IBM Security Identity Governance and Intelligence
Version 5.2.2.1

Troubleshooting and Support Topics

IBM Security Identity Governance and Intelligence
Version 5.2.2.1

Troubleshooting and Support Topics

IBM

Table of contents

Table list v

Chapter 1. Diagnostic tools 1

Chapter 2. Troubleshooting virtual appliance problems. 3

When a Postgres database is reset on the primary node in a cluster, the slave database retains the data . 3

The Identity Governance and Intelligence application is inaccessible after a Postgres database failover . . 3

DB2 reconfiguration validation fails after ACR takeover on standby 4

When you change the virtual appliance password, the Postgres database password does not change . . 4

Node activation fails. 4

Cannot reconnect a secondary node 5

Default gateway is lost when M.2 is enabled. . . . 5

If an external database is configured after a Postgres failover in a cluster environment, the failover condition remains if the Postgres database is reconfigured. 5

Clear the service integration bus. 6

Reset password for Identity Brokerage Adapters . . 7

Cluster problems occur after the application of a snapshot to the primary node. 7

Application login fails 8

If DB2 ACR is set, the user cannot log in after a DB2 failover and failback 8

Test connection fails after you promote a secondary node to primary node in cluster with PostgreSQL . 8

Chapter 3. Target Administration does not open from the Identity Governance and Intelligence administration console 11

Chapter 4. Target Administration is not available from the module menu. . . . 13

Chapter 5. Target application is deleted 15

Chapter 6. Troubleshooting Identity Brokerage Adapters 17

Chapter 7. Some table columns are unable to sort in the Service Center . . 19

Chapter 8. Cannot add account defaults for an attribute that is a multi-value widget on the adapter account form 21

Chapter 9. Modifying or removing the rights value for a string attribute causes errors 23

Chapter 10. Pagination footer cannot be fully displayed 25

Chapter 11. Role data does not show up in Identity Governance and Intelligence after the reconciliation of an LDAP, AIX, Linux, HPUX, or Solaris target 27

Chapter 12. Map issues in Role Compare 29

Index 31

Table list

1. Log files that are related to Identity Brokerage 17

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.

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.

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 create. 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.

If DB2 ACR is set, the user cannot log in after a DB2 failover and failback

DB2 automatic client reroute (ACR) is enabled and DB2 fails. The user performs a DB2 failover and failback. The user might not be able to access the Identity Governance and Intelligence login screen.

Cause

This problem is a known limitation.

Solution

Search for the following exception in the log files.

```
java.sql.SQLException: [jcc][t4][2043][11550][3.69.24]
Exception java.net.ConnectException:
Error opening socket to server /<dbServer> on port <port> with message:
Connection refused. ERRORCODE=-4499, SQLSTATE=08001 DSRA0010E:
SQL State = 08001, Error Code = -4,499
```

If that exception is found, restart the Identity Governance and Intelligence server.

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.

Chapter 3. Target Administration does not open from the Identity Governance and Intelligence administration console

The Target Administration user interface does not open up from the Identity Governance and Intelligence Administration Console. If you are not able to view the Target Administration user interface, your web browser might be configured to block all pop-up windows.

By default, Google Chrome or Mozilla Firefox blocks pop-up windows from automatically showing up on the web browser. When a pop-up window is blocked, the address bar on the web browser indicates that it is blocked.

To make sure that the Target Administration user interface opens from the Identity Governance and Intelligence Administration Console properly, change your web browser settings to display pop-up windows. Consult the browser documentation to configure your web browser to display pop-up windows for your requirements.

Chapter 4. Target Administration is not available from the module menu

If you are working in another module in the Administration Console and want to access the Target Administration Console, it is not accessible from the module menu. The module menu lists all the modules except Target Administration.

Cause

This problem is a known limitation.

Solution

To access the Target Administration Console from another module, click **Home** in the module menu. Then, you can select **Target Administration** from the Home page.

Chapter 5. Target application is deleted

When a target application is deleted from the Target Administration Console, the `OBJECT_NOT_FOUND -Target-` message is displayed in the **Events** > **OUT Events** screen.

Cause: When an application is deleted, the target is just disconnected from Identity Governance and Intelligence. All the permissions assigned to the application are removed from the Identity Governance and IntelligenceAdministration Console but not from the target cache.

Workaround: If you accidentally deleted the application from the target, just delete the existing target and create a new target. See Creating targets

Chapter 6. Troubleshooting Identity Brokerage Adapters

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

Verify the target status

If target reconciliation failed, check the target status. The IBM Security Identity Governance and Intelligence server tracks its ability to make remote connections and send provisioning requests to adapters on a per target basis. This ability is reflected in the Status for each target on the Manage Targets panel. On this panel, you can also search for targets with a specific 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 Target status.

Review the log file

Identity Brokerage requests tracing for all adapters.

Tracing an adapter request requires viewing the 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 system error • Identity Brokerage Application server system out • IBM Security Identity Governance and Intelligence trace log	You can view the Identity Brokerage log files from the Virtual Appliance Dashboard. See Retrieving logs.
Identity Brokerage Adapter related logs	• IBM Security Identity Governance and Intelligence trace log • Security Directory Integrator server logs • Adapter specific log	After the adapter installation is complete, the adapter creates an `<adapter_name>.log` file and usually stores it in the `logs` directory. For more information, see the adapter's *Installation and Configuration Guide.* **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 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 message that is 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, using the **Log Retrieval and Configuration** option. See Configuring logs.

Limitations

Certain behaviors and limitations are known to exist 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 7. 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 8. Cannot add account defaults for an attribute that is a multi-value widget on the adapter account form

On the Select an Attribute page in the Target Administration module, you cannot add an account default for a multi-value attribute as expected when you click **Add**. The account form widget page is wrongly displayed when you try to do a standard **Add** account default mapping on multi-value attributes.

Symptoms

When you click **Add** to define the account default for the "Full name" attribute, you do not see the correct page where you expect to do the standard account default mapping. Instead, you can only successfully click **Add (Advanced)** and do the account default mapping from that page.

Causes

This problem is experienced with certain target types, such as the IBM Security Access Manager adapter profile, in which the "Full name" attribute is a required, multi-value attribute on the account form of the profile.

Diagnosing the problem

To see the problem, follow these steps:

1. From the Administration Console, select **Target Administration**.
2. From the navigation tree, click **Manage Targets**.
3. On the Select a Target page, locate your target by completing these steps:
   a. Type information about the target in the **Search information** field.
   b. Select a target type from the **Target type** list.
   c. Select a status from the **Status** list and click **Search**. A list of targets that matches the search criteria is displayed.
4. In the **Targets** table, click the icon (▸) next to the target, and select **Account Defaults**.
5. On the Select Default Attribute page, click **Add** to view the list of account attributes.
6. On the Select an Attribute page, select a multi-value account attribute, such as "Full name," and click **Add**. The Security Identity Manager account form widget is displayed, which is not expected or correct.

Resolving the problem

To resolve the problem, import the adapter profile to upgrade the profile information that is available for Identity Governance and Intelligence 5.2.2. For information about importing the adapter profile, see Importing target types (adapter profiles).

After you import the adapter profile, go to the existing target for that profile (target type), and then define the account defaults. The correct Manage Account Defaults page is displayed.

If you need more information about modifying the target or adding the account defaults, see these topics:

- Changing targets
- Account defaults on a target

Chapter 9. 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 10. 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 11. 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 12. 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.

Index

C

Cluster errors
  after snapshot application 7

L

login fails 8

R

reset password
  Identity LifeCycle Management 7

S

Service Center 19
Sorting function 19
Sorting function not working 19

T

Tables are unable to sort in the Service Center 19
trouble shooting
  application login fails 8
troubleshooting
  clusters 7

Printed in USA