IBM Security Identity Governance and Intelligence
Version 5.2.1

Troubleshooting and Support Topics

IBM Security Identity Governance and Intelligence
Version 5.2.1

Troubleshooting and Support Topics

Table of contents

Table list

Chapter 1. Troubleshooting virtual appliance problems

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

Software firewall configuration in the virtual appliance

Before you start the installation of IBM® Security Identity Governance and Intelligence virtual appliance, check the considerations for the port numbers, apart from host names, user accounts, and fix packs.

Having a software firewall on the virtual appliance helps to control only the necessary ports for IBM Security Identity Governance and Intelligence to work.

IBM Security Identity Governance and Intelligence hides all the unwanted ports and provides only those ports that are required by the virtual appliance.

Use the default ports for a standard installation on a clean computer. For advanced or custom deployments, you might have to use different port numbers. If you intend to use the default ports, ensure that the port is not yet assigned and are available before you use the product installation program.

- Check the availability of the ports that are required by the IBM Security Identity Governance and Intelligence virtual appliance.
- Open a port checking utility on the computer. Alternatively, check the firewall rules for the system.
- If the port is already assigned, choose another value when prompted by the installation program.

Table 1 describes a list of available ports that you can use to work with IBM Security Identity Governance and Intelligence virtual appliance:

Table 1. Port numbers

Port numbers	Used by
22	Secure Shell (SSH).
161	SNMP server, if configured.
1098	Security Directory Integrator web server port.
1099	RMI Dispatcher service.
2821	Application server bootstrap.
8892	Application server SOAP port.
9112	Application server ORB Listener.
9343	Secure application server.
9443	Secure appliance management interface.
9437	CSIV2 SSL mutual authentication listener address.
9438	CSIV2 SSL server authentication listener address.
9439	SAS SSL server authentication listener address.

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 `SIMOWNER0` 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.

Chapter 2. 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 3. 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 4. 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 2.

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 List of Identity Brokerage Adapters.
- *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 5. 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.

Index

Printed in USA