IBM Security Identity Governance and Intelligence
Version 5.2.3.1

Troubleshooting and Support Topics

IBM Security Identity Governance and Intelligence
Version 5.2.3.1

Troubleshooting and Support Topics

Table of contents

Table list

Chapter 1. Diagnostic tools

Diagnostic tools that capture and record details about how the program operates. The information can help locate the product or component from which an error originates.

Logs The virtual appliance records system events during specific transactions. Log files contain levels of information about the product processes. Log files also include information about other software that is used to complete a task. Use the information in log files to facilitate isolating and debugging system problems.

Traces Trace data provides in-depth processing information to help you focus on a particular area that you suspect is causing a problem. Trace data is more complex and detailed than message data.

To view the virtual appliance event log, see Viewing the event logs. For information about viewing and configuring component-specific and virtual appliance log and trace files, see Managing the log configuration.

Chapter 2. Troubleshooting virtual appliance problems

The following topics describe solutions for problems that involve the virtual appliance.

When a Postgres database is reset on the primary node in a cluster, the slave database retains the data

If you reset the master Postgres database on the primary node, the data is removed from the master only. The slave Postgres database on the secondary node retains the existing data. The slave database cannot be reset on the secondary node.

Solution

To remove the old data from the slave database, you must use the **Force Synchronization** option. See Managing the PostgreSQL database.

The Identity Governance and Intelligence application is inaccessible after a Postgres database failover

After you perform a Postgres failover, you are unable to log in to the Identity Governance and Intelligence administration console.

Problem

You performed a Postgres failover. When you log in to the Identity Governance and Intelligence administration console, you receive the following error in your browser:

```
Exception thrown by application class 'com.vaadin.server.VaadinServlet.service:366'

javax.servlet.ServletException: com.vaadin.server.ServiceException: java.lang.NullPointerException
at com.vaadin.server.VaadinServlet.service(VaadinServlet.java:366)
at com.ibm.igi.toolkit.web.gestione.servlet.CIServlet.service(Unknown Source)
at javax.servlet.http.HttpServlet.service(HttpServlet.java:790)
at com.ibm.ws.webcontainer.servlet.ServletWrapper.service(ServletWrapper.java:1290)
at [internal classes]
Caused by:
com.vaadin.server.ServiceException: java.lang.NullPointerException
at com.vaadin.server.VaadinService.handleExceptionDuringRequest(VaadinService.java:1464)
at com.vaadin.server.VaadinService.handleRequest(VaadinService.java:1421)
at com.vaadin.server.VaadinServlet.service(VaadinServlet.java:364)
... 4 more
Caused by:
java.lang.NullPointerException:
at com.vaadin.server.AbstractClientConnector.getAllChildrenIterable(AbstractClientConnector.java:508)
at com.vaadin.ui.ConnectorTracker.markConnectorsDirtyRecursively(ConnectorTracker.java:605)
at com.vaadin.ui.ConnectorTracker.markConnectorsDirtyRecursively(ConnectorTracker.java:607)
at com.vaadin.ui.ConnectorTracker.markConnectorsDirtyRecursively(ConnectorTracker.java:607)
at com.vaadin.ui.ConnectorTracker.markAllConnectorsDirty(ConnectorTracker.java:581)
at com.vaadin.server.LegacyCommunicationManager.repaintAll(LegacyCommunicationManager.java:424)
at com.vaadin.server.communication.UIInitHandler.synchronizedHandleRequest(UIInitHandler.java:76)
at com.vaadin.server.SynchronizedRequestHandler.handleRequest(SynchronizedRequestHandler.java:41)
at com.vaadin.server.VaadinService.handleRequest(VaadinService.java:1409)
... 5 more
```

Solution

Search the IBM® Security Identity Governance and Intelligence Application server `messages.log` file for the following the exception.

```
org.postgresql.util.PSQLException: FATAL:
terminating connection due to administrator command:
org.postgresql.util.PSQLException:
An I/O error occurred while sending to the backend.:
java.io.EOFException
```

See Retrieving logs.

To correct this issue, you must restart the Identity Governance and Intelligence server.

The Identity Governance and Intelligence application is inaccessible after a Postgres database failover/failback

Following a Postgres failover recovery procedure, you are unable to log in to the Identity Governance and Intelligence administration console.

Problem

You ran a Postgres failover recovery procedure. When you log in to the Identity Governance and Intelligence administration console, you receive the following error in your browser:

```
Exception thrown by application class 'com.vaadin.server.VaadinServlet.service:366'

javax.servlet.ServletException: com.vaadin.server.ServiceException: java.lang.NullPointerException
at com.vaadin.server.VaadinServlet.service(VaadinServlet.java:366)
at com.ibm.igi.toolkit.web.gestione.servlet.CIServlet.service(Unknown Source)
at javax.servlet.http.HttpServlet.service(HttpServlet.java:790)
at com.ibm.ws.webcontainer.servlet.ServletWrapper.service(ServletWrapper.java:1290)
at [internal classes]
Caused by:
com.vaadin.server.ServiceException: java.lang.NullPointerException
at com.vaadin.server.VaadinService.handleExceptionDuringRequest(VaadinService.java:1464)
at com.vaadin.server.VaadinService.handleRequest(VaadinService.java:1421)
at com.vaadin.server.VaadinServlet.service(VaadinServlet.java:364)
... 4 more
Caused by:
java.lang.NullPointerException:
at com.vaadin.server.AbstractClientConnector.getAllChildrenIterable(AbstractClientConnector.java:508)
at com.vaadin.ui.ConnectorTracker.markConnectorsDirtyRecursively(ConnectorTracker.java:605)
at com.vaadin.ui.ConnectorTracker.markConnectorsDirtyRecursively(ConnectorTracker.java:607)
at com.vaadin.ui.ConnectorTracker.markConnectorsDirtyRecursively(ConnectorTracker.java:607)
at com.vaadin.ui.ConnectorTracker.markAllConnectorsDirty(ConnectorTracker.java:581)
at com.vaadin.server.LegacyCommunicationManager.repaintAll(LegacyCommunicationManager.java:424)
at com.vaadin.server.communication.UIInitHandler.synchronizedHandleRequest(UIInitHandler.java:76)
at com.vaadin.server.SynchronizedRequestHandler.handleRequest(SynchronizedRequestHandler.java:41)
at com.vaadin.server.VaadinService.handleRequest(VaadinService.java:1409)
... 5 more
```

or

```
Error 500:javax.servlet.ServletException:com.vaadin.server.ServiceException:java.lang.NullPointerException
```

Solution

Search the `IBM Security Identity Governance and Intelligence Application` server `messages.log` file for the following exception.

```
org.postgresql.util.PSQLException: FATAL:
terminating connection due to administrator command:
org.postgresql.util.PSQLException:
An I/O error occurred while sending to the backend.:
java.io.EOFException
```

See Retrieving logs.

To overcome this problem, you must restart the Identity Governance and Intelligence server.

DB2 reconfiguration validation fails after ACR takeover on standby

After a DB2 failover with automatic client rerout (ACR), you receive a connection error when you try to reconfigure DB2 on the primary node.

Cause

Database configuration validation is done on the primary Database. It is not done on the ACR nodes.

Solution

When you reconfigure the database on the primary node, you must make the ACR takeover database the primary database. Use the database name, port, and password of the takeover database when you reconfigure the **Connection** tab.

When you change the virtual appliance password, the Postgres database password does not change

By default Postgres Administrator user password is set the same as virtual appliance administrator password. Changing the virtual appliance administrator password does not change the password for the Postgres database administrator.

Problem

Although initially set to use the same password, the virtual appliance and the Postgres database passwords are changed independently. If you change the virtual appliance administrator password, that password does not work for the Postgres administrator.

Solution

To change the Postgres database administrator password for the first time, you must use the virtual administrator password that was set during the initial virtual appliance configuration. For information about how to change the Postgres administrator password from the Postgres Management page, see Changing the Postgres database password.

Node activation fails

Before new member node activation, if the primary nodes password is changed, and the other exiting member nodes are not synchronized, then the new member node activation fails.

Note: If the existing member nodes are unreachable or shut down, new member activation does work.

Solution

Before you activate new member nodes in a cluster, make sure that all the existing nodes in the cluster have the same password.

Error *Certificate key size exceeds the java security policy restriction* in member node

When you activate a member node after updating the Java security policy JAR files, you get message *Certificate key size exceeds the java security policy restriction error*.

Problem

After you update the Java security policy JAR files on the primary node, and you run `Test Connection` in the initial configuration wizard to activate a member node of the cluster, the following error message is displayed on the member node:

```
Certificate key size exceeds the java security policy restriction error
```

Cause

You modified the Java security policy JAR files on the primary node, but you failed to update them on the member node. The Java security policy JAR files must be identical on all nodes of a cluster.

Solution

Update the JAR files also on the member node. Follow these steps on the member node:

1. Follow the procedure described in Updating the JAVA security policy JAR files to upload the same JAR files that the primary node uses
2. Restart the Local Management Interface of the virtual appliance

Cannot reconnect a secondary node

You cannot reconnect a replaced secondary node to the cluster environment.

Problem

You shut down the secondary node in a cluster environment and removed it. Then, you promoted a member node to be the new secondary. You restarted the old secondary node and tried to reconnect it to the cluster. The reconnection fails.

Solution

If you want to reuse this node in the same cluster, you must deploy the `iso` image and activate the node through the primary node.

Default gateway is lost when M.2 is enabled

If you enable M.2 and set it as the default interface, the default gateway is lost from the **Manage** > **Routes** page. If you enter the gateway address in the **IPv4 Gateway** field, the **Save** button remains disabled.

Cause

The **Save** button is disabled because the correct gateway address is already in the backend.

Solution

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **Routes**.
2. On the **Static Routes** page, enter an incorrect gateway in the **IPv4 Gateway** field.
3. Click **Save**. The user interface is restarted automatically.
4. Enter the correct gateway address in the **IPv4 Gateway** field.
5. Click **Save**. The user interface is restarted automatically.

The default gateway is restored.

If an external database is configured after a Postgres failover in a cluster environment, the failover condition remains if the Postgres database is reconfigured.

If you configured an external database after you perform a Postgres failover, the data is not merged. If you want to access the data that is stored on the Postgres database, you must reconfigure the Postgres database.

Problem

When you reconfigure the Postgres database, the failover condition persists. The Postgres database on the primary node has the role of slave instead of the role of master.

Solution

Restore the master database on the primary node. See Recovering from a Postgres database failure.

Clear the service integration bus

If you encounter any configuration or login problems when you work with IBM Security Identity Governance and Intelligence, you must clear the Service Integration Bus (SIB) data from the database.

Ensure that you have the needed administrative authority. On Windows systems, the login user ID must be in the Administrators Group. On UNIX or Linux systems, the login user ID must be `root`.

To clear the**Service Integration Bus**, complete these steps.

1. Ensure that the database is running (`IGIDB`).
2. Start the DB2® command line.

   Windows

   a. Start the Windows command prompt.
   b. Run the following command:

      `set DB2INSTANCE=db2admin` where `db2admin` is the database administrator.
   c. Run **`db2cmd`** to start the DB2 command line.

   Linux Run the command `su - db2admin` where `db2admin` is the database administrator.

3. In the DB2 command line, enter the DELETE SQL statements that you require to delete all data from the tables in the Service Integration Bus schemas.

   Enter the following commands for each of the Service Integration Bus schema in your environment:

   ```
   db2 delete from schema_name.SIB000
   db2 delete from schema_name.SIB001
   db2 delete from schema_name.SIB002
   db2 delete from schema_name.SIBCLASSMAP
   db2 delete from schema_name.SIBKEYS
   db2 delete from schema_name.SIBLISTING
   db2 delete from schema_name.SIBXACTS
   db2 delete from schema_name.SIBOWNER
   db2 delete from schema_name.SIBOWNERO
   ```

   Where the Service Integration Bus schema schema_name is ITIML000 for a single server, and ITIML000, ITIML0001, ITIML002, ITIML003, and ITIMS000 are for a cluster environment. For a cluster, the number of schemas such as ITIML0001, ITIML0002, or other schemas vary depending on the number of nodes in the cluster. ITIMS000 is also one of the schema names for the cluster.

   Note: The SIBOWNER0 might not exist in all Identity data store environments. If it does not exist and the delete statement fails, you can ignore the failure.

Reset password for Identity Brokerage Adapters

To define security compliance standards and to ensure proper functioning of the Identity Brokerage Adapters, a predefined password is included with it. You might need to reset this password if all requests to the Identity Brokerage fails.

Password reset

If you have administrator permissions, you can reset the predefined password.

Administrators are typically granted administrative rights to manage business-critical applications. As an administrator, you can reset the password. Do these steps:

1. Stop the IBM Security Identity Governance and Intelligence server.
2. From the command-line interface, log on to the IBM Security Identity Governance and Intelligence virtual appliance.
3. Enter the **help** command at the igivasrv prompt for a list of available commands.
4. Enter the **igi** command at the igivasrv prompt.
5. Enter the **utilities** command at the igivasrv:igi prompt for a list of available commands.
6. Enter the **ib_settings** command at the igivasrv:utilities prompt for a list of available commands.
7. Enter the **ib_password_reset** command at the igivasrv:ib_settings prompt.
8. Enter **YES** to confirm the password reset. The message Password reset successful is displayed.
9. Restart the IBM Security Identity Governance and Intelligence server.

Note: A reset password complies with the configured password policy.

Settings are not synchronized

In a high availability environment, after you reset the password using the virtual appliance command-line interface (CLI), the change is not synchronized across all the nodes in the virtual appliance cluster.

To resolve this issue, synchronize the nodes. See Synchronizing a member node with a primary node..

Cluster problems occur after the application of a snapshot to the primary node

Cluster issues that occur after you apply a snapshot might be caused by a password change on the primary node.

After you apply a snapshot to a primary node and restart the nodes, you might see the following issues:

- Node status is **Undetermined**.
- Synchronization shows **Error**.

Typically these issues occur if the password on the primary node was changed after the snapshot was created. You must update the password on the restored primary node to the current password, then restart the nodes.

Application login fails

If you update the IBM Security Identity Governance and Intelligence default personal certificate, you might encounter a login problem.

The virtual appliance generates a certificate by default. You can use your own personal certificate instead of appliance default certificate. However, you must ensure that the CN of the certificate that you generate matches with appliance application interface FQDN.

```
CN=FQDN of the application interface
```

Otherwise, you are unable to log in to the application.

Test connection fails after you promote a secondary node to primary node in cluster with PostgreSQL

In a cluster environment that uses the PostgreSQL database, when you create a new target for a service, the Test Connection function fails.

Problem

You set up a cluster environment that uses the PostgreSQL database. When you create a new target for a service, for example LDAP, the Test Connection function fails.

Cause

This failure occurs in two situations:

- The master PostgreSQL database is reset from the Postgres Management pane.

- Replication is not running, and the secondary node is promoted to primary node.

Solution

Restore the backup of the PostgreSQL database by using an external client or utility.

Note: If a database backup is not available, from the Database Server Configuration pane, first unconfigure the PostgreSQL database, and then configure it again.

Virtual appliance periodically logs GLGUP1012E System Events

The virtual appliance periodically logs GLGUP1012E System Events.

Problem

The following message is logged in the **Monitor** > **Logs** > **Event Logs** page of the virtual appliance:

```
GLGUP1012E An attempt to download the primary update catalog has failed. Common
causes of this failure are not having a license installed and DNS errors.
```

Cause

There is a periodic check, even if the virtual appliance is configured not to connect over the internet.

Solution

Follow these steps to prevent this message from being logged:

1. In the virtual appliance dashboard, select **Manage** > **System settings** > **Advanced Tuning Parameters**.
2. In the Advanced Tuning Parameters pane, click **New**.
3. Create the `update.disable.remote.discovery` key and set 1 as its value.

   With `update.disable.remote.discovery` set to 1 (true), the appliance no longer searches the Internet for updates.

Note: Advanced tuning parameter values should be changed only under the supervision of IBM Customer Support.

Chapter 3. Troubleshooting Identity Brokerage Adapters

You might encounter some issues or limitations during connector integration. This section provides general information to prepare you for troubleshooting.

Verify the connector status

If connector reconciliation failed, check the connector status. The status icon links to a more detailed information about the state of the target, which can help you determine the corrective action.

See Connector Status.

Review the log files

Identity Brokerage requests can be traced for all adapters.

Tracing an adapter request requires viewing the IBM Security Identity Governance and Intelligence log files, Identity Brokerage log files, and the specific adapter log files. Logs can help you determine the background or cause of an issue and to find the proper solution.

Table 1. Log files that are related to Identity Brokerage

Category	Log files	Location
Identity Brokerage related logs	• Identity Brokerage Application Server message • Identity Brokerage Application Server system trace	You can view the Identity Brokerage log files from the Virtual Appliance Dashboard. See Retrieving logs.
IBM Security Identity Governance and Intelligence related logs	• IBM Security Identity Governance and Intelligence server message • IBM Security Identity Governance and Intelligence server system trace	You can view the log files from the IBM Security Identity Governance and Intelligence log files from the Virtual Appliance Dashboard. See Retrieving logs.
Identity Brokerage Adapter related logs	• Security Directory Integrator server logs • Adapter agent logs	You can view the Security Directory Integrator server log files from the Virtual Appliance Dashboard. See Retrieving logs. Adapter agent logs are found on the system where the agent is installed. For more information about setting agent trace level and retrieving adapter-specific logs, see the adapter documentation. **Note:** For the adapters that are installed on the virtual appliance, see the Security Directory Integrator server logs.

Set the log level

A log file records the events and messages that are communicated between entities during job processing. As such, it is important to specify the level of information to be recorded in the log file. The log level determines the granularity of the messages that are recorded in the log file. It is easier to troubleshoot or diagnose the problem if the log file provides detailed information.

You can set the log level in the Virtual Appliance Dashboard, by using the **Log Retrieval and Configuration** option. See Configuring logs.

Adapter agent log level must be set on the system where the agent is installed.

Limitations

This section contains information about known limitations in the operation of the Identity Brokerage Adapters.

For the relevant information, see the corresponding references:

- *Installation and Configuration Guide* at http://www.ibm.com/support/knowledgecenter/SSIGMP_1.0.0/com.ibm.itim_pim.doc/c_adapters_intro.htm.
- *Release Notes* at Adapters for IBM Security Identity Manager v7.0: http://www-01.ibm.com/support/docview.wss?uid=swg21687732.

Known issues and workarounds

During the operation of an Identity Brokerage Adapter, you might encounter some issues. Consult the corresponding *Installation and Configuration Guide* for the list of known issues and possible workarounds. Alternatively, visit the IBM Software Support website: https://www-947.ibm.com/support/entry/portal/support.

Warnings and error messages

A warning or error message might be displayed in the user interface to provide information about the adapter or when an error occurs. When you encounter a warning or error message, consult the corresponding *Installation and Configuration Guide* for the corrective action.

Chapter 4. Some table columns are unable to sort in the Service Center

Some table columns in the IBM Security Identity Governance and Intelligence Service Center environment cannot sort.

Workaround

You know whether the sorting function works for a particular column if an arrow appears when you click the column header of a table. If the column in a table cannot sort, this indicator does not appear when you click the column header.

Chapter 5. Modifying or removing the rights value for a string attribute causes errors

When you try to modify or remove the rights values on a required string attribute mapping, a 500 account modification error occurs. Although the error is displayed in the **Monitor** > **OUT events** tab, the operation is successful. You can ignore the error.

Symptoms

When you try to modify or remove the rights values on a required string attribute, the following error occurs: `500 Account modification failed. com.ibm.di.connector.MOD_FAILED [Error: usermod: group does not exist]`. The error does not accurately describe the problem. Although the error message occurs, the operation is successful.

Diagnosing the problem

To see the problem, follow these steps as an example:

1. In the Target Administration Console, create a Linux target. See Creating targets.
2. Click **Access Governance Core**.
3. Select **Manage** > **Accounts**.
4. In the **Account Configuration** pane, select the Linux account and click the Attribute-to-Permission Mapping tab.
5. In the **Attribute-to-Permission Mapping** tab, select **Actions** > **Discover account attributes from target**.
6. On the Discover Attributes from Target page, select the `erPosixPrimaryGroup` attribute, and then click **Import**.
7. Edit the `erPosixPrimaryGroup` attribute by selecting it and clicking **Actions** > **Edit**.
8. On the Edit Attribute Mapping page, adding attribute values and rights values to the `erPosixPrimaryGroup` attribute by clicking **Add Value**. For example, set an attribute-rights mapping as follows:

   Attribute value
   mail

   Rights value
   mail

   Then, click **Add Value** again and set another attribute-rights mapping as follows:

   Attribute value
   users

   Rights value
   users

   Click **Save**, and then click **OK**. The mail group and the users group are default groups from the Linux target.
9. Enable the `erPosixPrimaryGroup` attribute by clicking **Actions** > **Enable**, and then click **OK**.

10. Add an organizational unit to the `erPosixPrimaryGroup` attribute by clicking **Manage** > **Roles**.
11. Select the `erPosixPrimaryGroup` permission in the left pane, and click the **Organization Units** tab.
12. In the **Organization Units** tab, click **Actions** > **Add**.
13. Select an organizational unit and click **OK**. Then, click **OK** again.
14. Create a user. See Adding a user.
15. Add the Linux account for this user by clicking **Manage** > **Users**.
16. In the left pane, select the user and click the **Accounts** tab.
17. In the **Accounts** tab, click **Actions** > **Add**. Select the Linux account, and then click **Save** and **OK**. Make sure that the account is created successfully.
18. In the left pane, select the user and click the **Entitlements** tab. Then, click **Actions** > **Add**.
19. Select the `erPosixPrimaryGroup` attribute and click **OK**.
20. On the Associated Rights page, click "..." to show the rights values. In the **Available** column, select **mail** and click the arrow to move the mail value to the **Assigned** column. Then, click **OK** until the **Entitlements** tab is displayed.
21. Click **Monitor** > **OUT events** to ensure that the *Add Permission* operation is successful.
22. Click **Manage** > **Users**.
23. In the left pane, select the user and click the **Entitlements** tab.
24. Modify the rights value by clicking **Actions** > **Add**.
25. Select the `erPosixPrimaryGroup` attribute and click **OK**.
26. On the Associated Rights page, click "..." to show the rights values. Move **mail** to the **Available** column. Then, move **users** to the **Assigned** column. Then, click **OK** until the **Entitlements** tab is displayed.
27. Click **Monitor** > **OUT events** to see the 500 error.

Resolving the problem

Although the error is displayed in the **OUT events** tab, the operation is successful. You can ignore the error.

Chapter 6. Pagination footer cannot be fully displayed

In the **Access Optimizer** > **Configure** panel, the pagination footer cannot be fully displayed even if you use the horizontal bar to scroll through the entire panel.

This issue occurs in the following tabs:

- **Data Snapshot**
- **Access Dataset**
- **Relevance Criteria**

Solution: Expand the table. Drag the table border horizontally to view the hidden footer icons and to collapse it back if needed.

Chapter 7. Role data does not show up in Identity Governance and Intelligence after the reconciliation of an LDAP, AIX, Linux, HPUX, or Solaris target

Due to a failure in initial VA configuration, Identity Governance and Intelligence fails to reconcile groups (*Roles*) for targets of a default target type: LDAP, AIX, Linux, HPUX, or Solaris. Any subsequent operations that use the groups fail because they are not successfully imported into Identity Governance and Intelligence.

This issue happens if the loading of default target profiles (LDAP, PosixAix, PosixHpux, PosixLinux, and PosixSolaris) is incomplete during configuration of the virtual appliance. During the profile load, some information from the profile JAR file is added to the Identity Governance and Intelligence database. If the service that adds this data is not available before the profile load is initiated, the required data is not be added to the database. This issue is a race condition during the configuration process that does not happen every time.

The user can determine whether they have the configuration failure (it does not happen on every Identity Governance and Intelligence virtual appliance installation) in one of the following ways:

- Look for errors in the Identity Governance and Intelligence virtual appliance logs immediately after configuration.
  1. From the virtual appliance dashboard, Click **Manage** > **System Settings/Support Files**.
  2. Click **New**, and add a comment. Then, click **Save Configuration**.
  3. After the support package is created, download it and examine the files in the `var/ibm/tivoli/common/CTGIM/logs` folder. In particular, look for error messages in the trace points with these sources.`<Source FileName="com.ibm.iga.ilc.ib.client.rest.IdentityBrokerageRestClient" Method="post"/>` and `<Source FileName="com.ibm.itim.remoteservices.installation.ServiceProfileLoader" Method="loadTargetProfileDefinition"/>`.
- Look for missing role data after target reconciliation.
  1. Create a target of type LDAP, AIX, Linux, HPUX, or Solaris and make sure that some groups are defined on the target.
  2. Reconcile the target.
  3. In the Identity Governance and Intelligence console, click **Manage** > **Roles**.
  4. Click **Filter** and specify your target's application name in the **Application** field.
  5. Click **Search**. If you have the issue, you do not see any entries.
- If you have access to the database, examine the Identity Governance and Intelligence database.
  1. Connect to the Identity Governance and Intelligence database.

     If you have the issue, you see no data for the default profiles (LdapProfile, PosixAixProfile, PosixHpuxProfile, PosixLInuxProfile, and PosixSolarisProfile) in the following tables:

     ```
     ITIMUSER.IB_TARGET_PROFILE
     ```

```
ITIMUSER.IB_TARGET_RESOURCE_SCHEMA_EXT
ITIMUSER.IB_TARGET_RESOURCE_TYPE
```

Solution Manually import these profiles:

- LdapProfile
- PosixAixProfile
- PosixHpuxProfile
- PosixLinuxProfile
- PosixSolarisProfile

1. Download the *adapter*.zip package from the IBM Passport Advantage website and extract the files. Go to http://www.ibm.com/software/how-to-buy/passportadvantage/pao_customers.htm.
2. From the Identity Governance and Intelligence console **Home** page, click **Target Administration**.
3. In the Tasks panel, click **Manage Target Types**.
4. On the Manage Target Types panel, click **Import...**.
5. Click **Browse** to locate and select the profile.jar file that was extracted from the adapter package.
6. Click **Ok** to import the adapter profile.

Chapter 8. Map issues in Role Compare

Perform a role compare by selecting **Access Governance Core** > **Monitor** > **Role Compare**. Select a role with many permissions that are assigned to many users and click **Compare**. If you move the verticle separator all the way to the right and then back to the center, the map information disappears.

Cause

This problem is a known limitation.

Solution

Click any adjoining tab, then click the **Map of Permissions** tab and the map is displayed.

Chapter 9. Realm IDEAS not found in Identity Governance and Intelligence

When you connect to Service Center or Admin Console, might be shown the warning message *Realm IDEAS not found in Ideas system*.

The message appears when an accidental asynchrony occurs during startup sequence between the Identity Governance and Intelligence server and the DB2 database server.

IDEAS is the Administration Realm of Identity Governance and Intelligence.

In IDEAS, are stored all the information that is related to the Administrators that can manage the operative Realm, where you can model the properties of the organization to be governed.

For fixing this problem, you have to operate a sequence of stop and start operations that are related to the virtual appliance and DB2 database.

1. Log in to the virtual appliance.
2. In the Home Page, stop the server of Identity Governance and Intelligence.
3. Into the administrative context of DB2, with right DB2 privileges, stop the DB2 server.
4. Start the DB2 server.
5. In the Home Page of the virtual appliance, start the server of Identity Governance and Intelligence.

Chapter 10. Map issues in Role Compare

Perform a role compare by selecting **Access Governance Core** > **Monitor** > **Role Compare**. Select a role with many permissions that are assigned to many users and click **Compare**. If you move the verticle separator all the way to the right and then back to the center, the map information disappears.

Cause

This problem is a known limitation.

Solution

Click any adjoining tab, then click the **Map of Permissions** tab and the map is displayed.

Chapter 11. Restore account action fails on LDAP adapter because there is no auto-generation service or input field to enter a new account password

When you try to restore a Directory Server account on an LDAP target with an enterprise connector, the operation fails.

Cause

LDAP expects that a password be provided when an account is enabled or restored for a user. Enterprise Connectors does not have a self-generating password service nor does it provide an input field for entering a new password.

This problem is a known limitation.

Solution

See Pre-mapping and post-mapping rule examples. The sample rules address this specific scenario in the following way:

1. A pre-mapping rule uses the internal ID of the user for whom the account is restored on LDAP to retrieve the user's name and email address
2. A post-mapping rule generates a password upon the reactivation of the account
3. A post-mapping rule emails the password to the user whose data was retrieved in the pre-mapping rule

Copy these rules in your LDAP connector rules configuration to reset account passwords.

Chapter 12. Uncalled for entry in the virtual appliance event log

The event log of the virtual appliance intermittently records `admin@local logged in to the appliance` although user admin@local did not log in.

Cause

This event is triggered in the normal functioning of the virtual appliance as a result of internal calls and can be safely ignored.

Chapter 13. Limitations for the support of bidirectional languages

This document lists the known limitations of this version of Identity Governance and Intelligence for the support of bidirectional languages.

Limitations that affect charts, diagrams, and labels

The next table lists the locations in the Identity Governance and Intelligence user interface where you might find that charts, diagrams, and labels fail to be mirrored.

Table 2. Current limitations that affect charts, diagrams, and labels in bidirectional languages

Affected items	**Limitation description**	**Found in**
Charts, diagrams, labels	In Assignment Statistics, the diagram and its labels are not mirrored. In Entitlement Statistics, the bar chart and its labels are not mirrored.	Access Governance Core **Manage** > **Groups** > **Analysis** > **Statistics**
	The request chart, tool-tips, and its labels are not mirrored.	Process Designer **Monitor** > **Requests**
	The chart, labels and tool-tip of the chart (if any) are not mirrored in the following panes: • **Monitor** > **Access Distribution** • **Monitor** > **Coverage Factors** • **Monitor** > **Access Trend** • **Manage** > **Data Exploration** > **Details** (click on magnifier icon) **Entitlements Statistics** • **Manage** > **Data Exploration** > **Details** (click on magnifier icon) **Users Statistics** • **Manage** > **Role Mining** > **Details** (click on magnifier icon) **Statistics** > **Analysis Statistics** • **Manage** > **Role Mining** > **Details** (click on magnifier icon) **Statistics** > **Role Statistics** Maps are not mirrored in: • **Monitor** > **Access Summary** > **(click on magnifier icon)** • **Manage** > **Data Exploration** > **Details** (click on magnifier icon) **Map** • **Manage** > **Role Mining** > **Details** (click on magnifier icon) **Map** • **Manage** > **Role Mining** > **Details** (click on *i* icon) **Map**	Access Optimizer
	In **Monitor** > **Monitoring**, the coordinate maps of **Memory**, **CPU**, and **Storage** show incorrect mirroring.	virtual appliance
	The bar chart and its labels are not mirrored in **Tools** > **Configuration Set Comparison** > **Comparison Dashboard**. The diagram and labels are not mirrored in **Monitor** > **Role Warnings** > **Actions** > **Statistics**.	Access Risk Controls for SAP
	The bar chart and its labels are not mirrored in **Monitor** > **Configuration Set Comparison** > **Comparison Dashboard**.	Access Risk Controls
	In **Stats**, the diagram and its labels are not mirrored.	Access Certifier
	The chart of the User Access Change dashboard is mirrored incorrectly.	Service Center

Limitations that affect dates and calendars

The next table lists limitations that affect dates and calendars in bidirectional languages.

Table 3. Current limitations that affect dates and calendars in bidirectional languages

Affected items	Limitation description	Found in
Dates and calendars	Calendar widgets are displayed in Arabic-European digits when they should be in Arabic-Indic.	Administration Console and Service Center
	In Arabic locale, calendar widgets are not shown correctly. The working week starts on Saturday but it is shown starting from Sunday.	Administration Console and Service Center
	The calendar icon is mirrored incorrectly.	Access Governance Core, Enterprise Connectors, Task Planner, Reports in the Service Center, Access Requests

Limitations that affect tabs

The next table lists limitations that affect tabs in bidirectional languages.

Table 4. Current limitations that affect tabs in bidirectional languages

Affected items	Limitation description	Found in
Tabs	For Arabic and Hebrew, after you click the <> icon several times to scroll the tabs on the right, you must click your selected tab several times to display the contents.	Access Requests

Limitations that affect pop-up windows

The next table lists limitations that affect pop-up windows in bidirectional languages.

Table 5. Current limitations that affect pop-up windows in bidirectional languages

Affected items	Limitation description	Found in
Pop-up windows	The resize box of pop-up windows is not mirrored.	All the user interfaces

Limitations that affect reports

The next table lists limitations that affect reports in bidirectional languages.

Table 6. Current limitations that affect reports in bidirectional languages

Affected items	Limitation description	Found in
Reports	Reports lack the following attributes: • Mirroring • Proper display of text with natural text direction • Support for non Gregorian calendars • Numeric shaping	Reports in any format (PDF, DOCX, XLSX,, RTF, HTML) throughout the user interfaces.

Index

Printed in USA