATE.ACCOUNT_EXPIRY_DATE=`
   c) `[dd/MM/yyyy HH:mm:ss=dd/MM/yyyy HH:mm:ss]`
5. Import the updated mapping definition file through the Enterprise Connectors module. For more information, see *Attribute-to-permission mapping service* in the IBM Security Verify Governance Identity Manager product documentation.

Service or target form details

You must create a user account with administrative privilege that can access reports by using REST API for the adapter on the managed resource. Provide the account information when you create a managed target for the adapter on IBM Security Identity Governance and Intelligence.

The Guardium GDPR adapter requires a `client id` and corresponding `client secret` to be configured against a Guardium resource.

Table 4. Attributes for an adapter target

Attribute	Description	Required attribute?
Name	Specify a name that defines the adapter connector on Identity Governance and Intelligence server.	Yes
Description	Specify a description that identifies the connector for your environment.	No
Security Directory Integrator location	Specify the URL for the Security Directory Integrator instance. The valid syntax for the URL is `rmi://ip-address:port/ITDIDispatcher` where `ip-address` is the Security Directory Integrator host and `port` is the port number for the RMI Dispatcher. The default URL is `rmi://localhost:1099/ITDIDispatcher`.	Yes

Table 4. Attributes for an adapter target (continued)		
Attribute	**Description**	**Required attribute?**
HTTP URL for Guardium Appliance	For example, https://<Guardium_Host><Port_Number>/oauth/token?client_id=<client_ID>&grant_type=password &client_secret=<Client_Secret> &username=<Admin_Account>&password=<Password>	Yes
Entitlement report for GDPR classification	Name of the pre-generated entitlement report. This report needs to be generated on the resource by using the administrator account. For more information, see Chapter 6, "GDPR reports overview," on page 19.	Yes
Report name for permission to attribute mapping	Name of the pre-generated support data report. This report must be generated on the resource by using the administrator account.	Yes
Taxonomy criteria name - ID mapping file path	Absolute path of the mapping file. This file contains criteria name and corresponding IDs.	Yes

Verifying that the adapter is working correctly

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

Procedure

1. Test the connection for the service that you created on the Identity server.
2. Run a full reconciliation from the Identity server.
3. Verify the `ibmdi.log` file after each operation to ensure that no errors are reported.
4. Verify the `trace.log` file to ensure that no errors are reported when you run an adapter operation.

Installing the adapter language package

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

See the IBM Security Verify Governance Identity Manager product documentation and search for information about installing the adapter language pack.

Chapter 4. Troubleshooting

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

Error messages and problem solving

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

Table 5. Runtime problems

Warning or error message	**Corrective action**
An error occurred while establishing communication with the Security Directory Integrator server.	Identity and Governance Intelligence server cannot establish a connection with Security Directory Integrator. To fix this problem, ensure that: • Security Directory Integrator is running. • The URL specified on the service form for Security Directory Integrator is correct.
CTGDIJ109E Unable to connect to the resource. Login failed for user.	Verify that correct login credentials are specified.
CTGDIJ109E Initialize Error. Unable to connect to the resource.	Verify the connection properties. Make sure that an instance of Guardium is running on the host and accepting TCP/IP connections at the port. Make sure that TCP connections to the port are not blocked by a firewall.

Chapter 5. Reference

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

Adapter attributes and object classes

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

Attributes in `erGuardiumAccount` object class

Table 6. Supported attributes in `erGuardiumAccount` object class

Attribute	Adapter attribute	Description	Single or Multi-value	Data type	Required attribute?
GRANTEE	eruid	A user in a system to whom a grant is made.	Single	String	Yes
GRANTEE	erguardiumfirstname	A name of a user to whom a grant is made.	Single	String	No
TableName	erguardiumgroupname	Users have permissions for these tables that contain sensitive data.	Multi-value	String	No

Attributes in `erGuardiumGroup` object class

Table 7. Supported attributes in `erGuardiumGroup` object class

Attribute	Adapter attribute	Description	Single or Multi-value	Data type	Required attribute?
TableName	erGuardiumServiceGroup	Permission name on the system.	Single	String	Yes
RuleDescription	erGuardiumCriteriaName	Name of criteria type (type of sensitive data).	Multi-value	String	No
TaxonomycriteriaID	erTaxonomyCriteria	A unique identifier that matches with the taxonomy criteria for business activity mapping.	Multi-value	String	No

Chapter 6. GDPR reports overview

Entitlement reviews are the process of validating and ensuring that users have appropriate privileges that are required to perform their duties. Guardium predefined database entitlement or privilege report provides the information about who has access to GDPR data contained in databases.

Custom database entitlement reports are used to save configuration time and facilitate the uploading and reporting of data from the databases.

The Guardium GDPR Adapter imports the GDPR-related reports that are generated at Guardium environment into Verify Governance Identity Manager. The GDPR report that is created in Guardium is a custom entitlement report, which shows Grantees or User IDs and their table level entitlements or permissions.

Generated reports can be accessed through REST API commands. Therefore, `HTTPClientConnector` available in the Security Directory Integrator is used to connect to the appliance or report URL.

The adapter requires the following two reports to perform reconciliation:

- User Data Reconciliation: Entitlement report for user to permission mapping
- Support Data Reconciliation: Entitlement report for permission to taxonomy criteria mapping

Creating DB2 reports

You can configure and create customized DB2 reports.

Before you begin

You must complete the following prerequisites to create or generate GDPR reports.

- Install and configure Guardium for a database discovery and classification.
- A user must have administrative privileges for IBM Security Identity Governance and Intelligence server.

Procedure

1. Work with classification processes and view classification results. Complete the following steps.
   a) Log on to IBM Guardium.
   b) Open the Classification Process Builder by navigating to **Discover** > **Classification** > **Classification Process Builder** > **.**
   c) From the Classification Process Builder, click **ADD (+)** icon to open the **Define Classification Process** panel.
   d) Enter a name for the process in the **Process Description** box.
   e) Select a `Classification Policy` from the list or click **Modify** to create a new policy.
   f) In **Classification Policy Finder** panel, click **ADD (+)** to create a new policy.
   g) In **Classification Policy Definition**, provide the name, category, and description of the policy.
   h) Click **Apply**.
   i) Click **Edit Rules ..** to add the rules.
   j) In **Classification Policy Rules** panel, click **Add Rule**.
   k) In **Classification Rule** panel, provide rule name, category, classification, description, and rule type as per your GDPR data classification requirement.

      Note: Description in this panel is the `Taxonomy Criteria Name` for the `Permission to Business Activity` mapping activity.
   l) Click **Apply**.

m) Return to **Define Classification Process** window.

n) Select the newly created classification policy.

o) Add the data source for the database server. Make sure that the test connection to the database is successful.

p) Click **Apply**.

q) To view results, click **Run once now**.

This report displays all the table names and their respective column names that contain the GDPR data as per rules, policies, or processes that you defined.

2. Join the classification process with an entitlement report.

You can use predefined database entitlement or privilege report in Guardium to see who has access to GDPR data in databases. Complete the following steps.

a) Search for the `CUSTOM DOMAIN BUILDER` in the user interface search box.

b) Under the **Domain Finder**, click **ADD (+)**.

c) Provide a domain name.

d) Click **Filter**.

e) Clear the **Custom** box for available entities.

f) Click **Save**.

g) From the **Available entities** list, select `Classification Process Results` and move it to the right pane in **Domain entities**.

h) Select the applicable entitlement report from the left pane.
For example, select `DB2 Table Level Privs`.

i) Click **Add Pair** and move `DB2 Table Level Privs` to right pane with `Classification Process Results`.

j) Select the `Timestamp Attribute` and click **Apply**.

Custom domain is now complete. Click **Back**.

3. Generate the database entitlement reports.

a) Search for the `CUSTOM QUERY BUILDER` in the user interface search box.

b) Under the **Domain Finder**, find the domain name that was created in the previous step.

c) Select the domain name and click **Search**.

4. In next **Query Finder** screen, select the **Main Entity**, and click **ADD (+)**.
5. Provide the query details.

Note: The field **Query Name** field is the **Entitlement Report for GDPR classification** on the service form.

6. Click **Next**.
7. On the next screen, from the entities in the left pane, add conditions and field values.
8. After you add all fields, in the right pane, enable **Order By** box for **GRANTEE** attribute.

Note: The **Order By** clause column that creates entries on the service form, is different for both the following reports.

- User Data Reconciliation - Entitlement report for user to permission mapping must be order by `GRANTEE`.
- Support Data Reconciliation - Entitlement report for permission to taxonomy criteria mapping must be order by `TABSCHEMA`.

9. Click **Save**.
10. Click **Create Report**.
11. After the report is created, click **Add to My Custom Reports**.

Results

The custom reports are available under **Reports** > **My Custom Reports** > **Query Name**.

Creating Oracle12c reports

You can configure and create customized Oracle12c reports.

Before you begin

You must complete the following prerequisites to create or generate Oracle12c reports.

- Install and configure Guardium for a database discovery and classification.
- A user must have administrative privileges for IBM Security Identity Governance and Intelligence server.

Procedure

1. Work with classification processes and view classification results. Complete the following steps.
   a) Log on to IBM Guardium.
   b) Open the Classification Process Builder by navigating to **Discover** > **Classification** > **Classification Process Builder** > **.**
   c) From the Classification Process Builder, click **ADD (+)** icon to open the **Define Classification Process** panel.
   d) Enter a name for the process in the **Process Description** box.
   e) Select a `Classification Policy` from the list or click **Modify** to create a new policy.
   f) In **Classification Policy Finder** panel, click **ADD (+)** to create a new policy.
   g) In **Classification Policy Definition**, provide the name, category, and description of the policy.
   h) Click **Apply**.
   i) Click **Edit Rules ..** to add the rules.
   j) In **Classification Policy Rules** panel, click **Add Rule**.
   k) In **Classification Rule** panel, provide rule name, category, classification, description, and rule type as per your GDPR data classification requirement.

      Note: Description in this panel is the `Taxonomy Criteria Name` for the `Permission to Business Activity` mapping activity.
   l) Click **Apply**.
   m) Return to **Define Classification Process** window.
   n) Select the newly created classification policy.
   o) Add the data source for the database server. Make sure that the test connection to the database is successful.
   p) Click **Apply**.
   q) To view results, click **Run once now**.

      This report displays all the table names and their respective column names that contain the GDPR data as per rules, policies, or processes that you defined.
2. Join the classification process with an entitlement report.

   You can use predefined database entitlement or privilege report in Guardium to see who has access to GDPR data in databases. Complete the following steps.
   a) Search for the `CUSTOM DOMAIN BUILDER` in the user interface search box.
   b) Under the **Domain Finder**, click **ADD (+)**.
   c) Provide a domain name.
   d) Click **Filter**.

e) Clear the **Custom** box for available entities.

f) Click **Save**.

g) From the **Available entities** list, select `Classification Process Results` and move it to the right pane in **Domain entities**.

h) Select the applicable entitlement report from the left pane.
For example, select `ORA Object Privileges`.

i) Provide column name on which join condition to be applied

j) Click **Add Pair** and move `ORA Object Privileges` to right pane with `Classification Process Results`.

k) Select the `Timestamp Attribute` and click **Apply**.

l) Open `Custom Table Builder` in the user interface search box.

m) Select the entity you have selected in `Custom Table Builder` and click **Upload Data**. For Oracle select `ORA Object Privs`.

n) Click on **Add Data source** to add Oracle Database.

o) Click **Run Once Now** button.

Success messages are displayed with total records inserted.

p) Click **OK**.

3. Generate the database entitlement reports.

a) Search for the `CUSTOM QUERY BUILDER` in the user interface search box.

b) Under the **Domain Finder**, find the domain name that was created in the previous step.

c) Select the domain name and click **Search**.

d) In next **Query Finder** screen, select the **Main Entity**, and click **ADD (+)**.

e) Provide the query details.

Note: The field **Query Name** field is the **Entitlement Report for GDPR classification** on the service form.

f) On the next screen, from the entities in the left pane, add conditions and field values.

g) After you add all fields, in the right pane, enable **Order By** clause for the **GRANTEE** attribute.

h) Include fields **Rule Description** and **Schema** from `Classification Process Result` in left pane

i) Right click on `PRIVILEGE` and click **Add Condition**.

j) Under operator select `LIKE` and mention `SELECT`.

k) Check the **Add Distinct** check box to generate the final report with Unique records.

l) Save the query.

m) Click **Create Report**.

n) After the report is created, click **Add to My Custom Reports**.

Note: The **Order By** clause column that creates entries on the service form, is different for both the following reports.

- User Data Reconciliation - Entitlement report for user to permission mapping must be order by `GRANTEE`.
- Support Data Reconciliation - Entitlement report for permission to taxonomy criteria mapping must be order by `SCHEMA`.
- The **Rule Description** field is a must in the Support Data Reconciliation report.
- The `Data source` type is a must in the User Data Reconciliation and Support Data Reconciliation report.

Results

The custom reports are available under **Reports** > **My Custom Reports** > **Query Name**.

Creating MSSQL reports

You can configure and create customized MSSQL reports.

Before you begin

You must complete the following prerequisites to create or generate MSSQL reports.

- Install and configure Guardium for a database discovery and classification.
- A user must have administrative privileges for IBM Security Identity Governance and Intelligence server.

Procedure

1. Work with classification processes and view classification results. Complete the following steps.
   a) Log on to IBM Guardium.
   b) Open the Classification Process Builder by navigating to **Discover** > **Classification** > **Classification Process Builder** > **.**
   c) From the Classification Process Builder, click **ADD (+)** icon to open the **Define Classification Process** panel.
   d) Enter a name for the process in the **Process Description** box.
   e) Select a `Classification Policy` from the list or click **Modify** to create a new policy.
   f) In **Classification Policy Finder** panel, click **ADD (+)** to create a new policy.
   g) In **Classification Policy Definition**, provide the name, category, and description of the policy.
   h) Click **Apply**.
   i) Click **Edit Rules ..** to add the rules.
   j) In **Classification Policy Rules** panel, click **Add Rule**.
   k) In **Classification Rule** panel, provide rule name, category, classification, description, and rule type as per your GDPR data classification requirement.

      Note: Description in this panel is the `Taxonomy Criteria Name` for the `Permission to Business Activity` mapping activity.
   l) Click **Apply**.
   m) Return to **Define Classification Process** window.
   n) Select the newly created classification policy.
   o) Add the data source for the database server. Make sure that the test connection to MSSQL is successful.
   p) Click **Apply**.
   q) To view results, click **Run once now**.

      This report displays all the table names and their respective column names that contain the GDPR data as per rules, policies, or processes that you defined.
2. Join the classification process with an entitlement report.

   You can use predefined database entitlement or privilege report in Guardium to see who has access to GDPR data in databases. Complete the following steps.
   a) Add the database to the applicance and assign data sources to entitlements.
   b) Navigate to **Comply** > **Custom Reporting** > **Custom Table Builder**.
   c) Click **Upload Definition**.
   d) Provide a name for **Entity Description** and **Table Name**.

e) Place the this statement under the SQL statement: `EXEC sp_table_privileges @table_name = '%';`.

f) Click **Add Data source** and select your MS SQL database.

g) Click **Retrieve**.

You see the report under **Custom Tables**.

h) Click **Run Once Now** and new insets should be imported.

i) Navigate to **Comply** > **Custom Reporting** > **Custom Domain Builder**.

j) Search for the `CUSTOM DOMAIN BUILDER` in the user interface search box.

k) Under the **Domain Finder**, click **ADD (+)**.

l) Provide a domain name.

m) Click **Filter**.

n) Clear the **Custom** box for available entities.

o) Click **Save**.

p) From the **Available entities** list, select `Classification Process Results` and move it to the right pane in **Domain entities**.

q) Select the applicable entitlement report from the left pane. It is the same as the one created above.

r) Provide the input join condition.

s) Click **Add Pair** and move applicable entity selected above to the right pane with `Classification Process Results`.

t) Select the `Timestamp Attribute` and click **Apply**.

3. Generate the database entitlement reports.

a) Navigate to **Comply** > **Custom Reporting** > **Custom Query Builder**.

b) Under the **Domain Finder**, find the domain name that was created in the previous step.

c) Select the domain name and click **Search**.

d) Click **ADD (+)** to add a new query.

e) Enter a name and select the domain from the **Main Entity** dropdown.

f) Provide the query details.

Note: The field **Query Name** field is the **Entitlement Report for GDPR classification** on the service form.

g) Build query for the report.

h) Drag the entities shown from the left pane into the query.

i) After you add all fields, in the right pane, enable **Order By** clause for **GRANTEE** attribute.

j) Include fields **Rule Description** and **Schema** from `Classification Process Result` in left pane

k) Right click on `PRIVILEGE` and click **Add Condition**.

l) Under operator select `LIKE` and mention `SELECT`.

m) Check the **Add Distinct** check box to generate the final report with Unique records.

n) Click **Save**.

o) Click **Create Report**.

p) After the report is created, click **Add to My Custom Reports**.

Results

The custom reports are available under **Reports** > **My Custom Reports** > **Query Name**.

Creating Support data reports

You can create custom Support data reports.

About this task

Steps for generating the Support Data report for DB2, Oracle and MSSQL databases are the same.

Procedure

1. Click the **Edit the Query For This Report** icon on the User Data report created in one of the following reports:
   - GDPR reports
   - Oracle 12c reports
   - MSSQL reports
2. Click **Clone** to clone the report.
3. In the clone report, select `Order By` for `Schema` field.

   Note: Select TABSCHEMA if you are generating for DB2.
4. Save the report.
5. Regenerate the report.
6. Click **Add To My Custom Report** to add the report to custom report.

Bulk loading

The business activities must be defined in IBM Security Verify Governance Identity Manager before permissions can be mapped to a business activity. Verify Governance Identity Manager provides an option to bulk load business activities.

Importing activities with bulk upload

Use a bulk upload file to load business activities.

Procedure

1. Log in to the IBM Security Verify Governance Identity Manager Administration Console.
2. On the **Access Risk Controls** tab, select **Tools** > **Bulk Data Load**.
3. Click **Insert Activities Hierarchy** and upload the **IGI Bulk Load Activities File**, `Insert+Activities+Hierarchy_GDPR.xlsx`.
4. Refresh the operation until it is complete.

Contents of Activities Bulk Load file

The file format is the pre-determined format of the bulk load files in Identity server.

Table 8.

Information	Description	Validation
CODE	Activity code	Mandatory
ACTIVITY	Activity name	Mandatory
ENVIRONMENT	Environment identifier name	Optional
DESCRIPTION	Activity description	Optional
PARENT_CODE	Activity parent code	Optional

The **ENVIRONMENT** field is optional. If this field is populated, the existence of an environment with the specified name is verified. Otherwise, the row is skipped. If left blank, the default environment is used (Working Environment).

The **CODE** and **ACTIVITY** fields contain the activity code and name, respectively. The existence of an activity with the given code is verified. If the given name does not match the activity name, the row is skipped. If there is no such activity, it is inserted.

The **PARENT_CODE** field is used for positioning the activity in the hierarchy. If this field is left blank, the activity is inserted as a child of the root activity. If there is no such activity associated to the given parent code, the activity is inserted as a child of a technical activity called "Undefined", which is created as needed.

The table shows a sample of the bulk load file:

	A	B	C	D	E
1	**CODE**	**ACTIVITY**	**ENVIRONMENT**	**DESCRIPTION**	**PARENT_CODE**
2	**GDPR**	**GDPR**			**Root**
3	**42**	**Credit Cards**			**GDPR**
4	**74**	**Passwords**			**GDPR**

Accessing GDPR reports through REST API

To authenticate to the Guardium REST API, a client ID must be registered in Guardium and the associated client secret retrieved. Registering a client ID is done by using the `grdapi` command line utility of Guardium.

Procedure

1. Create a client ID.
   a) Log in to Guardium command line interface by using SSH.
   b) Run the `grdapi` command line utility of Guardium.

```
grdapi register_oauth_client client_id=gdpr ID=0
{"client_id":"gdpr","client_secret":"164ae54e-b03c-
4366-bd43-9e38bdd562f1",
"grant_types":"password","scope":"read,write","redirect_uri"
:"https://someApp"}
ok
```

   c) Save the client secret.
2. Provide the `client_id` and `client_secret` in the HTTP URL for Guardium appliance.
   For example,

```
https://<Guardium_Host><Port_Number>/oauth/token?
client_id=<client_ID>&grant_type=password&client_secret=<Client_Secret>&username=<Admin_Accou
nt>&password=<Password>
```

Guardium GDPR Adapter Taxonomy Mapping properties file

During the Guardium GDPR adapter reconciliation operation, values in the `Rule Description` column of the **Support Data report** is mapped to `Activity` on IBM Security Verify Governance Identity Manager. For Guardium GDPR Adapter, the **Def file** consist of `Criteria Name` and `relevant Criteria_ID`. For example, `Credit Card=42`.

This file must be present on the TDI machine and the file path must be specified on the service form with label the `Taxonomy Criteria Name-ID` mapping file path. `Criteria Name` in **Def file** is the same as

the value for Rule Description column in the final **Support Data report**. For example, Credit Cards and Passwords are the values under the Rule Description column in **Support Data report**. This means that Credit Cards and Passwords are the values for Criteria Name in the **Def file** .

Criteria_ID in the **Def file** must have the same values as the CODE column in Insert+Activities +Hierarchy_GDPR.xlsx. For example, in "Contents of Activities Bulk Load file" on page 25, the table shows that the value under CODE is 42 for Credit Cards. This means that the code for Criteria_ID and Credit Cards is 42 in the **Def file**.

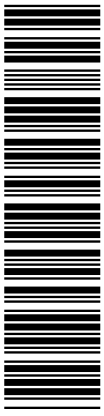
The Guardium application does not have Criteria_ID of its own. It fetches the Criteria_ID from the **Def file** based on the **Criteria Name** that it retrieves from the Rule Description column. Taxonomy Criteria is the relevant Criteria_ID that is present in the **Def file** for the particular Criteria Name. The adapter uses this mapping file to retrieve the Criteria_ID while it is returning the report entry to IBM Security Verify Governance Identity Manager.

If there is another GDPR adapter (For example, StealthBits GDPR adapter) on IBM Security Verify Governance Identity Manager, and the bulk load for activity is already done, we can reuse the activity that is common with Guardium. In such a scenario, for correct activity to permission mapping Guardium adapter must return the Criteria_ID values with Table permission, that matches the activity ID value that is already bulk loaded on IBM Security Verify Governance Identity Manager. This can be accomplished when the Criteria_ID of bulk loaded data on IBM Security Verify Governance Identity Manager is the same in the **Def file**. For example, if the bulk loaded data on Verify Governance Identity Manager contains Credit Cards=43, then the **Def file** must also contain Credit Cards=43.

Note:

1. **Def file** is vital for Activity to Permission Mapping as it is the only source for the adapter to fetch Criteria_ID. For below cases **Guardium GDPR Adapter** uses Criteria Name as Criteria_ID:
   - If **Def file** path mentioned on service form is incorrect
   - If the file is present on mentioned path but is empty
   - If Criteria Name present in Rule Description column of Support Data report is not present in **Def file**
   - If Criteria_ID for Criteria Name is empty
2. Criteria_ID not necessary to be numeric value only. It can be alphanumeric value also but it should be in sync with Insert+Activities+Hierarchy_GDPR.xlsx

Part Number: 99F1234
Product Number: 1234-SS1



BA21-8475-00