IBM Security Identity Governance and Intelligence
Version 5.2.1

Installation Topics

IBM

IBM Security Identity Governance and Intelligence
Version 5.2.1

Installation Topics

Table of contents

Table list

Chapter 1. Overview

The IBM® Security Identity Governance and Intelligence virtual appliance is an appliance-based solution that delivers the IBM Security Identity Governance and Intelligence application.

Hardware and software requirements

Check the hardware and software requirements before you install the IBM Security Identity Governance and Intelligence virtual appliance.

For the detailed system requirements, see the IBM Security Identity Governance and Intelligence Software Product Compatibility Report.

1. Enter `Security Identity Governance and Intelligence`.
2. Select the product version.
3. Select the deployment unit.
4. Click **Submit**.

Deployment overview

The following table describes the main installation stages or tasks.

Table 1. Virtual appliance administrators deployment tasks

Tasks	**Subtasks and references**
Install and configure the database server.	For Oracle: • Installing the Oracle server • Configuring the Oracle server For DB2®: • Installing the DB2 server • Configuring the DB2 server
(Optional) Install and configure the directory server to use the Identity Brokerage Providers module.	Installing and configuring the directory server
Prepare the virtual machine.	Setting up the virtual machine
Install and set up the virtual appliance.	• Installing the IBM Security Identity Governance and Intelligence virtual appliance • Setting up the initial virtual appliance

Table 1. Virtual appliance administrators deployment tasks (continued)

Tasks	**Subtasks and references**
For high availability, set up a virtual appliance cluster.	Setting up a virtual appliance cluster • "Setting up a member node for IBM Security Identity Governance and Intelligence" on page 28 • "Changing a member node to a primary node" on page 29 • "Removing a node from the cluster" on page 30 • "Reconnecting a node into the cluster" on page 30 • "Synchronizing a member node with a primary node" on page 31
Configure the virtual appliance settings.	• Enabling Identity Brokerage Providers • Managing directory server configuration • Managing the database server configuration • Managing OpenID connect configuration • Managing the mail server configuration • Managing application interfaces

Chapter 2. Prerequisite software

Install and configure the prerequisite software before you install the IBM Security Identity Governance and Intelligence virtual appliance.

Changing the default password for the database schemas

You can change the default password that grants access to the schemas of the IBM Security Identity Governance and Intelligence database.

About this task

In the Identity Governance and Intelligence database, the password that is required to access the database schemas is defined by the scripts that install the schemas. See "Configuring the Oracle server" on page 4 and "Configuring the DB2 server" on page 7. The default password is `ideas`.

Attention: Complete the procedure before you start the schema installation steps.

Procedure

On both Oracle and DB2

1. Unpack the following compressed file from the product package image or DVD. Extract the subdirectory that corresponds to your database into a directory of your choice in your database serve, such as the *SCRIPT* directory.

   SEC_IDNTY_GVN_INTL_*xxx*_V5.2.1_DT_IN_.zip

   Where *xxx* can be CMP, ANL, LFC, or IEE, depending on which product media type that includes the `IBM Security Identity Governance and Intelligence V5.2.1 Database Installation Scripts` file you are using.
2. Open the following file with an editor:

   UNIX *SCRIPT*/DB_INSTALLATION/IGI_5_2_1_INSTALLATION/00-COMMON/01-COMMON.sql

   Windows
   SCRIPT\DB_INSTALLATION\IGI_5_2_1_INSTALLATION\00-COMMON\01-COMMON.sql
3. In the file, find the following section:
   - On Oracle

     ```
     ------------------------------------------------------------
     -- DEFAULT PASS VALUES                                     --
     ------------------------------------------------------------
     DEFINE IDEAS_SCHEMA_DEF_PASS = '"ideas"'
     ```
   - On DB2

     ```
     ------------------------------------------------------------
     -- DEFAULT PASS VALUES                                     --
     ------------------------------------------------------------
     DEFINE IDEAS_SCHEMA_DEF_PASS = '''ideas'''
     ```
4. Replace `ideas` with the new password, keeping the original database-dependent semantics.
   - `'"`*`new_password`*`"'` (new password enclosed within double quotation marks enclosed within single quotation marks) on Oracle

- `'''`*`new_password`*`'''` (new password enclosed within sets of three single quotation marks) on DB2

5. On DB2 only, continue as follows:
   a. Open the following file with an editor:

      UNIX `SCRIPT/__FOR_DBAs__/unix_create_users.sh`

      Windows
      `SCRIPT\__FOR_DBAs__\win_create_users.bat`

   b. Replace all of the `ideas` password strings with the value used in step 4. Omit the quotation marks.

Installing the Oracle server

The IBM Security Identity Governance and Intelligence virtual appliance requires an external Oracle database. If you do not have an existing Oracle database host, install it by following the directions in the Oracle product documentation.

Configuring the Oracle server

You must configure an installed Oracle server to work with IBM Security Identity Governance and Intelligence virtual appliance.

Before you begin

- Install the Oracle server.
- Know the common database parameters, such as the IP address, server port, and SID. See Table 2.
- If you want to change the default password, `ideas`, that is required to access the Identity Governance and Intelligence schemas, do so before you create the database. See "Changing the default password for the database schemas" on page 3.
- Understand and comply with the hardware and software requirements. See Chapter 1, "Overview," on page 1.

About this task

Important: IBM Security Identity Governance and Intelligence, Version 5.2.1, does not support the pluggable database option in Oracle. When you install the Oracle database for IBM Security Identity Governance and Intelligence, clear the pluggable database option in Oracle, otherwise applying the database schema is not successful.

Use the following tags to customize the Oracle database.

Table 2. Tags to customize the IBM Security Identity Governance and Intelligence Oracle database installation

Tags	Description
IdeasSID	Oracle database instance name (SID)
DBServer	Oracle Server IP address or DNS name
DBPort	Oracle listener port

To install the IBM Security Identity Governance and Intelligence database on Oracle, complete the following procedure.

Note: You must be a root user to change the `.ora` file.

Procedure

1. Configure the `tnsnames.ora` file.
   a. Log in with root privileges.
      ```
      sudo su -
      ```
   b. Switch to the `oracle` user.
      ```
      sudo su oracle
      ```
   c. Set the *env* variables:
      ```
      . /usr/bin/oraenv
      ```
   d. Start listener.
      ```
      lsnrctl start
      ```
   e. Start the database.
   f. Browse to the `tnsnames.ora` file. For example, *oracle_home*`/db/network/admin`
   g. Open the file in a text editor. For example, **vi**
   h. If the network instance is not configured correctly, add the following section:
      ```
      <IdeasSID> =
        (DESCRIPTION =
          (ADDRESS_LIST =
            (ADDRESS = (PROTOCOL = TCP)(HOST = <DBserver>)(PORT = <DBport>))
          )
          (CONNECT_DATA =
            (SERVICE_NAME = <IdeasSID>)
          )
        )
      ```
   i. Verify that the configuration is working by connecting to the database with the following command:
      ```
      sqlplus system/<password>@<IdeasSID>
      ```
2. Unpack the following compressed file from the product package image or DVD:
   ```
   SEC_IDNTY_GVN_INTL_xxx_V5.2_DT_IN_.zip
   ```

   Where *xxx* can be CMP, ANL, LFC, or IEE, depending on which product media type that includes the `IBM Security Identity Governance and Intelligence V5.2 Database Installation Scripts` file you are using.
3. Extract the `oracle_installation.zip` file into a directory of your choice in your database server. For example, *SCRIPT*.
4. Choose and run the appropriate database creation script.

   The following database scripts address different customer requirements and access restrictions to Oracle system accounts. The scripts in the following table are in the folder `DB_INSTALLATION`.

   Note: Windows systems might require a blank space before the data file path, when you run the `sql` file. Verify that the database path value is correct before you press Enter to start the installation.

Table 3. Database scripts for different environments and access restrictions.

File name	Description
`01-FULL-TBLS_USER_AND_OBJ-CREATION.sql`	Interactive full DB creation.

Table 3. Database scripts for different environments and access restrictions. (continued)

File name	Description
`02-FULL-TBLS_AND_USER-CREATION.sql`	DBA service script. Table space and database user creation only.
`02-FULL-TBLS_AND_USER-SIMULATION.sql`	DBA service script. It generates as the output of the Oracle version-specific database installation script.
`03-FULL-OBJ-CREATION.sql`	DBA service script. Object creation only.

Only the first script is necessary for a common database configuration scenario with the following attributes:

- Installation in a single realm
- Installation by using Oracle system accounts for the entire installation

In this script, you can modify the debug level for getting a more verbose indication in the shell command window and also in the related log file.

You can obtain this result:

a. Open the script and find the section:

```
--DEBUG ONLY
--SET ECHO ON
```

b. Change the string:

```
--SET ECHO ONTo
SET ECHO ON
```

The same operation can be applied to all scripts of the Table 1.

The `IGI_5_2_1_INSTALLATION` folder in the `DB_INSTALLATION` folder contains files that are used by the database scripts.

5. To prepare the database, run the installation script for the IDEAS User Realm:

`sqlplus system/<password>@<IdeasSID> @01-FULL-TBLS_USER_AND_OBJ-CREATION.sql`

The script runs with the following result:

```
================================
= IGI SUITE V5.2.1 INSTALLATION =
================================

To continue with the installation you must input some values.
Some questions have a default answer, but you can otherwise input different values.

Enter datafile Path. Ex. /opt/oracle/oradata/<INSTANCE_NAME>
/ ATTENTION! ERROR ON INPUT MAY RESULT WITH WRONG INSTALLATION.
BE SURE THAT THE INPUT PATH EXISTS AND THAT IT IS AN ABSOLUTE PATH!
Enter datafile Path. NO DEFAULT! ->
Value:

================================================================================
VARIABLE SUBSTITUTION RESULTS:
IGA Core RELATED ACCESS ANALYTICS SCHEMA:
-  DEFAULT VALUE : AA_CORE/ideas
-  NEW VALUE     : AA_CORE/ideas
IGA Core SCHEMA:
-  DEFAULT VALUE : IGA_CORE/ideas
-  NEW VALUE     : IGA_CORE/ideas
IGA Core RELATED CCS SCHEMA:
-  DEFAULT VALUE : CCS_CORE/ideas
-  NEW VALUE     : CCS_CORE/ideas
IGA Core RELATED REPORT SCHEMA:
-  DEFAULT VALUE : IGA_REPORT_CORE/ideas
-  NEW VALUE     : IGA_REPORT_CORE/ideas
================================================================================
Please choose tablespace installation size (Small/Medium/Large). (default=M) [S/M/L]
```

Installing the DB2 server

The IBM Security Identity Governance and Intelligence virtual appliance requires an external DB2 database.

If you do not have an existing DB2 database host, install it by following the directions in the product documentation. See http://www-01.ibm.com/support/knowledgecenter/SSEPGG/welcome.

Configuring the DB2 server

Set up the DB2 database to install the IBM Security Identity Governance and Intelligence database on the DB2 server.

Before you begin

- You must have the DB2 server installed.
- Know the common database parameters such as the IP address or server port. See Table 1.
- This procedure works only on DB2 Enterprise Server Edition (DB2 ESE), Version 10.5.0.3 or later.
- If you want to change the default password - `ideas` - required to access the Identity Governance and Intelligence schemas, you must do so before you create the database. See "Changing the default password for the database schemas" on page 3.
- Understand and comply with the Hardware and software requirements.

About this task

Use the following tags to customize the DB2 database.

Table 4. Tags to customize IBM Security Identity Governance and Intelligence DB2 installation.

Tags	**Description**
DBServer	DB2 Server IP address or DNS name
DBPort	DB2 instance port **Important:** Make sure you know what the actual port number is. You can verify it at `/etc/services`.
IGI_DB	DB2 database name
INSTANCE_OWNER	DB2 instance owner of the database instance
PASSWORD	DB2 instance owner password
FQ_IGI_DB	*<DBServer>*:*<DBPort>*/*<IGI_DB>*
TABLESPACE_SIZE	Identity Governance and Intelligence table space size (small, medium, or large)
TABLESPACE_PATH	The location of the database

Procedure

1. Log in as the instance owner.

   On Windows, the instance owner must be a member of the DB2ADMNS and Administrator groups.

   If you need to create an instance for IBM Security Identity Governance and Intelligence virtual appliance on UNIX, take the following steps:

a. Create an operating system user. For example, add the user as `igiinst` and assign the password as `ideas` as in the following commands.

   Note: You must add the user to the `root` group when you create the operating system user.

   ```
   useradd -g root igiinst
   passwd igiinst
   - use "ideas" for new password
   ```

b. Create an `igiinst` folder under the `/home` directory and make user `igiinst` as the owner. Run the following commands:

   ```
   cd /home
   mkdir igiinst
   chown igiinst igiinst
   ```

c. Run the following command to create a database instance.

   ```
   DB2_Install_Location/instance/db2icrt -u igiinst igiinst
   ```

   For example, `/opt/IBM/db2/V10.5/instance/db2icrt -u igiinst igiinst`.

d. Run the following commands to set up the instance.

   ```
   su - igiinst
   . ~igiinst/sqllib/db2profile
   db2 update dbm cfg using SVCENAME <DBPort_value>
   db2set DB2COMM=tcpip
   db2set -all DB2COMM
   db2start
   ```

   The instance for IBM Security Identity Governance and Intelligence virtual appliance is now created.

2. From the instance, create the database by using the following statements.

   ```
   db2set DB2_COMPATIBILITY_VECTOR=ORA
   db2set DB2_RESTRICT_DDF=TRUE
   db2stop force
   db2start
   db2 create database IGI_DB
   db2 connect to IGI_DB
   db2 update db cfg using LOGFILSIZ 5000 LOGPRIMARY 50 LOGSECOND 50
   db2 create bufferpool IDEAS_BP IMMEDIATE PAGESIZE 32K
   db2 create system temporary tablespace IDEAS_SYS_TEMP pagesize 32k bufferpool IDEAS_BP
   db2 create user temporary tablespace IDEAS_TEMP pagesize 32k bufferpool IDEAS_BP
   db2stop force
   db2start
   ```

3. Complete one of the following sets of instructions based on your operating system.

   - On UNIX systems

     a. Log in with root privileges.

     b. Unpack the following compressed file from the product package image or DVD and extract the subdirectory for DB2 into a directory of your choice in your database server, for example, *SCRIPT*:

        ```
        SEC_IDNTY_GVN_INTL_xxx_V5.2.1_DT_IN_.zip
        ```

        Where *xxx* can be CMP, ANL, LFC, or IEE, depending on which product media type that includes the `IBM Security Identity Governance and Intelligence V5.2.1 Database Installation Scripts` file you are using.

        Change the path to this directory (`SCRIPT` in the example).

     c. Run the **`chmod -R 777 *`** command.

     d. Change the directory to `<SCRIPT>/__FOR_DBAs__`.

     e. Run the **`dos2unix unix_create_users.sh`** script.

     f. Run the **`unix_create_users.sh`** script.

- On Windows systems
  a. Log in as Administrator.
  b. Unpack the following compressed file from the product package image or DVD and extract the subdirectory for DB2 into a directory of your choice in your database server, for example, *SCRIPT*:

     SEC_IDNTY_GVN_INTL_*xxx*_V5.2.1_DT_IN_.zip

     Where *xxx* can be CMP, ANL, LFC, or IEE, depending on which product media type that includes the `IBM Security Identity Governance and Intelligence V5.2.1 Database Installation Scripts` file you are using.

     Change the path to this directory (`SCRIPT` in the example).
  c. Change the directory to `<SCRIPT>\__FOR_DBAs__` and run the **`win_create_users.bat`** command.

     Verify that no restrictive password creation policies that inhibit user creation exist.

4. Apply the schema to the DB2 database. If you are applying the schema from a remote DB2 installation, complete these steps.

   Note: You must log in as the instance owner to run the `sql` script files.
   a. Install the DB2 Client library for DB2 server Version 10.5.0.5 or later.
   b. Unpack the following compressed file from the product package image or DVD and extract the subdirectory for DB2 into a directory of your choice in your database server. For example, *SCRIPT*.

      SEC_IDNTY_GVN_INTL_*xxx*_V5.2.1_DT_IN_.zip

      Where *xxx* can be CMP, ANL, LFC, or IEE, depending on which product media type that includes the `IBM Security Identity Governance and Intelligence V5.2.1 Database Installation Scripts` file you are using.
   c. Change the path to `<SCRIPT>/DB_INSTALLATION` (UNIX) or `<SCRIPT>\DB_INSTALLATION` (Windows).
   d. Modify the `login.sql` file by setting the appropriate connection string. See the following string:

```
DEFINE IGI_DB = xxx.xxx.xxx.xxx:yyyyy/zzz

--xxx.xxx.xxx.xxx – DB2 Server IP address or DNS name
--yyyyy           - DB2 Server DATABASE port
--zzz             - DB2 Server DATABASE name
DEFINE ISIG_DB = xxx.xxx.xxx.xxx:yyyyy/zzz
DEFINE TABLESPACE_PATH = 'NO_DEFAULT'
DEFINE TABLESPACE_SIZE = 'NO_DEFAULT'
```

   e. Choose and run the appropriate database creation script. The following database scripts address different customer requirements and access restrictions to DB2 system accounts. The scripts that are specified in the following table are stored in the `DB_INSTALLATION` directory.

      Note: Windows systems might require a blank space before the data file path, when you run the `sql` file. Verify that the database path value is correct before you press Enter to start the installation.

Table 5. Database scripts for different environments and access restrictions.

File name	Description
`01-FULL-TBLS_USER_AND_OBJ-CREATION.sql`	Interactive full database creation.

Table 5. Database scripts for different environments and access restrictions (continued).

File name	Description
02-FULL-TBLS_AND_USER-CREATION.sql	DBA service script. Table space and database user creation only.
02-FULL-TBLS_AND_USER-SIMULATION.sql	DBA service script. Generate as output the DB2 version-specific database installation script.
03-FULL-OBJ-CREATION.sql	DBA service script. Object creation only.

Only the first script (`01-FULL-TBLS_USER_AND_OBJ-CREATION.sql`) is necessary for a common database configuration scenario with the following attributes:

- Installation in a single realm.
- Installation by using DB2 system accounts for the entire installation. Subsequent points are referred to this case.

In this script, you can modify the debug level for getting a more verbose indication in the shell command window and also in the related log file.

You can obtain this result:

1) Open the script and find the section:

```
--DEBUG ONLY
--SET ECHO ON
```

2) Change the string:

`--SET ECHO ON` To

```
SET ECHO ON
```

The same operation can be applied to all scripts of the Table 2.

f. Run the following command to prepare the database.

Note: You must run the command as the instance owner.

- On UNIX systems, as the root user

```
. ~igiinst/sqllib/db2profile
clpplus -nw <INSTANCE_OWNER>/<INSTANCE_OWNER_PASSWORD>@<FQ_IGI_DB> @01-FULL-TBLS_USER_AND_OBJ-CREATION.sql
```

- On Windows systems

```
clpplus -nw <INSTANCE_OWNER>/<INSTANCE_OWNER_PASSWORD>@<FQ_IGI_DB> @01-FULL-TBLS_USER_AND_OBJ-CREATION.sql
```

Where *<FQ_IGI_DB>* is `<DBServer>:<DBPort>/<IGI_DB>`

For example, your command might be like the following one in UNIX:

```
clpplus -nw igiinst/ideas@<db2hostname>:50000/igidb @01-FULL-TBLS_USER_AND_OBJ-CREATION.sql
```

When the script is complete, at the SQL prompt run the **Exit** command.

If an error occurs during the run of this script, see the log file:

UNIX systems

```
<SCRIPT>/DB_INSTALLATION/IGI_V5_2_1_Installation.log
```

Windows systems

```
<SCRIPT>\DB_INSTALLATION\IGI_V5_2_1_Installation.log
```

g. Depending on your operating system, specify one of the following commands when prompted for a path.

```
<INSTANCE_OWNER_HOME>/<INSTANCE_OWNER>/<NODE_DB>/<IGI_DB>
```

or

```
<INSTANCE_OWNER_HOME>\<INSTANCE_OWNER>\<NODE_DB>\<IGI_DB>
```

For example, /home/db2inst1/db2inst1/NODE0000/IGI_DB

h. Select one of these options when prompted for a table size.
   - Large
   - Medium
   - Small

   For example, select M.

Installation of database schemas in a high availability environment

Create the Identity Governance and Intelligence database schemas for Oracle and DB2 for every new virtual appliance node in a cluster.

The SEC_IDNTY_GVN_INTL_*xxx*_V5.2.1_DT_IN_.zip file has subdirectories for the Oracle and DB2 installations. They include a number of scripts that create an Identity Governance and Intelligence database schema. The schemas are created in different modalities for a new virtual appliance node before the node is added to the cluster.

The DB Administrator, or a non-DB Administrator (depending on the script) can then run any of the scripts that are listed. The scripts create a SIB schema for every node in the cluster.

The database installation compressed file includes several scripts. They cover different installation scenarios. The following table lists the scripts, their purpose, and whether they must be run by a DBA.

Table 6. Schema installation scripts for virtual appliance nodes in an Identity Governance and Intelligence cluster.

Script name	Objective	DBA required
07-ADD_NODE-USER_AND_OBJ-CREATION.sql	Adds a schema and creates all the associated objects. When first run on a fresh installation, it creates schema ITIML001. Schema ITIML000 is created when you first install the database. If you run it repeatedly, it creates another schema at every iteration with the ITIML002, ITIML003, ITIML*n* nomenclature up to ITIML999.	Yes
08-ADD_NODE-USER-CREATION.sql	Adds a schema without the objects that belong to it.	Yes
08-ADD_NODE-USER-SIMULATION.sql	Generates the new schema creation script ton screen and in logs. It can generate the DML script that can be handed to the DBA to create the next virtual appliance node schema.	No
09-ADD_NODE-OBJ-CREATION.sql	Creates the objects that belong to the most recent virtual appliance node schema created by a DBA. The script automatically selects the last of the installed schemas and tries to install the objects in it.	No

Run the script that best matches your scenario. The scripts can create schemas for up 1000 nodes.

At completion time, each script displays the following message on screen and logs to inform the DBA that the schema was created:

```
=========================
= SIB NODE INSTALLATION =
=========================
SIB NODE Created:
ITIML00n
Use this schema name to configure the VA
```

Where 00*n* is the progressive number of the schema, starting from 001.

Unlike DB2, the Oracle authentication method is independent of the operating system and requires an operating system user to be defined before a schema is created. For this reason, the installation and migration scripts of the schemas on DB2 also create users from `ITIML000` to `ITIML010`. If you need to go beyond the number of nodes in your cluster, define the additional users before you install the schemas.

Installing and configuring the directory server

If you want to use the Identity Brokerage Providers, install and configure the directory server before you install the virtual appliance.

Before you begin

Install the database server.

Procedure

1. Install the directory server. See http://www.ibm.com/support/knowledgecenter/SSVJJU/welcome?lang=en and search for *Installing and Configuring*.
2. Configure the directory server for IBM Security Identity Governance and Intelligence virtual appliance by creating and configuring the directory server instance.
   a. Create a user with the following commands:

   For Windows

   ```
   LDAP_Install_Location\sbin\idsadduser -u ldapinst -w ldapinstpwd -g idsldap
   ```

   Where
   - `ldapinst` is the user name.
   - `ldapinstpwd` is the password.

   For UNIX and Linux

   ```
   LDAP_Install_Location/sbin/idsadduser -u ldapinst -w ldapinstpwd -g idsldap
   ```

   Where
   - `ldapinst` is the LDAP instance name.
   - `ldapinstpwd` is the password.
   - `idsldap` is the default LDAP group.

   b. Create a directory server instance with the following command:

   ```
   LDAP_Install_Location/sbin/idsicrt -I ldapinst -e encryptionseed -l /home/ldapinst
   ```

   Where
   - `ldapinst` is the LDAP instance name.

- encryptionseed is the encryption seed.
- /home/ldapinst is the instance home.

c. Create a database for the newly created LDAP instance with the following command:

```
LDAP_Install_Location/sbin/idscfgdb -I ldapinst -a ldapdb -w ldapdb -t ldapinst -l /home/ldapinst/
```

Where

- ldapinst is the LDAP instance name.
- ldapdb is the database administrator.
- ldapdb is the database administrator password.
- ldapinst is the database name.
- /home/ldapinst is the instance home.

d. Set the password for directory server instance Principal DN with the following command:

```
LDAP_Install_Location/sbin/idsdnpw -I ldapinst -u cn=root -p root
```

Where

- ldapinst is the LDAP instance name.
- cn=root is the Principal DN.
- root is the Principal DN password.

e. Add the suffix (dc=com) in the directory server instance with the following commands:

```
LDAP_Install_Location/sbin/idscfgsuf -I ldapinst -s dc=com
```

Where

- ldapinst is the LDAP instance name.
- dc=com is the suffix.

f. Start the directory server instance with the following commands:

For Windows

```
LDAP_Install_Location/sbin/ibmslapd -I ldapinst -n
```

Where

- ldapinst is the LDAP instance name.

For UNIX and Linux

```
LDAP_Install_Location/sbin/ibmslapd -I ldapinst -n -t
```

Where

- ldapinst is the LDAP instance name.

g. Prepare a ldif file. For example, dccom.ldif with the following content.

```
dn:dc=com
objectclass:domain
```

Run the command:

```
LDAP_Install_Location/bin/idsldapadd -h ldap_server_host
 -p ldap_server_port -D bind_root_dn -w bind_root_password
 -f dccom.ldif
```

For example,

```
/opt/IBM/ldap/V6.4/bin/idsldapadd -D cn=root -w password -p port
 -f dccom.ldif
```

Chapter 3. Installation

Complete the installation tasks to prepare the IBM Security Identity Governance and Intelligence environment.

Installation of the IBM Security Identity Governance and Intelligence virtual appliance

Use the following tasks to install and set up the IBM Security Identity Governance and Intelligence virtual appliance.

VMware support

The IBM Security Identity Governance and Intelligence virtual appliance can be installed on a VMware, Versions ESXi 5.0, 5.1, 5.5, and 6.0.

The Identity Governance and Intelligence virtual appliance for VMware is distributed as a pre-installed disk image of the virtual appliance in `.iso` format.

To deploy the `.iso` virtual appliance image to VMware, use the VMWare vSphere console.

Setting up the virtual machine

Create a virtual machine to host the IBM Security Identity Governance and Intelligence.

Procedure

1. Download the `igi_*.iso` build.
2. Create a virtual machine on ESXi 5.x or ESXi 6.0.
   a. From the VMware vSphere Client, click **File** > **New** > **Virtual Machine**.
   b. In **Configuration**, select **Custom**.
   c. Provide a name for the virtual machine. The virtual machine name can contain up to 80 characters, and the name must be unique within each vCenter Server VM folder.
   d. Choose the destination storage for this virtual machine.
   e. Set the virtual machine version to 8.
   f. Set the guest operating system to **Linux**. Under **Version**, select **Other 2.6.x Linux (64-bit)**.
   g. Enter the number of virtual sockets and cores per virtual sockets for the virtual machine, depending on your requirements. For example, enter the value as `2` for the following options to sum up the total number of cores to `4`.
      - **Number of virtual sockets**
      - **Number of cores per virtual socket**
   h. Enter the memory size. The minimum memory size is 16 GB.
   i. Set the number of network connections, depending on your requirements.

      Important: You must create at least three network interfaces to set up the virtual machine.

   j. Select **VMXNET 3** from a list of network adapters for better results. You can also use the **E1000** adapter to set up the virtual machine.
   k. Set the SCSI controller type to **LSI Logic Parallel**.
   l. Select the **Create a new virtual disk** option.
   m. Enter the disk size for virtual machine. The minimum disk size is 100 GB.
   n. Accept the default settings in the Advanced Options page.
3. Verify the settings for the virtual machine.
4. Select **Edit the virtual machine settings before completion** to proceed.
5. Click **Add** in the **Hardware** tab of the Virtual Machine Properties window.
6. Choose **CD/DVD drive**.
7. Select the type of media that you want the virtual drive to access. For example, select **Use ISO image**.
8. Browse to the data store location where you uploaded the `.iso` file.
9. Click **Finish** on the Add Hardware window.
10. Select **Connect at power on** on the Virtual Machine Properties window.
11. Click **Finish** on the Virtual Machine Properties window.
12. Optional: To mount or change the IBM Security Identity Governance and Intelligence media for an existing virtual machine, complete these steps.
   a. List the options. Right-click on the virtual machine that you created and select **Edit Settings**.
   b. Click **Add** in the **Hardware** tab of the Virtual Machine Properties window.
   c. Choose **CD/DVD drive 1**.
   d. Browse to the data store location where you uploaded the `.iso` file.
   e. Select the type of media that you want the virtual drive to access. For example, select **Use ISO image**.
   f. Select the **Connect at power on** check box on the Virtual Machine Properties window.
   g. Click **Power on the virtual machine**.

What to do next

Proceed with the IBM Security Identity Governance and Intelligence installation. See "Installing the IBM Security Identity Governance and Intelligence virtual appliance."

Installing the IBM Security Identity Governance and Intelligence virtual appliance

Install the IBM Security Identity Governance and Intelligence virtual appliance after you set up the virtual machine.

Procedure

1. When you start the virtual machine for the first time, press Enter to begin with the virtual appliance installation process.
2. Select the language that you want to use during the installation.
3. Type `yes` to continue.
4. When the installation process is complete, unmount the installation media.
   a. Right-click on the virtual machine and select **Edit Settings**.
   b. On the **Hardware** tab of the Virtual Machine Properties window, select **CD/DVD drive 1**.

   c. Clear these check boxes.
      - **Connected**
      - **Connect at power on**
5. Click **OK** to close the Virtual Machine Properties window.
6. Select **Yes** and click **OK** to confirm the installation media disconnection.
7. Press Enter and then press any key to continue.

What to do next

Go to "Setting up the initial virtual appliance."

Setting up the initial virtual appliance

The appliance setup wizard runs the first time that you connect to the virtual console of an unconfigured virtual appliance.

Before you begin

Complete the virtual appliance installation. See "Installing the IBM Security Identity Governance and Intelligence virtual appliance" on page 16.

Important: During the installation, maintain the same date and time between the system where you installed the virtual appliance and the system where you installed the database. A change in date or time between them can create problems when you run different processes that are managed through the Task Planner module.

About this task

Use the appliance setup wizard to manage host, port, or other configuration details, and then apply the changes to work with the virtual appliance.

Procedure

1. Provide the following user credentials when the system restarts.
   - **Unconfigured.appliance login**: `admin`
   - **Password**: `admin`
2. On the setup wizard screen, press Enter.
3. If necessary select a language, then read and accept the terms.

```
Software License Agreement
Currently selected language: English
1: Select language for license display
2: Read IBM terms
3: Read non-IBM terms
4: Proceeed to acceptance

Select option: 4


By choosing 'I agree,' you agree that (1) you have had the opportunity to
review the terms of both the IBM and non-IBM licenses presented above and (2)
such terms govern this transaction. If you do not agree, choose 'I do not
agree'.
1: I agree
2: I do not agree

Select option: 1
```

4. Change the virtual appliance password and go to the next screen.

```
Appliance Password
Password changes are applied immediately.
Password has not been modified.
1: Change password
x: Exit
p: Previous screen
n: Next screen

Select option: 1

Change Password
Enter old password:
Enter new password:
Confirm new password:
Password changed successfully.


Appliance Password
Password changes are applied immediately.
Password has been modified.
1: Change password
x: Exit
p: Previous screen
n: Next screen

Select option: n
```

5. Change the host name. You must use an FQDN host name.

```
Host Name Configuration
Host name: unconfigured.appliance
1.: Change the host name
x: Exit
p: Previous screen
n: Next screen

Select option: 1

Change the Host Name
Enter the new host name (FQDN): igiva.us.example.com

Host Name Configuration
Host name: igiva.us.example.com
1: Change the host name
x: Exit
p: Previous screen
n: Next screen

Select option: n
```

Note: The host name is cited in the SSL certificate for the virtual appliance.

6. Configure network interface M1 with the IP address, subnet mask, and default gateway.

```
Management Interface Settings
1: Display device settings
2: Display policy
3: Configure M.1
4: Configure M.2
x: Exit
p: Previous screen
n: Next screen

Select option: 3

Configure M.1
Select an IPv4 configuration mode:
1: Automatic
2: Manual
Enter index: 2
Enter the IPv4 address: 192.0.2.21
Enter the IPv4 subnet mask: 255.255.254.0
Enter the IPv4 default gateway: 192.0.2.12
Select an IPv6 configuration mode:
1: Automatic
2: Manual
Enter index: 1

Management Interface Settings
1: Display device settings
2: Display policy
3: Configure M.1
4: Configure M.2
x: Exit
p: Previous screen
n: Next screen

Select option: n
```

7. Configure the DNS for the virtual appliance.

```
DNS Configuration
No DNS servers configured.
1: Set DNS server 1
2: Set DNS server 2
3: Set DNS server 3
x: Exit
p: Previous screen
n: Next screen

Select option: 1

Set DNS Server 1
Enter the DNS Server IP address: 198.51.100.0


DNS Configuration
DNS server 1: 198.51.100.0
1: Set DNS server 1
2: Set DNS server 2
3: Set DNS server 3
x: Exit
p: Previous screen
n: Next screen

Select option: n
```

8. Configure the time settings for the virtual appliance.

```
Time Configuration
Time configuration changes are applied immediately.
Time: 08:28:58
Date: 12/05/2014
Time Zone: Asia/Kolkata
1: Change the time
2: Change the date
3: Change the time zone
x: Exit
p: Previous screen
n: Next screen

Select option: n
Command cancelled
1: Change the time
2: Change the date
3: Change the time zone
x: Exit
p: Previous screen
n: Next screen

Select option: n
```

9. Review the summary of configuration details.

   Note: If necessary, record the details of the assigned IP address, DNS, and host name of the virtual appliance.
10. Press 1 to accept the configuration.

Results

A message indicates that the policy changes are successfully applied, and the local management interface is restarted.

What to do next

Configure the IBM Security Identity Governance and Intelligence virtual appliance. See "Setting up a stand-alone or primary node for IBM Security Identity Governance and Intelligence with the initial configuration wizard" on page 23.

Amazon EC2 support

You can deploy IBM Security Identity Governance and Intelligence to the Amazon Elastic Compute Cloud (Amazon EC2) environment.

Amazon EC2 is a web service that provides:

- Scalable computing capacity in the Amazon Web Services (AWS) cloud
- Capability to deploy an Amazon Machine Image (AMI)

Deploying IBM Security Identity Governance and Intelligence to Amazon EC2 involves the following processes:

1. Create an Amazon Machine Image (AMI) from the appliance VHD image.
2. Launch an instance of the AMI in Amazon EC2.

For details about how to use the Amazon EC2 command line interface to launch an instance, see Launching an Instance Using the Amazon EC2 CLI.

Creating an Amazon Machine Image (AMI) from the Virtual Hard Disk (VHD) file

Upload the appliance VHD image to Amazon EC2 and create an AMI so that it can be deployed in Amazon EC2.

About this task

Follow these steps to manually upload an image and create an AMI with the Amazon EC2 console.

Procedure

1. Download and install the Amazon EC2 API Tools. You can download the tool from the Amazon EC2 API Tools page.
2. Run the following commands in the specified sequence to upload the VHD to Amazon EC2 and create an AMI.

Sequence	Command	Description
1	ec2-import-volume	Imports the appliance VHD into Amazon EC2.
2	ec2-describe-conversion-tasks	Monitors the `ec2-import-volume` task to show when the task is complete.
3	ec2-create-snapshot	Creates a snapshot of the imported disk image. This snapshot is required during the AMI registration process.
4	ec2-describe-snapshots	Monitors the status of the snapshot creation to show when the snapshot task is complete.
5	ec2-register	Registers a snapshot as a new AMI. You must use the following parameter values when you register the AMI: **architecture:** x86_64 **kernel:** Use the appropriate parameter value for the kernel ID. **root device name:** /dev/xvda **virtualization type:** paravirtual

Sequence	Command	Description
6	ec2-delete-disk-image	Removes the uploaded disk image from the storage bucket. The image is no longer required after you finish registering an AMI from the image.

Launching the appliance AMI

Launch an instance of the appliance AMI to run the appliance in Amazon EC2.

About this task

Follow these steps to manually launch an instance of the appliance AMI with the Amazon EC2 console.

Procedure

1. Log in to the Amazon EC2 console.
2. Go to **INSTANCES** > **Instances** > **Launch Instance**.
3. Select the IBM Security Identity Governance and Intelligence AMI that you want to launch.
4. Click **Launch**.
5. In the Choose an Instance Type window, select an instance type and click **Next: Configure Instance Details**.
6. In the Configure Instance Details window, select the options that best fit your environment and click **Next: Add Storage**.
7. In the Add Storage window, validate the storage and click **Next: Tag Instance**.
8. In the Tag Instance window, add any desired tags and then click **Click Next: Configure Security Group**.
9. In the Configure Security Group window, ensure that the selected security group allows inbound SSH and HTTPS access to the appliance. Restrict the access to only those IP addresses from which the appliance is administered. Click **Review and Launch**.
10. Review the details in the Review Instance window and click **Launch**.
11. In the Select an existing key pair or Create a new key pair window, you can opt to **Proceed without a key pair**. Check the acknowledgment check box. Click **Launch Instances** to proceed.

    Note: You do not need to associate a key pair with the instance. If you want to log on to the console of the launched instance, log on as the **admin** user.
12. Click **NETWORK & SECURITY** > **Network Interfaces**.
    a. Click **Create Network Interface**.
    b. On the Create Network Interface window, select a subnet and an appropriate security group. Since IBM Security Identity Governance and Intelligence requires 3 network interface cards, you must create another network interface.

       Note: By default, only one network interface is created with every instance. This interface is the primary interface, which cannot be removed from the instance.

   c. Select a network interface. Right-click the interface and click **Change** > **Source/Dest.Check** > **Disable**. Repeat this step for all the interfaces.

13. Select the appliance instance and complete these steps.
   a. Right-click the appliance instance.
   b. Select **Instance State** > **Stop**.
   c. Right-click the appliance instance.
   d. Select **Networking** > **Attach Network Interface**. Similarly, attach another network interface and start the instance.
14. Go to **INSTANCES** > **Instances** to check the status of the appliance instance.

Setting up a stand-alone or primary node for IBM Security Identity Governance and Intelligence with the initial configuration wizard

Log on to the initial configuration wizard from the web user interface to complete the virtual appliance setup tasks for IBM Security Identity Governance and Intelligence.

Before you begin

- Configure the initial virtual appliance settings.
- Collect the following information for this task:
  - Setup mode selection.

    Choose from **Guided** or **Advanced** setup mode. If **Advanced**, then supply a file with all configuration details in the expected format.
  - Application Interfaces configuration.
  - Mail server configuration.
  - If you choose to enable Identity Brokerage Providers, you must configure a directory server.
  - Database server configuration

About this task

During the setup process for configuring the IBM Security Identity Governance and Intelligence, the Setup Progress pane displays these links.

Import Settings
Imports the service settings. See Exporting or importing the configuration settings.

View logs
Checks for any messages and errors in the log files. See Managing the log configuration.

Manage snapshots
Uploads or applies a snapshot. See Managing the snapshots.

Procedure

1. In a web browser, enter the host name of the configured virtual appliance in the following format.

   `https://`*`host name of the virtual appliance`*`:9443`

   For example, `https://igiva1.jk.example.com:9443`
2. Log on to the virtual appliance console with the administrator credentials.

Note: The default user password is `admin`. If you changed the password during the virtual machine setup, use that password. If you did not change the password, use the default administrator password.

- **User name:** `admin`
- **Password:** `admin`

3. Select Primary. Click **Setup** under the appropriate image.
4. Choose a configuration mode and click **Next page**.

Option	Description
Guided Configuration	Define the configuration details one step at a time with the wizard. To continue, go to step 5 to configure the application interfaces.
Advanced Configuration	Do these steps. 1. Define the configuration with a `properties` response file that contains the necessary predefined values for the configuration parameters. See "Sample configuration response file" on page 25. 2. Upload the response file to the Mode Selection page. 3. Click **Next page**. 4. Go to step 10.

5. From the Application Interfaces Configuration page, configure the application interfaces and click **Next page**. For more information, see Managing application interfaces.
6. Configure the mail server and click **Next page**. For more information, see Managing the mail server configuration.
7. Optional: Enable Identity Brokerage Providers. If you want to use Identity Brokerage Providers, perform these steps.
   a. Click the **Use Identity Brokerage Providers** check box and click **Next**.
   b. When the confirmation message is displayed, click **Yes**.

   For more information about the Identity Brokerage Providers, see IBM Security Identity Governance and Intelligence .

   Note: If you select **Use Identity Brokerage Providers** , you must configure an external directory server. Continue to and perform step 8.
8. Optional: Configure the directory server and click **Next page**.

   For more information about the directory server settings, see Managing the directory server configuration.
9. Configure the database settings for the `Identity data store` and click **Next page**.

   For more information, see Managing the database server configuration.
10. On the **Completion** page, complete the following tasks that depend on the configuration mode you selected.

    Important: When the configuration process is completed successfully, restart the virtual appliance.

    - For **Guided Configuration**, review the instructions and click **Complete Setup**.

Important: When the configuration process begins, do not refresh the page or close the browser session.

- For **Advanced Configuration**, review the instructions and click **Start Configuration**.

After the configuration completes, a link to go to the dashboard is displayed. If the mail server configuration setup is correct, an email notification is sent when the virtual appliance configuration is complete.

Sample configuration response file

Set your configuration parameters for the IBM Security Identity Governance and Intelligence in a response file. After you update the response file with the correct values, upload the response file to configure the virtual appliance in the advanced configuration mode.

```
#######################################################
#
# You can do initial configuration of the
# IBM Security Identity Governance and Intelligence Appliance
# using a response file.
# Update the response file with correct values and provide it during the advanced mode
# of Initial configuration wizard.
#
# Note : Remove the redirection symbols(<>) from the input.
#
#######################################################

#
# Appliance Administrator User Credentials
#
igi.appliance.adminUserPwd=<admin user password>

#
# Identity Data store configuration Properties.
# You can either use IBM_DB or ORACLE_DB or ORACLE_DB_CUSTOM as the database type.
# Required inputs for database type
# 1) IBM_DB       - Provide input for igi.datastore.hostName, igi.datastore.port,
#                         igi.datastore.dbName and igi.datastore.userPwd.
#                         Other fields are optional
# 2) ORACLE_DB    - Provide input for igi.datastore.hostName, igi.datastore.port,
#                         igi.datastore.dbName, igi.datastore.userPwd and
#                         igi.datastore.isOracleServiceName.
#                         Set this value to true if igi.datastore.dbName
#                         is an Oracle Service name.
#                         and set it to false if it is a SID
# 3) ORACLE_DB_CUSTOM   - Provide input for igi.datastore.jdbcurl
#                         and igi.datastore.userPwd.
#                         Other fields are optional
#
igi.datastore.dbType=<IBM_DB or ORACLE_DB or ORACLE_DB_CUSTOM>
igi.datastore.hostName=<hostname>
igi.datastore.port=50000
igi.datastore.dbName=igidb
igi.datastore.jdbcurl=jdbc:oracle:thin:@//<hostname>:<port>/<dbName>
igi.datastore.userPwd=<user password>
igi.datastore.isOracleServiceName=<true or false>

#
# Identity Brokerage Providers Enablement
# If you want to enable Identity Brokerage Providers,
# provide a yes
# Else, you can leave this field blank or provide no
# If you enable Identity Brokerage Providers,
# you must provide the external directory server configuration details.
#
igi.identity.brokerage.providers.enable=
#
# Directory Server configuration properties
#

igi.ldap.hostName=<hostname>
igi.ldap.port=389
igi.ldap.organization.shortname=org
igi.ldap.organization.name=Organization
igi.ldap.bindDN=cn=root
igi.ldap.bindDNPwd=<password>
igi.ldap.dnLocation=dc=com

#
# Mail Server configuration properties
#
igi.mail.server=localhost
igi.mail.from=admin@in.ibm.com
igi.mail.port=25


#
# Application Interface configuration properties
#
igi.application.interface.FQDN=<FQDN for the interface>
igi.application.interface.type=<ipv4 or ipv6>
igi.application.interface.address=<ipv4 address or ipv6 address>
igi.application.interface.netmask=<Net mask for ipv4 address>
igi.application.interface.prefix=<Prefix for ipv6 address>
```

Planning for high availability

IBM Security Identity Governance and Intelligence virtual appliance with a load balanced cluster provides not only the expected high availability but also provides scalability.

Load balancer settings and requirements

Load balancing is a technique to extend user requests between two or more virtual appliances in a predefined cluster. Each virtual appliance in this cluster is called a node. Use of multiple nodes in such a cluster increases reliability and availability through redundancy.

Load balancer requirements

The most common mechanism to make a highly available deployment is to add a load balancer that distributes user requests to underlying servers. This deployment locks down any direct access to individual servers. In addition to making a highly available deployment of the IBM Security Identity Governance and Intelligence virtual appliance, it also provides horizontal scalability. See Figure 1 on page 27.

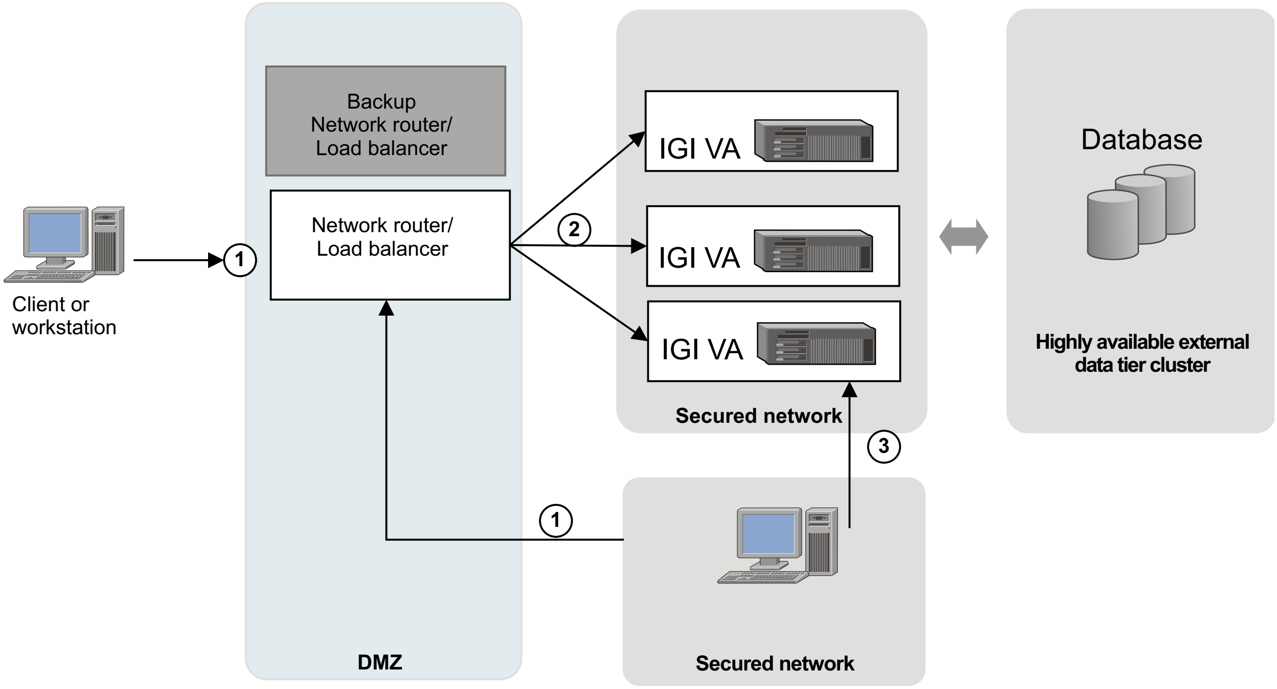

Figure 1. Deployment diagram of a typical load balancer in a customer environment

As shown in Figure 1, provide one or more backup load balancers or routers to avoid the load balancer itself from becoming a single point of failure.

The load balancer can be a dedicated hardware or software node that can route incoming requests to an IBM Security Identity Governance and Intelligence virtual appliance. This condition is true irrespective of whether the requests are coming from inside or outside a company network. See the request that is numbered as 1 in the diagram. Since these requests typically contain sensitive information such as user IDs or passwords, both the traffic paths must be over SSL. For example, see requests 1 and 2. The client request over SSL (marked #1) ends at the load balancer and a new SSL request (marked #2) is sent to a virtual appliance.

Load balancer installation requirements

The load balancer must meet the following requirements:

- Choose `Layer-7` or Layer-4 load balancers for this installation.

  To use layer-4 load balancer, all nodes must have the same fully qualified domain name (FQDN). The SSL certificates for all nodes must have the same distinguished name.
- The load balancer must be able to send separate SSL requests for each of the incoming requests.

Load balancer configuration requirements

In the load balancer configuration

- Enable Session Affinity for the load balancer. Use a load balancer with session affinity to route the traffic for the same client session to the same virtual appliance.
- The load balancer must detect unresponsive virtual appliances and stop directing any traffic to them.

- As shown in Figure 1 on page 27, keep one or more of the load balancer backups ready to avoid the load balancer as a single point of failure.

Setting up a virtual appliance cluster

IBM Security Identity Governance and Intelligence virtual appliance supports a high availability deployment mode. A high availability deployment is a cluster of multiple servers that are active and can process a request.

Before you begin

To set up a virtual appliance cluster, you must have a primary node ready and running and then add member nodes to it.

About this task

The IBM Security Identity Governance and Intelligence virtual appliance cluster is made of one primary node and other member nodes.

Procedure

1. Set up a primary node. See Setting up a stand-alone or primary node for IBM Security Identity Governance by using the initial configuration wizard. The primary node must be ready and running.
2. Add member nodes. See Add member nodes to the cluster.

Setting up a member node for IBM Security Identity Governance and Intelligence

For high availability deployment mode, you can set up a member node for the IBM Security Identity Governance and Intelligence cluster. The initial configuration tasks for the IBM Security Identity Governance and Intelligence are done in the initial configuration wizard. The initial configuration wizard uses the web interface to start and configure the virtual appliance.

Before you begin

Configure the initial virtual appliance settings.

About this task

In a web browser, log on to the initial configuration wizard from the web user interface after you complete the virtual appliance logon configuration. Complete the virtual appliance setup tasks from either the command line or the IBM Security Identity Governance and Intelligence virtual appliance management user interface.

Procedure

1. In a web browser, enter the host name of the configured virtual appliance in the following format.

   `https://`*`host name of the virtual appliance`*`:9443`

   For example, `https://igiva1.jk.example.com:9443`
2. Log on to the virtual appliance console with the administrator credentials.

   Note: The default user password is `admin`. If you changed the password during the virtual machine setup, use that password. If you did not change the password, use the default administrator password.

- **User name:** `admin`
- **Password:** `admin`

3. Select **Member**. Click **Setup** under the appropriate image.
4. In the **Connect to Primary** tab of the Setup Progress page, provide the details of the primary node.
   a. Type the host name in the **Primary node host name** field. For example, `isigva1.jk.example.com`.

      The primary node host name must be same that was used to create the primary virtual appliance host name.

   b. Type the user ID in the **Primary node administrator** field. The user ID must be the same ID that you used to log on to the IBM Security Identity Governance and Intelligence virtual appliance For example, `admin`.
   c. Type the password in the **Primary node administrator password** field. For example, `admin`.
5. Click **Test Connection** to validate the details and to verify this connection of the member node with the primary node. The system verifies whether the connection to the primary node can be made.
6. Click **Next page**.

   Note: The **Next page** button is activated only when the connection to the primary node is successful.

   The **Completion** tab is displayed.
7. From the Application Interfaces Configuration page, configure the application interfaces and click **Next page**. For more information, see Managing application interfaces.
8. Click **Fetch Configuration** to obtain configuration details from the primary node. A progress bar indicates about fetching the configuration details from the primary node. The **Start Configuration** button is activated only when the **Fetch Configuration** operation is completed successfully.
9. Optional: To review or edit the data in the **Connect to Primary** tab, click **Previous page**.
10. Click **Start Configuration** to start the initial configuration for the IBM Security Identity Governance and Intelligence virtual appliance. The Completion page opens to indicate the data synchronization process. Do one of these actions:
    - If the configuration is successful, a message indicates that the configuration is complete and provides a link to the dashboard.
    - If the configuration is not complete or not successful, a message indicates the reason. Do one of the following actions:
      – Click the **Log files** link to open the Log Retrieval and Configuration page and check for any messages and errors in the log files.
      – Click the **Click here** link to restart the configuration process in case of failures.

Changing a member node to a primary node

Use the Cluster Node Configuration page to change a member node to primary node in the IBM Security Identity Governance and Intelligence virtual appliance.

Before you begin

No active primary node must exist in this cluster.

About this task

If the primary node becomes unavailable for some reason, you can make another node the primary node. You might also want to change a member node to a primary node in the cluster for maintenance and other such tasks.

The **Configure** > **Manage Cluster** menu is displayed only in a cluster environment and not in a stand-alone environment.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Manage Cluster** > **Cluster Node Configuration**.
2. Select the member node that you want to make as a primary node from the list of available nodes.
3. Click **Make Primary**.
4. Click **Yes** to confirm the changes.

Removing a node from the cluster

Use the Cluster Node Configuration page to remove a node from the cluster.

About this task

The option to remove a node is available only from the primary node. You can remove a member node from a primary node, but you cannot remove the primary node itself.

If a primary node ceases to function, you can promote a member node to be the new primary node. See “Changing a member node to a primary node” on page 29. Then, you can remove the affected node from the cluster configuration. After the node is removed, it no longer functions as part of the cluster. After the node is repaired, you can add it back to the cluster.

The **Configure** > **Manage Cluster** menu is displayed only in a cluster environment and not in a stand-alone environment.

Procedure

1. From the **Appliance Dashboard** top-level menu, click **Configure** > **Manage Cluster** > **Cluster Node Configuration**.
2. Select a member node that you want to remove from the list of available nodes.
3. Click **Remove**.
4. Click **Yes** to confirm.

Results

The selected node is removed from the cluster.

Reconnecting a node into the cluster

Use the Cluster Node Configuration page to reconnect a node into the cluster of the IBM Security Identity Governance and Intelligence virtual appliance.

About this task

Depending on your requirement, you can reconnect a node into the cluster due to the following reasons:

- Adding a previously configured node to a cluster to increase scalability.
- A node that was shut off for maintenance is revived and must be introduced back in the cluster.
- If you see a reconnect notification on the **Appliance Dashboard** of a `Member node`.

You can reconnect only a `Member node` back to the cluster from the **Appliance Dashboard** of a `Member node`. You must provide the `Primary node` details to reconnect a node into the cluster.

The **Configure** > **Manage Cluster** menu is displayed only in a cluster environment and not in a stand-alone environment.

Procedure

1. From the **Appliance Dashboard** top-level menu, click **Configure** > **Manage Cluster** > **Cluster Node Configuration**.
2. Select the `Member node`.
3. Click **Reconnect**. The Reconnect pane is displayed.
4. In the Reconnect pane, provide the details for the node that you want to reconnect into the cluster.

   Primary node host name
   The host name of the `Primary node`. For example, `igiva1.jk.example.com`.

   Primary node administrator
   The user ID of the `Primary node` administrator. For example, `admin`.

   Primary node administrator password
   The administrator password of the `Primary node`. For example, `admin`.
5. Click **Yes** to confirm.

Results

The `Member node` is reconnected into the cluster.

Synchronizing a member node with a primary node

Use the Cluster Node Configuration page to synchronize a member node with a primary node in the IBM Security Identity Governance and Intelligence virtual appliance.

About this task

The **Configure** > **Manage Cluster** menu is displayed only in a cluster environment and not in a stand-alone environment.

In the primary node virtual appliance console, all nodes in the cluster are displayed in the Cluster Node Configuration table.

In the member node virtual appliance console, only the current member node is displayed in the Cluster Node Configuration table.

Synchronize the following nodes in the cluster for any configuration changes that you make in the IBM Security Identity Governance and Intelligence virtual appliance.

Member node

In the Cluster Node Configuration table of the Cluster Node Configuration page, select a member node for synchronization. The **Synchronize** button is not active until you select a node.

Wait for the synchronization process to complete.

Primary node

In the Cluster Node Configuration page, select one or more member nodes except the primary node for synchronization. The **Synchronize** button is not active when:

- The primary node is selected.
- The status of the selected node is displayed as `Synchronizing` in the **Synchronization State** column of the Cluster Node Configuration table.

The primary node submits the synchronization request to each of the node that was selected. You can view the synchronization status in the **Synchronization State** column of the Cluster Node Configuration table.

Note: Before you do a synchronization operation, address all the notifications on the primary node.

The **Synchronization State** column displays these synchronization states:

Table 7. Synchronization state table

Status	Description	Action
`Not Connected`	Displays when a member node cannot connect to a primary node or when a primary node cannot connect to the member node.	Connect the member node with the primary node. For a node with the `Not Connected` status, click **Reconnect Node** to connect that node into the cluster. See "Reconnecting a node into the cluster" on page 30.
`Not Synchronized`	Displays when the member node is not synchronized with the primary node.	Synchronize the member node with the primary node. See the following procedure.
`Synchronized`	Displays when the member node is synchronized with the primary node.	No action is required.
`Synchronizing`	Displays when the member node is synchronizing with the primary node.	Wait until the synchronization is complete. Click the **Refresh** icon to get the most recent status.
`Not Applicable`	Displays if the cluster node is a primary node because the primary node does not require any synchronization.	No action is required.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Manage Cluster** > **Cluster Node Configuration**.
2. Do the following actions.

- From the member node console, select the current member node and click **Synchronize** to synchronize it with the primary node.

  A progress bar indicates the synchronization process. It retrieves configuration information from the primary node for any configuration changes and synchronizes within the same node.
- From the primary node console, select one or more member nodes and click **Synchronize**.

  A synchronization request is submitted to each of the node that was selected.

The member node is synchronized with the primary node.

3. Optional: Click **Refresh** to display the recently updated data.

Logging on to the virtual appliance console

To access the virtual appliance, you must know the login URL and the user name and password.

About this task

The default user name and password for the virtual appliance console is `admin`. If you changed the password during the virtual machine setup, use that password. If you did not change the password, use the default administrator password, which is `admin`.

Procedure

1. In a web browser, type the URL as `https://`*`igiva_hostname`*`:9443` to open the **Appliance Dashboard** of the IBM Security Identity Governance and Intelligence virtual appliance console. For example, `https://igiva.example.com:9443`.
2. Enter the user name as `admin`.
3. Enter the password as `admin` or the password that was supplied during the virtual machine setup.
4. Click **Login**.

Results

The appliance dashboard is displayed. For more information, see Appliance Dashboard.

Logging on to the consoles from the appliance dashboard

You can log on to the administrative and self-service consoles from the **Appliance Dashboard**.

Procedure

1. Log on to the **Appliance Dashboard**.

   See "Logging on to the virtual appliance console" to log on to the appliance dashboard.
2. In the **Quick Links** widget of the **Appliance Dashboard**, click a link to open the application. The available links that you can access are the IBM Security Identity Governance and Intelligence administration console and the service center. The Log In page for the application is displayed.

3. Log on to IBM Security Identity Governance and Intelligence application. The default user ID is `admin` and password is `admin`. Change the password before you start any operations.

Chapter 4. Upgrade or migrate the virtual appliance to IBM Security Identity Governance and Intelligence Version 5.2.1

You can use either a USB device or a firmware update transfer utility to upgrade the virtual appliance. You can also migrate from Version 5.1.1 to Version 5.2.1.

Note: After you complete the upgrade or migration, change the reverse proxy or load balancer configuration to update the port number to `9343` if you use an external authentication for IBM Security Identity Governance and Intelligence.

Upgrading the virtual appliance from a USB Device

Install the firmware update to upgrade the IBM Security Identity Governance and Intelligence virtual appliance.

Before you begin

Before you apply the firmware update to upgrade the IBM Security Identity Governance and Intelligence virtual appliance, back up your data tier, which is all the databases and the directory server.

Note: JVM properties are not upgraded during the virtual appliance upgrade.

About this task

The virtual appliance has two partitions with separate firmware on each partition. The partitions are swapped during the firmware updates to roll back the firmware updates when required. Either partition can be active.

In the factory-installed state, Partition 1 is active and contains the firmware version of the currently released product. When you apply a firmware update, the update is installed on Partition 2, and your policies and settings are copied from Partition 1 to Partition 2.

The IBM Security Identity Governance and Intelligence virtual appliance restarts the system by using Partition 2, which is now the active partition.

You must use the command-line interface (CLI) to install the upgrade.

Procedure

1. Download the `igi_*.pkg` build to a location of your choice on the virtual system.
2. Access the command-line interface (CLI) of the virtual appliance by using either an `ssh` session or the console.
3. Copy the `igi_*.pkg` to a USB device.
4. Attach the USB device to your virtual system.
5. In the virtual appliance CLI, run the **`igi`** command to display the `igi` prompt.
6. At the `igi` prompt, do the following steps.
   a. Run the **`upgrade`** command.
   b. Run the **`list`** command to list the firmware updates from the USB device.

c. Run the **transfer** command to transfer the firmware updates from the USB device to the virtual system.
d. Run the **install** command.
e. Select the index of the firmware update that you want to install to the virtual system and press Enter.

   The following results occur.

   - The upgrade process formats Partition 2 and installs the new firmware.
   - When you apply the firmware update, your policies and settings are copied from Partition 1 to Partition 2.
   - On completion, the process indicates that you must restart the virtual system.

7. Type the **reboot** command and press Enter to restart the virtual system. Partition 2 is now the active partition.

   The following results occur.

   - After the virtual appliance restarts from the Partition 2, all Partition 1 configuration is applied to the Partition 2.
   - After the configuration is applied to the virtual appliance, the process indicates you to restart the virtual appliance.
8. Restart the virtual appliance to complete the upgrade process.
9. For the Identity data store, clear the **Service Integration Bus** before you restart the IBM Security Identity Governance and Intelligence. See Clear the service integration bus.
10. Restart the IBM Security Identity Governance and Intelligence.
11. Optional: Back up Partition 2 in to Partition 1 after the successful completion of the firmware upgrade. The backup process overwrites the information that is in Partition 1.

    Do the following actions:

    - If the upgrade process failed, check and fix any errors.
    - Use Partition 1 to set it as the active partition and restart it.

      Partition 1 now becomes the active partition.

Upgrading the IBM Security Identity Governance and Intelligence virtual appliance with firmware update transfer utility

Previously you could update the IBM Security Identity Governance and Intelligence virtual appliance firmware by using a USB device only. Starting at firmware release 5.2.0.1, firmware (`.pkg`) files can be transferred with the Java™ utility. A USB device is no longer required to update the Identity Governance and Intelligence virtual appliance.

Before you begin

You need the appropriate compressed file such as `5.2.-ISS-ISGI-FP0001` file. Go to https://www.ibm.com/support/entry/portal/product/security_systems/ibm_security_identity_governance?productContext=2132047255to determine the file name and to download the file. This compressed file contains the following files.

- The firmware update `.pkg` file, for example `5.2-ISS-ISGI-FP0001.pkg`).
- The keystore `.jks` file (`temptrust.jks`). The `temptrust.jks` file is the default file. You can use a custom keystore file instead of the default file.
- The Java Utility .jar file (`File Upload.jar`)

About this task

This utility performs the same function as the command-line interface (CLI) command of the Identity Governance and Intelligence virtual appliance.

igi > **upgrade** > **transfer**

For general information about this utility, see http://www.ibm.com/support/docview.wss?uid=swg21965218.

Procedure

1. Download the package from the IBM Fix Central.
2. Extract the `*.pkg` build to a location of your choice.
3. Copy the utility to a system where Java, Version 1.7 is installed.
4. Copy these files to the file system.
   - The `.pkg` firmware update file.
   - The keystore (`jks`) file.
   - The Java utility `File Upload.jar`.
5. Run the following Java command to upload the `.pkg` file.

   Usage

   ```
   java -jar FileUpload.jar Hostname:PortAdminIdAdminPasswordTruststore FilepathTruststore
        PasswordAbsolute path to pkg file
   ```

   Example

   ```
   java -jar FileUpload.jar igiva.in.ibm.com:9443 admin admin /work/temptrust.jks WebAS
        /Downloads/5.2-ISS_SIGI-FP0001.pkg
   ```
6. If you did not update the default certificates, use the supplied `temptrust.jks` file.

   If you previously updated the default certificate on the Identity Governance and Intelligence virtual appliance, `temptrust.jks` does not work. Use an updated `jks` file that is based on your updated certificate.
7. Access the command-line interface (CLI) of the Identity Governance and Intelligence virtual appliance to install the firmware with the following command.

   Note: Run this command after you transfer the `.pkg` file.

   igi > **upgrade** > **install**
8. Restart the virtual appliance.

Migrating a virtual appliance cluster

Use this procedure to migrate a virtual appliance cluster from IBM Security Identity Governance and Intelligence Version 5.2 to Version 5.2.1.

Procedure

1. Select one of the nodes in the cluster and upgrade it to Version 5.2.1 by using the firmware upgrade utility. See "Upgrading the IBM Security Identity Governance and Intelligence virtual appliance with firmware update transfer utility" on page 36. This node becomes the primary node in the new cluster.
2. Discard all the other nodes.
3. Use the Version 5.2.1 `.iso` image to install a new IBM Security Identity Governance and Intelligence virtual appliance. When prompted by the activation wizard, select member node setup for this virtual appliance. Then connect it to the primary node that you created in Step 1.

4. Repeat Step 3 for each node that you want to add to the cluster.

Migrating the virtual appliance from Version 5.1.1 to Version 5.2.1

Migration from the virtual appliance Version 5.1.1 to Version 5.2.1 is a two stage process. You must first migrate the virtual appliance to Version 5.2 and then migrate to Version 5.2.1.

Procedure

1. Migrate from IBM Security Identity Governance and Intelligence Version 5.1.1 to Version 5.2. Follow the migration instructions listed at Migrating the virtual appliance from V5.1.1 to V5.2.0 with the Export/Import Settings.
2. Update to Version 5.2.1. You can use either the USB device method or the firmware update transfer utility method to migrate to Version 5.2.1.
   - “Upgrading the virtual appliance from a USB Device” on page 35
   - “Upgrading the IBM Security Identity Governance and Intelligence virtual appliance with firmware update transfer utility” on page 36

Verify current set of tasks and jobs for the Task Planner module

The migration process acts on tasks and jobs of IBM Security Identity Governance and Intelligence.

The migration process does not include the following jobs or tasks:

- Customized jobs or tasks that were possibly added after the installation of Version 5.2.
- The original jobs or tasks of product that were possibly renamed.

Table 8 lists the entire set of tasks and jobs.

Table 8. Tasks and Jobs collection for IBM Security Identity Governance and Intelligence installation

Task	Jobs
AccessRiskControls4SAP	BatchProcessedActionsARCS
AccessRiskControls4SAPSync	ARCSRiskAlign
	ARCSSoDAlign
	CorePermissionStateRefresh
Advanced Rules [example]	AdvancedRuleFlow
CleanUp Demo Env [Warning!]	CleanUp DEMO Env
Connectors	ConnectorPolling4Connect
	ConnectorPolling4Reconciliation
EmailService	SystemEmailService
Housekeeping	CoreUserAuthorizationRefresh
	CoreHistoryRefresh
	BatchProcessActionsAGC
	ACContinousCampaignManagement
	BatchProcessedActionsARC
	Persistent Consolidation
HousekeepingOptimizer	BatchProcessedActionAO

Table 8. Tasks and Jobs collection for IBM Security Identity Governance and Intelligence installation (continued)

Task	Jobs
NightShift	CoreTimeBoundActions
	SystemRiskAnalysis
	ACRefreshCampaignReviewer
	CorePermissionStateRefresh
ReportSpooler	BatchProcessedActionsReports
RoleMining	RoleCandidatePublished
	RoleConsolidation
	RoleDeprovisioning
RuleEngine	Event IN Dispatcher
	Event TARGET Dispatcher
	Event OUT Dispatcher
	Event INTERNAL Dispatcher
SystemHierarchyAttributeRefresh	CoreHierarchyAttributeRefresh

Procedure

1. Log on as administrator to the **Task Planner**.
2. Select **Task Planner** > **Manage** > **Tasks**.
3. Select a task in the left frame and click the **Jobs** tab in the right frame to view the jobs that are joined to the selected task.
4. Select **Task Planner** > **Manage** > **Jobs** to view the entire set of jobs.
5. Before you go to the next step, verify that all these tasks or jobs are in your current environment.
6. If you renamed one or more of the original tasks or jobs, restore the original names.

Closing campaigns

Use the **Certification Campaigns** tab to close all open campaigns.

About this task

Before you run the migration scripts, you must close all open campaigns. Complete the following steps to close all the open campaigns.

Procedure

1. Log on as administrator to the Access Governance Core.
2. Select **Configure** > **Certification Campaigns**.
3. In the left frame of **Certification Search**, select an open campaign, which is indicated by a green icon.
4. In the same frame, click **Actions** > **Close**.
5. Repeat steps 3 and 4 to close all open campaigns.

Updating the Oracle server for V5.2.1 semi-automatically

To update an IBM Security Identity Governance Version 5.2 installation to IBM Security Identity Governance and Intelligence Version 5.2.1, install the firmware update. After you install the Oracle server, you must configure it for IBM Security Identity Governance and Intelligence virtual appliance.

Before you begin

- The Oracle Server version 12c must be installed. It is the minimum version level required for updating to IBM Security Identity Governance and Intelligence Version 5.2.1.
- The Oracle Client must be installed.
- You must know the common database parameters such as the IP address, server port, and SID.

Note: During the migration procedure, for some particular conditions, this diagnostic message can be present in the log file.

```
"NO FLOW <something> FOUND".
```

This message does not identify an error of the procedure and can be ignored.

About this task

The following tags customize the IBM Security Identity Governance and Intelligence Oracle database installation.

Table 9. Tags to customize the IBM Security Identity Governance and Intelligence Oracle database installation.

Tags	Description
IgiSID	Oracle database instance name (SID)
DBServer	Oracle Server IP address or DNS name
DBPort	Oracle listener port
ServiceName	Oracle Service Name

The scripts for the installation of the DB can be delivered in 4 distinct `.zip` files, all containing the same set of files and distinguished by the license:

- `SEC_IDNTY_GVN_INTL_CMP_V5.2.1_DT_IN_.zip`
- `SEC_IDNTY_GVN_INTL_ANL_V5.2.1_DT_IN_.zip`
- `SEC_IDNTY_GVN_INTL_LFC_V5.2.1_DT_IN_.zip`
- `SEC_IDNTY_GVN_INTL_IEE_V5.2.1_DT_IN_.zip`

Depending on the license that you purchased, unpack one of these `.zip` files into a directory of your choice, *<your_path>/<UPDSCRIPTDIR>*.

Procedure

1. Configure the `tnsnames.ora` file.
   a. Log in with root or Administrator privileges. On UNIX and Linux:
   ```
   sudo su -
   ```
   b. Switch to the `oracle` user. On UNIX and Linux:
   ```
   sudo su oracle
   ```

c. Browse to the `tnsnames.ora` file. For example,

   oracle_home/db/network/admin

d. Edit the file in a text editor such as **vi** or Notepad.

e. If the network instance is not configured correctly, add the following section.

```
<IgiSID> =
  (DESCRIPTION =
   (ADDRESS_LIST =
     (ADDRESS = (PROTOCOL = TCP)(HOST = <DBserver>)(PORT =
<DBport>))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = < ServiceName>)
    )
      )
```

   Example 1

```
XE =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = 127.0.0.0)(PORT = <1521>))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = <XE>)
    )
  )
```

   Example 2

```
MYDB =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = <oracle_server_ip>)(PORT = <1521>))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = <MyDB_service_name>)
    )
  )
```

2. On UNIX and Linux systems, change the file permissions in the installation directory.

   a. Use the following command to change directory to <*UPDSCRIPTDIR*>:

      cd <*your_path*>/<*UPDSCRIPTDIR*>

   b. Use the following command to ensure that the data base user has `write` permission to access the log file output:

      chmod -R 777 *

3. As the instance owner, check that the configuration is working by connecting to the database with the following command:

   `sqlplus system/<password>@<IgiSID>`

   If the connection test ended well, you can exit from the `sqlplus` with the following command:

   `exit`

   And exit from the `oracle` user with the following command:

   `exit`

4. Configure the `oracle_update.sh` or `oracle_update.bat` file.

   a. Open the `oracle_update` file with a text editor.

b. Modify the **ORACLE_BASE** and **ORACLE_HOME** variables according to your installation.

   These variables are necessary for **sqlplus** to work.

c. Modify the **ORACLE_SERVER** variable with the value of *IgiSID* previously configured in the tnsnames.ora file.

d. If you changed the default product password from ideas, change it accordingly in the sqlplus commands.

5. Connect as root or Administrator, run the update script, and record the results in the log file.

   On UNIX and Linux:

```
dos2unix oracle_update.sh
./oracle_update.sh > upgrade.log
```

   On Windows:

```
oracle_update.bat > upgrade.log
```

Updating the Oracle server for V5.2.1 manually

To update an IBM Security Identity Governance Version 5.2 installation to IBM Security Identity Governance and Intelligence Version 5.2.1, install the firmware update. After you install the Oracle server, you must configure it for IBM Security Identity Governance and Intelligence virtual appliance.

Before you begin

- Verify that you are starting your migration from IBM Security Identity Governance Version 5.2.
- The Oracle Server version 12c must be installed. It is the minimum version level required for updating to IBM Security Identity Governance and Intelligence Version 5.2.1.
- The Oracle Client must be installed.
- You must know the common database parameters such as the IP address, server port, and SID.

Note: During the migration procedure, for some particular conditions, this diagnostic message can be present in the log file.

```
"NO FLOW <something> FOUND".
```

This message does not identify an error of the procedure and can be ignored.

About this task

The following tags customize the IBM Security Identity Governance and Intelligence Oracle database installation.

Table 10. Tags to customize the IBM Security Identity Governance and Intelligence Oracle database installation.

Tags	Description
IgiSID	Oracle database instance name (SID)
DBServer	Oracle Server IP address or DNS name
DBPort	Oracle listener port
ServiceName	Oracle Service Name

The scripts for the installation of the DB can be delivered in 4 distinct .zip files, all containing the same set of files and distinguished by the license:

- SEC_IDNTY_GVN_INTL_CMP_V5.2.1_DT_IN_.zip
- SEC_IDNTY_GVN_INTL_ANL_V5.2.1_DT_IN_.zip
- SEC_IDNTY_GVN_INTL_LFC_V5.2.1_DT_IN_.zip
- SEC_IDNTY_GVN_INTL_IEE_V5.2.1_DT_IN_.zip

Depending on the license that you purchased, you must use the right .zip file. See step 2.

Procedure

1. Configure the tnsnames.ora file.
   a. Log in with root or Administrator privileges. On UNIX and Linux:
      ```
      sudo su -
      ```
   b. Switch to the oracle user. On UNIX and Linux:
      ```
      sudo su oracle
      ```
   c. Browse to the tnsnames.ora file. For example, *oracle_home*/db/network/admin.
   d. Edit the file in a text editor. For example, **vi** or Notepad.
   e. If the network instance is not configured correctly, add the following section:
      ```
      <IgiSID> =
        (DESCRIPTION =
          (ADDRESS_LIST =
            (ADDRESS = (PROTOCOL = TCP)(HOST = <DBserver>)(PORT = <DBport>))
          )
          (CONNECT_DATA =
            (SERVICE_NAME = <ServiceName>)
          )
        )
      ```

      Example 1
      ```
      XE =
        (DESCRIPTION =
          (ADDRESS_LIST =
            (ADDRESS = (PROTOCOL = TCP)(HOST = 127.0.0.0)(PORT = <1521>))
          )
          (CONNECT_DATA =
            (SERVICE_NAME = <XE>)
          )
        )
      ```

      Example 2
      ```
      MYDB =
        (DESCRIPTION =
          (ADDRESS_LIST =
            (ADDRESS = (PROTOCOL = TCP)(HOST = <oracle_server_ip>)(PORT = <1521>))
          )
          (CONNECT_DATA =
            (SERVICE_NAME = <MyDB_service_name>)
          )
        )
      ```
   f. Check that the configuration is working by connecting to the database with the following command:
      ```
      sqlplus system/<password>@<IgiSID>
      ```

If the connection test ended well, you can exit from the `sqlplus` with the following command:

```
exit
```

And exit from the `oracle` user with the following command:

```
exit
```

2. Run the update scripts.

   Note: Check the log in the folders after you run each script to see any errors. The log content is the same that you see on the screen during the script execution.

   a. With root or Administrator privileges, unpack the `.zip` file that contains the scripts into a directory of your choice, *<your_path>/<UPDSCRIPTDIR>*.

   b. Change the directory to *<UPDSCRIPTDIR>* with the following command.

   ```
   cd <your_path>/<UPDSCRIPTDIR>
   ```

   c. On UNIX and Linux systems, run the following command.

   ```
   chmod -R 777 *
   ```

   d. Change the directory to `AccessGovernanceCoreBackend`.

   ```
   cd <UPDSCRIPTDIR>/AccessGovernanceCoreBackend
   ```

   Run the following commands.

   ```
   sqlplus iga_admin/ideas@<IgiSID> @agc_pre_req_upgrade_73_to_74.sql
   sqlplus iga_core/ideas@<IgiSID> @agc_pre_req_upgrade_73_to_74.sql
   sqlplus ccs_core/ideas@<IgiSID> @arc4s_pre_req_upgrade_73_to_74.sql
   ```

   e. Change the directory to `Localization`.

   ```
   cd ../Localization
   ```

   Run the following commands.

   ```
   sqlplus iga_admin/ideas@<IgiSID> @agc_localization.sql
   sqlplus iga_core/ideas@<IgiSID> @agc_localization.sql
   sqlplus ccs_core/ideas@<IgiSID> @arc4s_localization.sql
   ```

   f. Change the directory to `AccessGovernanceCoreBackend`.

   ```
   cd ../AccessGovernanceCoreBackend
   ```

   Run the following commands.

   ```
   sqlplus iga_admin/ideas@<IgiSID> @agc_upgrade_73_to_74.sql
   sqlplus iga_core/ideas@<IgiSID> @agc_upgrade_73_to_74.sql
   sqlplus ccs_core/ideas@<IgiSID> @arc4s_upgrade_73_to_74.sql
   ```

   g. Change the directory to `AccessRequestsBackend`.

   ```
   cd ../AccessRequestsBackend
   ```

   Run the following commands.

   ```
   sqlplus iga_admin/ideas@<IgiSID> @arm_upgrade_13_to_14.sql
   sqlplus iga_core/ideas@<IgiSID> @arm_upgrade_13_to_14.sql
   ```

   h. Change the directory to `AccessOptimizerBackend`.

   ```
   cd ../AccessOptimizerBackend
   ```

   Run the following commands.

   ```
   sqlplus aa_admin/ideas@<IgiSID> @aa_upgrade_53_to_54.sql
   sqlplus aa_core/ideas@<IgiSID> @aa_upgrade_53_to_54.sql
   ```

   i. Change the directory to `AccessRiskControlsForSAPBackend`.

   ```
   cd ../AccessRiskControlsForSAPBackend
   ```

   Run the following command.

   ```
   sqlplus ccs_core/ideas@<IgiSID> @arc4s_upgrade_43_to_44.sql
   ```

   j. Change the directory to `DeskBackend`.

```
cd ../DeskBackend
```

Run the following command.

```
sqlplus iga_service/ideas@<IgiSID> @desk_upgrade_23_to_24.sql
```

k. Change the directory to EmailBackend. :

```
cd ../EmailBackend
```

Run the following commands.

```
sqlplus iga_admin/ideas@<IgiSID> @es_upgrade_23_to_24.sql
sqlplus iga_core/ideas@<IgiSID> @es_upgrade_23_to_24.sql
```

l. Change the directory to EnterpriseConnectorsBackend.

```
cd ../EnterpriseConnectorsBackend
```

Run the following commands.

```
sqlplus iga_admin/ideas@<IgiSID> @ec_upgrade_33_to_34.sql
sqlplus iga_core/ideas@<IgiSID> @ec_upgrade_33_to_34.sql
```

m. Change the directory to JobBackend.

```
cd ../JobBackend
```

Run the following commands.

```
sqlplus iga_admin/ideas@<IgiSID> @job_upgrade_23_to_24.sql
sqlplus iga_core/ideas@<IgiSID> @job_upgrade_23_to_24.sql
sqlplus ccs_core/ideas@<IgiSID> @job_upgrade_23_to_24.sql
sqlplus aa_admin/ideas@<IgiSID> @job_upgrade_23_to_24.sql
sqlplus aa_core/ideas@<IgiSID> @job_upgrade_23_to_24.sql
sqlplus iga_report_admin/ideas@<IgiSID> @job_upgrade_23_to_24.sql
sqlplus iga_report_core/ideas@<IgiSID> @job_upgrade_23_to_24.sql
```

n. Change the directory to ReportBackend.

```
cd ../ReportBackend
```

Run the following commands.

```
sqlplus iga_report_admin/ideas@<IgiSID> @rd_upgrade_23_to_24.sql
sqlplus iga_report_core/ideas@<IgiSID> @rd_upgrade_23_to_24.sql
```

o. Change the directory to RuleEngineBackend.

```
cd ../RuleEngineBackend
```

Run the following commands.

```
sqlplus iga_admin/ideas@<IgiSID> @re_upgrade_23_to_24.sql
sqlplus iga_core/ideas@<IgiSID> @re_upgrade_23_to_24.sql
sqlplus ccs_core/ideas@<IgiSID> @re_upgrade_23_to_24.sql
```

p. Change the directory to TaskPlannerBackend.

```
cd ../TaskPlannerBackend
```

Run the following commands.

```
sqlplus iga_quartz/ideas@<IgiSID> @quartz_upgrade.sql
sqlplus iga_service/ideas@<IgiSID> @sk_upgrade_23_to_24.sql
```

q. Change the directory to AuditHelper.

```
cd ../AuditHelper
```

Run the following command.

```
sqlplus iga_service/ideas@<IgiSID> @account_upgrade_33_to_34.sql
```

r. Change the directory to SIB_IB_ILC.

```
cd ../SIB_IB_ILC
```

Run the following commands.

```
sqlplus itimuser/ideas@<IgiSID> @IB_ILC_upgrade.sql
sqlplus itiml000/ideas@<IgiSID> @SIB_upgrade.sql
```

s. Change the directory to AccessGovernanceCoreBackend.

```
cd ../AccessGovernanceCoreBackend
```

Run the following commands.

```
sqlplus iga_admin/ideas@<IgiSID> @report_assignment.sql
sqlplus iga_core/ideas@<IgiSID> @report_assignment.sql
```

t. Change the directory to `ReportBackend`.

```
cd ../ReportBackend
```

Run the following commands.

```
sqlplus iga_report_admin/ideas@<IgiSID> @revoke_from_agc.sql
sqlplus iga_report_core/ideas@<IgiSID> @revoke_from_agc.sql
```

u. Change the directory to `IdeasModule`.

```
cd ../IdeasModule
```

Run the following commands.

```
sqlplus iga_admin/ideas@<IgiSID> @ideas_module_upgrade.sql
sqlplus iga_core/ideas@<IgiSID> @ideas_module_upgrade.sql
sqlplus ccs_core/ideas@<IgiSID> @ideas_module_upgrade.sql
sqlplus aa_admin/ideas@<IgiSID> @ideas_module_upgrade.sql
sqlplus aa_core/ideas@<IgiSID> @ideas_module_upgrade.sql
sqlplus iga_report_admin/ideas@<IgiSID> @ideas_module_upgrade.sql
sqlplus iga_report_core/ideas@<IgiSID> @ideas_module_upgrade.sql
```

Updating the DB2 server for V5.2.1 semi-automatically

To update IBM Security Identity Governance V5.2 to IBM Security Identity Governance and Intelligence Version 5.2.1, you must configure it with these instructions.

Before you begin

- The DB2 Server, Version 10.5.0, Fix Pack 5, must be installed. It is the minimum version level that is required to update to IBM Security Identity Governance and Intelligence Version 5.2.1.
- The DB2 Client must be installed.
- You must know the common database parameters such as the IP address, server port, and SID.

Note: During the migration procedure, under particular conditions, this diagnostic message can be found in the log file.

```
"NO FLOW <something> FOUND".
```

This message does not identify an error in the procedure and can be ignored.

About this task

The following tags are used to customize the IBM Security Identity Governance and Intelligence DB2 database installation.

Table 11. Tags to customize the IBM Security Identity Governance and Intelligence DB2 database installation.

Tags	Description
DBServer	DB2 Server IP address or DNS name.
DBPort	DB2 instance port.
IGI_DB	DB2 database name.
INSTANCE_OWNER	DB2 instance owner of the database instance.
PASSWORD	DB2 instance owner password.

Table 11. Tags to customize the IBM Security Identity Governance and Intelligence DB2 database installation (continued).

Tags	Description
FQ_IGI_DB	*<DBServer>*:*<DBPort>*/*<IGI_DB>*

The scripts for the installation of the DB can be delivered in 4 distinct `.zip` files, all containing the same set of files and distinguished by the license:

- `SEC_IDNTY_GVN_INTL_CMP_V5.2.1_DT_IN_.zip`
- `SEC_IDNTY_GVN_INTL_ANL_V5.2.1_DT_IN_.zip`
- `SEC_IDNTY_GVN_INTL_LFC_V5.2.1_DT_IN_.zip`
- `SEC_IDNTY_GVN_INTL_IEE_V5.2.1_DT_IN_.zip`

Depending on the license that you purchased, unpack one of these `.zip` files into a directory of your choice, *<your_path>*/*<UPDSCRIPTDIR>*, and proceed as indicated in the following steps.

Procedure

1. On UNIX and Linux systems, change the file permissions in the installation directory.
   a. Use the following command to change directory to *<UPDSCRIPTDIR>*:
   ```
   cd <your_path>/<UPDSCRIPTDIR>
   ```
   b. Use the following command to ensure that the data base user has `write` permission to access the log file output:
   ```
   chmod -R 777 *
   ```
2. On UNIX and Linux systems, use the following command to connect as instance owner:
   ```
   su - INSTANCE_OWNER
   ```
3. As the instance owner, check the connection to the database with the following command:
   ```
   clpplus -nw INSTANCE_OWNER/INSTANCE_OWNER_PASSWORD@FQ_IGI_DB
   ```
   then quit.
4. Configure the `db2_update.sh` or `db2_update.bat` file.
   a. Open the `db2_update` file with a text editor.
   b. Modify the **DB2_HOME** variable according to your installation. This variable is necessary for `clpplus` to work.
   c. Modify the **DB2_SERVER** variable with the value of *FQ_IGI_DB*.
   d. If you changed the default product password from `ideas`, change it accordingly in the `clpplus` commands.
5. Connect as root or Administrator, run the update script, and record the results in the log file.

   On UNIX and Linux:
   ```
   dos2unix db2_update.sh
   ./db2_update.sh > upgrade.log
   ```
   On Windows:
   ```
   db2_update.bat > upgrade.log
   ```

Updating the DB2 server for V5.2.1 manually

To update IBM Security Identity Governance V5.2 to IBM Security Identity Governance and Intelligence Version 5.2.1, you must configure it with these instructions.

Before you begin

- The DB2 Server, Version 10.5.0, Fix Pack 5, must be installed. It is the minimum version level that is required to update to IBM Security Identity Governance and Intelligence Version 5.2.1.
- The DB2 Client must be installed.
- You must know the common database parameters such as the IP address, server port, and SID.

Note: During the migration procedure, under particular conditions, this diagnostic message can be found in the log file.

```
"NO FLOW <something> FOUND".
```

This message does not identify an error in the procedure and can be ignored.

About this task

The following tags are used to customize the IBM Security Identity Governance and Intelligence DB2 database installation.

Table 12. Tags to customize the IBM Security Identity Governance and Intelligence DB2 database installation.

Tags	Description
DBServer	DB2 Server IP address or DNS name.
DBPort	DB2 instance port.
IGI_DB	DB2 database name.
INSTANCE_OWNER	DB2 instance owner of the database instance.
PASSWORD	DB2 instance owner password.
FQ_IGI_DB	*<DBServer>*:*<DBPort>*/*<IGI_DB>*

The scripts for the installation of the DB can be delivered in 4 distinct .zip files, all containing the same set of files and distinguished by the license:

- SEC_IDNTY_GVN_INTL_CMP_V5.2.1_DT_IN_.zip
- SEC_IDNTY_GVN_INTL_ANL_V5.2.1_DT_IN_.zip
- SEC_IDNTY_GVN_INTL_LFC_V5.2.1_DT_IN_.zip
- SEC_IDNTY_GVN_INTL_IEE_V5.2.1_DT_IN_.zip

Depending on the license that you purchased, unpack one of these .zip files into a directory of your choice, *<your_path>*/*<UPDSCRIPTDIR>*, and proceed as indicated in the following steps.

Procedure

1. On UNIX and Linux systems, change the file permissions in the installation directory.
   a. Use the following command to change directory to *<UPDSCRIPTDIR>*:

```
cd <your_path>/<UPDSCRIPTDIR>
```

b. Use the following command to ensure that the data base user has `write` permission to access the log file output:

```
chmod -R 777 *
```

2. On UNIX and Linux systems, use the following command to connect as instance owner:

```
su - INSTANCE_OWNER
```

3. As the instance owner, check the connection to the database with the following command:

```
clpplus -nw INSTANCE_OWNER/INSTANCE_OWNER_PASSWORD@FQ_IGI_DB
```

then quit.

4. Run the update scripts.

a. Change the directory to `AccessGovernanceCoreBackend`.

```
cd <your_path>/<UPDSCRIPTDIR>/AccessGovernanceCoreBackend
```

Run the following commands.

```
clpplus -nw igaadm/ideas@<FQ_IGI_DB> @agc_pre_req_upgrade_73_to_74.sql
clpplus -nw igacore/ideas@<FQ_IGI_DB> @agc_pre_req_upgrade_73_to_74.sql
clpplus -nw ccscore/ideas@<FQ_IGI_DB> @arc4s_pre_req_upgrade_73_to_74.sql
```

b. Change the directory to `Localization`.

```
cd ../Localization
```

Run the following commands.

```
clpplus -nw igaadm/ideas@<FQ_IGI_DB> @agc_localization.sql
clpplus -nw igacore/ideas@<FQ_IGI_DB> @agc_localization.sql
clpplus -nw ccscore/ideas@<FQ_IGI_DB> @arc4s_localization.sql
```

c. Change the directory to `AccessGovernanceCoreBackend`.

```
cd ../AccessGovernanceCoreBackend
```

Run the following commands.

```
clpplus -nw igaadm/ideas@<FQ_IGI_DB> @agc_upgrade_73_to_74.sql
clpplus -nw igacore/ideas@<FQ_IGI_DB> @agc_upgrade_73_to_74.sql
clpplus -nw ccscore/ideas@<FQ_IGI_DB> @arc4s_upgrade_73_to_74.sql
```

d. Change the directory to `AccessRequestsBackend`.

```
cd ../AccessRequestsBackend
```

Run the following commands.

```
clpplus -nw igaadm/ideas@<FQ_IGI_DB> @arm_upgrade_13_to_14.sql
clpplus -nw igacore/ideas@<FQ_IGI_DB> @arm_upgrade_13_to_14.sql
```

e. Change the directory to `AccessOptimizerBackend`.

```
cd ../AccessOptimizerBackend
```

Run the following commands.

```
clpplus -nw aaadm/ideas@<FQ_IGI_DB> @aa_upgrade_53_to_54.sql
clpplus -nw aacore/ideas@<FQ_IGI_DB> @aa_upgrade_53_to_54.sql
```

f. Change the directory to `AccessRiskControlsForSAPBackend`.

```
cd ../AccessRiskControlsForSAPBackend
```

Run the following command.

```
clpplus -nw ccscore/ideas@<FQ_IGI_DB> @arc4s_upgrade_43_to_44.sql
```

g. Change the directory to `DeskBackend`.

```
cd ../DeskBackend
```

Run the following command.

```
clpplus -nw igaserv/ideas@<FQ_IGI_DB> @desk_upgrade_23_to_24.sql
```

h. Change the directory to `EmailBackend`.

```
cd ../EmailBackend
```

Run the following commands.

```
clpplus -nw igaadm/ideas@<FQ_IGI_DB> @es_upgrade_23_to_24.sql
clpplus -nw igacore/ideas@<FQ_IGI_DB> @es_upgrade_23_to_24.sql
```

i. Change the directory to `EnterpriseConnectorsBackend`.

```
cd ../EnterpriseConnectorsBackend
```

Run the following commands.

```
clpplus -nw igaadm/ideas@<FQ_IGI_DB> @ec_upgrade_33_to_34.sql
clpplus -nw igacore/ideas@<FQ_IGI_DB> @ec_upgrade_33_to_34.sql
```

j. Change the directory to `JobBackend`.

```
cd ../JobBackend
```

Run the following commands.

```
clpplus -nw igaadm/ideas@<FQ_IGI_DB> @job_upgrade_23_to_24.sql
clpplus -nw igacore/ideas@<FQ_IGI_DB> @job_upgrade_23_to_24.sql
clpplus -nw ccscore/ideas@<FQ_IGI_DB> @job_upgrade_23_to_24.sql
clpplus -nw aaadm/ideas@<FQ_IGI_DB> @job_upgrade_23_to_24.sql
clpplus -nw aacore/ideas@<FQ_IGI_DB> @job_upgrade_23_to_24.sql
clpplus -nw repadm/ideas@<FQ_IGI_DB> @job_upgrade_23_to_24.sql
clpplus -nw repcore/ideas@<FQ_IGI_DB> @job_upgrade_23_to_24.sql
```

k. Change the directory to `ReportBackend`.

```
cd ../ReportBackend
```

Run the following commands.

```
clpplus -nw repadm/ideas@<FQ_IGI_DB> @rd_upgrade_23_to_24.sql
clpplus -nw repcore/ideas@<FQ_IGI_DB> @rd_upgrade_23_to_24.sql
```

l. Change the directory to `RuleEngineBackend`.

```
cd ../RuleEngineBackend
```

Run the following commands.

```
clpplus -nw igaadm/ideas@<FQ_IGI_DB> @re_upgrade_23_to_24.sql
clpplus -nw igacore/ideas@<FQ_IGI_DB> @re_upgrade_23_to_24.sql
clpplus -nw ccscore/ideas@<FQ_IGI_DB> @re_upgrade_23_to_24.sql
```

m. Change the directory to `TaskPlannerBackend`.

```
cd ../TaskPlannerBackend
```

Run the following commands.

```
clpplus -nw igaqrz/ideas@<FQ_IGI_DB> @quartz_upgrade.sql
clpplus -nw igaserv/ideas@<FQ_IGI_DB> @sk_upgrade_23_to_24.sql
```

n. Change the directory to `AuditHelper`.

```
cd ../AuditHelper
```

Run the following command.

```
clpplus -nw igaserv/ideas@<FQ_IGI_DB> @account_upgrade_33_to_34.sql
```

o. Change the directory to `SIB_IB_ILC`.

```
cd ../SIB_IB_ILC
```

Run the following commands.

```
clpplus -nw itimuser/ideas@<FQ_IGI_DB> IB_ILC_upgrade.sql
clpplus -nw itimuser1000/ideas@<FQ_IGI_DB> SIB_upgrade.sql
```

p. Change the directory to `AccessGovernanceCoreBackend`.

```
cd ../AccessGovernanceCoreBackend
```

Run the following commands.

```
clpplus -nw igaadm/ideas@<FQ_IGI_DB> @report_assignment.sql
clpplus -nw igacore/ideas@<FQ_IGI_DB> @report_assignment.sql
```

q. Change the directory to `ReportBackend`.

```
cd ../ReportBackend
```

Run the following commands.

```
clpplus -nw repadm/ideas@<FQ_IGI_DB> @revoke_from_agc.sql
clpplus -nw repcore/ideas@<FQ_IGI_DB> @revoke_from_agc.sql
```

a. Change the directory to `IdeasModule`.

```
cd ../IdeasModule
```

Run the following commands.

```
clpplus -nw igaadm/ideas@<FQ_IGI_DB> @ideas_module_upgrade.sql
clpplus -nw igacore/ideas@<FQ_IGI_DB> @ideas_module_upgrade.sql
clpplus -nw ccscore/ideas@<FQ_IGI_DB> @ideas_module_upgrade.sql
clpplus -nw aaadm/ideas@<FQ_IGI_DB> @ideas_module_upgrade.sql
clpplus -nw aacore/ideas@<FQ_IGI_DB> @ideas_module_upgrade.sql
clpplus -nw repadm/ideas@<FQ_IGI_DB> @ideas_module_upgrade.sql
clpplus -nw repcore/ideas@<FQ_IGI_DB> @ideas_module_upgrade.sql
```

Synchronizing data

After you close all the campaigns, all schedulers are listed with the **Inconsistent Task** icon. Resynchronize the schedulers in the case of the first installation of IBM Security Identity Governance and Intelligence.

Procedure

1. Log on to the Central Administration. If you are logging on to Central Administration for the first time, use these default credentials.
   - User name: `admin`
   - Password: `admin`
2. Click the **Task Planner** icon.
3. Select **Settings** > **Scheduler**.
4. Select an item from the Scheduler frame.
5. In the same frame, from the **Actions** menu, click **Actions** > **Synchr**.
6. Repeat steps 4 and 5 for each scheduler that is listed.

Loading role mining data

The role mining starts without data to analyze. For this reason, do a new data load.

About this task

The **Access Optimizer** has two parts:

- Role Mining
- Access Summary

Two procedures for data uploads are available for the **Access Optimizer**.

Procedure

1. Log on as administrator to the **Access Optimizer**.
2. Select **Tools** > **Bulk Data Load**.
3. In the **Bulk Data Load** tab, select **Actions** > **Add** to start the data load.

Building hierarchies

Run **SystemHierarchyAttributeRefresh** to automatically build of the hierarchies.

Procedure

1. Log on as administrator to the **Task Planner**.
2. Select **Manage** > **Tasks**.
3. In the left frame **Task**, select **SystenHierarchyAttributeRefresh**.
4. Select **Actions** > **Start**.

Results

The task builds the hierarchies according to the configured schedule.

Chapter 5. Installing and configuring Identity Brokerage Adapters

Identity Brokerage is the gateway to directly integrate Identity Governance and Intelligence with targets and hubs using IBM Security Identity Manager Adapters. These IBM Security Identity Manager Adapters are called Identity Brokerage Adapters in Identity Governance and Intelligence.

The Identity Brokerage uses an internal Security Directory Integrator to include the following embedded Identity Brokerage Adapters:

- AIX®
- HP
- LDAP
- Linux
- Solaris

To install additional adapters or update the embedded adapters, the Administrator must install the adapters externally. Depending on the adapter, an external Security Directory Integrator may be required. See the Adapters *Installation and Configuration Guide* for the installation procedure.

Note:

- The Adapters *Installation and Configuration Guide* content reference IBM Security Identity Manager but it is valid for Identity Governance and Intelligence.
- The following sections in the Adapters *Installation and Configuration Guide* do not apply to Identity Governance and Intelligence. See the corresponding Identity Governance and Intelligence topics instead.

Table 13. Installation and Configuration topics

Adapters *Installation and Configuration Guide***topics**	**See the following Identity Governance and Intelligence topics instead**
Importing the adapter profile	Importing target types (adapter profiles)
Creating a service	Creating targets
Configuring the SSL connection	Configuring the SSL connection for Identity Brokerage Adapters

See Supported Identity Adapters for the list of supported adapters and their corresponding *Installation and Configuration Guide*.

Installation roadmap

Before you can use the Identity Brokerage Adapters, you must complete the following tasks.

For Security Directory Integrator based adapters

1. “Installing the dispatcher” on page 54
2. Importing target types (adapter profiles)
3. “Installing the adapter binary” on page 54

For adapters that do not require Security Directory Integrator

1. Importing target types (adapter profiles)
2. "Installing the adapter binary"

Note: For information about prerequisites and other installation and configuration tasks specific to the Identity Brokerage Adapter that you want to use, see the corresponding *Installation and Configuration Guide*.

Installing the dispatcher

Note: If you already have a previous installation of the dispatcher, do not re-install it unless there is an upgrade to the dispatcher.

All Security Directory Integrator based adapters require the dispatcher so that these adapters can function correctly.

1. Obtain the Dispatcher installer from the IBM Passport Advantage website.
2. Install the dispatcher on the same Security Directory Integrator Server where you want to install the adapter. For the detailed instructions, see the *IBM Security Identity Manager Dispatcher Installation and Configuration Guide*.
3. Verify whether the dispatcher components are placed in the correct directories on the Security Directory Integrator Server.

Installing the adapter binary

Some Security Directory Integrator based adapters only have an adapter profile and do not include binaries. As such, they do not require Security Directory Integrator configuration. Those adapters can just use the internal Security Directory Integrator.

For all other adapters, see their corresponding *Installation and Configuration Guide* at Supported Identity Adapters.

Chapter 6. Administration of the virtual appliance

The virtual appliance administrator is responsible for the setup and activation of the Identity Governance and Intelligence virtual appliance and for its day-to-day administration.

For more information about the tasks that virtual appliance administrators can do, see Personas and use cases.

Appliance Dashboard

The Appliance Dashboard provides important status information, statistics, and appliance management tools.

Use the following information to log in to the **Appliance Dashboard**:

Login URL

```
https://hostname:9443
```

Default login user name

```
admin
```

Default login password

```
admin
```

Viewing the notifications widget

View warning information about potential problems and required actions with the **Notifications** dashboard widget.

About this task

The **Notifications** widget refreshes automatically after every 2 minutes to display the most recent state or condition of the virtual appliance.

Note: Before you make any other configuration changes, you must act on any current notifications to clear them out.

Procedure

1. From the **Appliance Dashboard**, locate the **Notifications** widget. Warning messages about potential problems and expected actions are displayed as follows.

   ```
   Appliance restart required
   Middleware components not configured
   The disk space utilization has exceeded the warning threshold.
   ```

2. Take the appropriate actions. For example

   If the following warning message is displayed, restart the identity service by using the option in the **Server Control** widget.

   ```
   Appliance server restart required
   ```

   If a message for restarting the **Appliance Dashboard** is displayed, restart the virtual machine from the `vSphere` console. This condition occurs only if you did not restart after your first configuration.

3. Optional: Click **Refresh** to display the most recent state or condition of the virtual appliance.

Viewing the middleware and server monitor widget

The health status of a middleware server is determined by the state of the middleware and services. You can view the health status information with the **Middleware and Server Monitor** dashboard widget.

Procedure

1. From the **Appliance Dashboard**, locate the **Middleware and Server Monitor** widget.

   The widget displays the installed middleware. For example, `Identity data store`.

   The **Middleware status** displays the status of a middleware server as follows:

   Started
   Indicates that the middleware started.

   Stopped
   Indicates that the middleware stopped.

   Not configured
   Indicates that the middleware is not configured.

   For example:

`Identity data store`	`Started`

2. Optional: Click **Refresh** to display the updated data.

Viewing partition information

The **Partition Information** widget displays information about the active and backup partitions on the virtual appliance firmware.

Procedure

1. From the **Appliance Dashboard**, locate the **Partition Information** widget to display details about the active and backup partitions, such as **Partition 1 (Active)** and **Partition 2**.

   Firmware version
   Displays the version. For example, `IBM Security Identity Governance and Intelligence 5.2`.

   Installation date
   Displays the installation date. For example, `Sep 28, 2015 8:15:51 PM`.

   Installation type
   Displays the type of installation. For example, `ISO`.

   Last boot
   Displays the time when the virtual appliance was last started. For example, `Sep 28, 2015 8:19:40 PM`.

2. Click **Firmware Settings** to modify settings of the firmware. See Managing the firmware settings.

Viewing disk usage

You can view the disk space status and remaining disk life with the **Disk Usage** widget on the **Appliance Dashboard**.

Procedure

1. From the **Appliance Dashboard**, locate the **Disk Usage** widget. A pie chart displays the disk usage statistics.

   Disk Space Pie Chart
   Displays disk usage information.

   Used Space
   Displays the number of GB of disk space that is used.

   Note: Most of the disk space is typically used by log files and trace files. To minimize the disk footprint, set the virtual appliance to store log and trace files on a remote server. You can also clear unused log and trace files on a periodic basis.

   Free Space
   Displays how many GB of disk space is available.

   Total Space
   How much space in total (in GB) is available to the virtual appliance.

   Note: The disk space in a hardware appliance is limited by the capacity of the hard disk drive it holds.
2. Optional: Click **Refresh** to display updated data.

Viewing IP addresses

You can view a categorized list of IP addresses that the virtual appliance is listening on with the **Interfaces** dashboard widget.

Procedure

1. From the **Appliance Dashboard**, locate the **Interfaces** widget. The **Interfaces** widget displays a categorized list of IP addresses in a table with the following columns:
   - **Type**
   - **Name**
   - **Address**
2. Optional: Click **Refresh** to display the recently updated data

Viewing the server control widget

You can view the status and start or stop the IBM Security Identity Governance and Intelligence services by using the **Server Control** widget.

Procedure

1. On the **Appliance Dashboard**, locate the **Server Control** widget. The **Server name** column displays a server list. For example, Identity Governance and Intelligence server.
2. Select a server from the list.
3. Do one of the following actions:

Start Click **Start** to start the selected server.

Stop Click **Stop** to stop the selected server.

Restart
Click **Restart** to restart the selected server.

The **Server status** column displays the status of each server as follows:

Started
Indicates that the server is started.

Stopped
Indicates that the server is stopped.

4. Optional: Click **Refresh** to display the recently updated data.

Viewing the cluster status

You can view a list of all the nodes in the cluster on the **Cluster Status** widget of the **Appliance Dashboard**.

About this task

You can view the **Cluster Status** widget only on a cluster node.

The **Cluster Status** widget is displayed only when you are in a cluster setup. In a stand-alone environment, the widget is not displayed.

Procedure

1. On the **Appliance Dashboard**, locate the **Cluster Status** widget.

   If the **Cluster Status** widget is not displayed on the **Appliance Dashboard**, select **Dashboard** > **Cluster Status** and click **Save**.

   The **Cluster Status** widget displays the following table columns:

   Host Name
   Displays the host name of a node in the cluster. Click the host name of a node to open the **Appliance Dashboard** in a separate web browser. A node with no link indicates that it is the same node that you are working from.

   Role Displays the role of the node in the cluster.

   `Primary`
   Indicates that the node is the primary node in the cluster.

   `Member` Indicates that the node is a member node in the cluster.

   Status Displays the status of the node in the cluster.

   `Available`
   It indicates that the node is available for your business requirement.

   `Not Available`
   It indicates that the node is not available for your business requirement.

   Note: If the status of a node is displayed as `Not Available`, you can still click the host name link to start the **Appliance Dashboard**.

Undetermined

It indicates that the status of the node cannot be determined.

Synchronization State

Displays the synchronization state of the node in the cluster. For more information, see the following table.

Table 14. Synchronization states table.

State	Description	Action
Not Connected	Displays when a member node cannot connect to a primary node or when a primary node cannot connect to the member node.	Connect the member node with the primary node. For a node with the Not Connected status, click **Reconnect Node** to connect that node into the cluster. See "Reconnecting a node into the cluster" on page 30.
Not Synchronized	Displays when the member node is not synchronized with the primary node.	Synchronize the Member node with the primary node. See "Synchronizing a member node with a primary node" on page 31.
Synchronized	Displays when the member node is synchronized with the primary node.	No action is required.
Synchronizing	Displays when the member node is synchronizing with the primary node.	Wait until the synchronization is complete. Click the **Refresh** icon to get the most recent status.
Not Applicable	Displays if the cluster node is a primary node because the primary node does not require any synchronization.	No action is required.
Error	Displays when the action fails to retrieve synchronization details for the node.	Check log files for more information.

2. Optional: Click the **Refresh** icon to display the updated data again.

Validating configuration with quick links

A virtual appliance administrator can view links for accessing the administration console application to validate the success of the IBM Security Identity Governance and Intelligence configuration.

About this task

You can view the **Quick Links** widget only on a stand-alone node.

Procedure

1. From the **Appliance Dashboard**, locate the **Quick Links** widget. You can view the following administrative console links:
   - **Identity Governance and Intelligence Administration Console**

- **Identity Governance and Intelligence Service Center**

2. Click the **Identity Governance and Intelligence Administration Console** link to open and log on to administrative console.

Virtual appliance administration

With the Appliance Dashboard, you can manage the virtual appliance configuration for the data store, directory server, and mail server. You can also customize the server properties and manage logs.

To manage the virtual appliance, log on to the **Appliance Dashboard** at `https://`*`isigva_hostname`*`:9443`. For example: `https://isigva1.jk.example.com:9443`.

Viewing the event logs

System events are logged when the system settings are changed and when problems occur with the system. Use the Event Log management page to view and to export system events on your network.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Monitor** > **Logs** > **Event Log**. The Event Log page displays system events in the **System Events** tab.
2. From the **System Events** tab, do one of the following actions.
   - Click **Pause Live Streaming** to stop the live updating of the event log.
   - Click **Start Live Streaming** to resume live updating of the event log.
   - Filter the system events with the following steps:
     a. Click the **Define filter** icon to display the Filter window.
     b. From the **Match** menu, choose whether the event must match all or can match any of the filter rules.
     c. From the **Column** list, select a column name to filter on it. The column names are as follows:
        - **Any Column**
        - **Priority**
        - **Event ID**
        - **Event Description**
        - **Time Occurred**

        Note: The virtual appliance does not return results for the **Time Occurred** column when you select **Any Column**. Select the **Time Occurred** column to filter values in that column.
     d. From the **Condition** list, select a filter condition. Available filter conditions vary depending on the tab that you selected in the Event log. The possible filtering conditions include these options:
        - **contains**
        - **is**
        - **starts with**
        - **ends with**
        - **before**
        - **after**

- **range**

  Note: You can also add a rule for filtering the system events.

  e. In the **Value** field, specify a filter value.

  f. Click **Filter**.

  g. Click **Clear** to clear all the filter changes.

- Click **Export** to download the displayed event log data to a CSV file.

  Note: The default file name is `export.csv`.

  a. In the exported event log file, the **Time Occurred** column shows the time since Epoch (1 January 1970, 00:00:00 Universal time).

  b. When you use the table filter on the **Priority** field, the values that can be filtered are in English only (`low`, `medium`, and `high`) on all language versions of the virtual appliance.

Viewing the memory usage

View the memory graph to see the memory that is used by the IBM Security Identity Governance and Intelligence virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Monitor** > **Monitoring** > **Memory**. The System Memory Statistics page is displayed.
2. Select a **Date Range**.

Option	Description
1 Day	Displays data points for every minute during the last 24 hours.
3 Days	Displays data points for every 5 minutes during the last three days. Each data point is an average of the activity that occurred in that hour.
7 Days	Displays data points every 20 minutes during the last seven days. Each data point is an average of the activity that occurred in that hour.
30 Days	Displays data points for every hour during the last 30 days. Each data point is an average of the activity that occurred in that hour.

3. In the Legend area, select **Memory Used** to review the total used memory. The **Details** section displays these statistics:

   Total Indicates the total system memory.

   Used Indicates the system memory that is used.

   Free Indicates the system memory that is available.

   As of Indicates the current date, time, and the UTC identifier.

Viewing the CPU usage

View the CPU graph to see the CPU that is used by the IBM Security Identity Governance and Intelligence virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Monitor** > **Monitoring** > **CPU**. The System CPU Statistics page is displayed.
2. Select a **Date Range**.

Option	Description
1 Day	Displays data points for every minute during the last 24 hours.
3 Days	Displays data points for every 5 minutes during the last three days. Each data point is an average of the activity that occurred in that hour.
7 Days	Displays data points every 20 minutes during the last seven days. Each data point is an average of the activity that occurred in that hour.
30 Days	Displays data points for every hour during the last 30 days. Each data point is an average of the activity that occurred in that hour.

3. In the Legend area, select the following options to review the CPU data.

User CPU
Indicates the CPU use by the user.

System CPU
Indicates the CPU use by the system.

Idle CPU
Indicates the idle use of the CPU.

As of Indicates the current date, time, and the UTC identifier.

Viewing the storage usage

View the storage graph to see the percentage of disk space that is used by the boot and root partitions of the IBM Security Identity Governance and Intelligence virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Monitor** > **Monitoring** > **Storage**. The Storage Statistics page is displayed.
2. Select a **Date Range**.

Option	Description
1 Day	Displays data points for every minute during the last 24 hours.
3 Days	Displays data points for every 5 minutes during the last three days. Each data point is an average of the activity that occurred in that hour.
7 Days	Displays data points every 20 minutes during the last seven days. Each data point is an average of the activity that occurred in that hour.

Option	Description
30 Days	Displays data points for every hour during the last 30 days. Each data point is an average of the activity that occurred in that hour.

3. In the Legend area, select which partitions that you want to review.

   Root Indicates the base file system, where the system user is root.

   Boot Indicates the boot partition.

Managing the SNMP monitoring

You can monitor the current IBM Security Identity Governance and Intelligence virtual appliance status with SNMP. This status shows an SNMP agent, which can be queried by any SNMP manager or monitoring tools that support SNMP to obtain the status of the running virtual appliance.

About this task

When configured, the SNMP agent listens on all management interfaces.

The SNMP Monitoring function can monitor the virtual appliance in an IBM Tivoli® Monitoring environment. Use the Agentless Monitoring for Linux OS agent. For more information about configuring the IBM Tivoli Monitoring environment and the Agentless Monitoring for Linux OS agent, see the IBM Knowledge Center.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Monitor** > **Monitoring** > **SNMP Monitoring**.
2. On the SNMP Monitoring page, click **SNMP Monitoring**.
3. Click **Reconfigure**.
4. In the Configure SNMP window, select one of these SNMP protocols.

   SNMPv1/SNMPv2c
   In the **Community** field, type the name of the community that the SNMP manager uses to authenticate with the SNMP agent.

   SNMPv3
   Configure the following options to describe the user that accesses the SNMP agent.

Option	Description
Security Level	The security level of the user.
Security User	Type the name of the user that accesses the SNMP agent.
Auth Protocol	From the **Auth Protocol** list, select the authentication protocol to use.
Auth Password	Type the password to use for authentication. The password must be minimum 8 characters in length.
Auth Password (Confirm)	Retype the authentication password to confirm.

Option	Description
Privacy Protocol	From the **Privacy Protocol** list, select the privacy protocol to use.
Privacy Password	Type the password to be used as a privacy passphrase. The password must be a minimum of 8 characters in length.
Privacy Password (Confirm)	Retype the privacy password to confirm.

5. In the **Port** field, type the number that the SNMP agent must listen on. Alternatively, you can also change the port number with the range controller next to it.

   Note: The default port number is 161.
6. Click **Save Configuration**. The **Enabled** field is set to `True`.
7. Optional: To disable SNMP Monitoring, do these steps:
   a. On the SNMP Monitoring page, click **SNMP Monitoring**.
   b. Click **Reconfigure**.
   c. In the Configure SNMP window, select **Disable**. The **Enabled** field is set to `False`.

Enabling Identity Brokerage Providers in the virtual appliance

You can use the IBM Identity Brokerage Providers in the IBM Security Identity Governance and Intelligence virtual appliance to communicate with managed resources.

Before you begin

By default, IBM Identity Brokerage Providers is not configured in the Identity Governance and Intelligence virtual appliance. If you want to use the Identity Brokerage Providers and did not enable the component during installation, you must complete this task.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **Maintenance** > **Identity Brokerage Providers**. The Identity Brokerage Providers page is displayed.
2. Click the **Use Identity Brokerage Providers** check box.
3. Click **Enable**.
4. For clustered deployments, synchronize the member nodes.
5. Restart the server.

Managing directory server configuration

Use the Directory Server Configuration page to configure the directory server in the IBM Security Identity Governance and Intelligence virtual appliance.

Before you begin

Install and configure the directory server. Make sure that you create the directory server DN location. See https://www-01.ibm.com/support/knowledgecenter/SSRMWJ_7.0.0/com.ibm.isim.doc_7.0/installing/tsk/tsk_ic_ins_dir_itds_config_manual.htm

About this task

Note: You need not configure the directory server if you do not want to enable Identity Brokerage Providers.

Configure or reconfigure the directory server options. See Table 15.

Table 15. Directory server configuration details.

Function	Directory server options
Configure	**Host name** Specify the name of the server that hosts the directory server. The acceptable formats for the host name are IPv4, FQDN, and IPv6. For example, `igildap.example.com`. **Port** Specify the directory server port. For example, `389`. **Principal DN** Specify the principal distinguished name. For example, `cn=root`. **Password** Specify the password for the directory server. **Organization name** Specify the name of the enterprise or the organization. For example, `JK Enterprises`. **Default organization short name** Specify the abbreviation or short form of the organization name. For example, `jke`. **DN Location** Specify the directory server DN location. For example, `dc=com`.

Table 15. Directory server configuration details (continued).

Function	Directory server options
Reconfigure	**Host name** Specify the name of the server that hosts the directory server. The acceptable formats for the host name are IPv4, FQDN, and IPv6. For example, `igildap.example.com`. **Port** Specify the directory server port. For example, `389`. **Principal DN** Specify the principal distinguished name. For example, `cn=root`. **Password** Specify the password for the directory server.

Note: If a directory server was configured during the virtual appliance setup, you can reconfigure or unconfigure the directory server only. The configure function is disabled.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Manage External Entities** > **Directory Server Configuration**.
2. Click **Configure**.
3. In the Directory Server configuration details window, specify the expected variables. For more information, see Table 15 on page 65.
4. Click **Save Configuration**.

   Note: The directory server configuration takes time. Do not refresh or close the page until the configuration process is complete.
5. Optional: Reconfigure an existing directory server configuration.
   a. Create a snapshot to recover from any configuration failures. See "Managing the snapshots" on page 93.
   b. From the Directory Server Configuration table, select the directory server configuration record, `Identity User Registry`.
   c. Click **Reconfigure**.
   d. In the Edit directory server configuration details window, edit the configuration variables. For more information, see Table 15 on page 65.
   e. Click **Save Configuration**.

      Note: The directory server reconfiguration takes some time. Do not refresh or close the page until the reconfiguration process is complete.
6. Optional: Unconfigure an existing directory server configuration.
   a. From the Directory Server Configuration table, select the directory server configuration record, `Identity User Registry`.
   b. Click **Unconfigure**.

c. Click **Yes** to confirm the deletion.

What to do next

After you use the Directory Server Configuration page on the IBM Security Identity Governance and Intelligence virtual appliance to configure the directory server, you must configure the database server. If you already configured the database server, you must reconfigure it.

Managing the database server configuration

Use the Database Server Configuration page to configure, reconfigure, or unconfigure the database server for the IBM Security Identity Governance and Intelligence virtual appliance.

About this task

Configure or reconfigure the Identity data store options for the database server. See Table 16 on page 68.

Table 16. Identity data store configuration

Button	Data store options
Configure	**Database type** Select the database type from the list. To configure the database server, select one of these options. - **IBM DB2** - **Oracle (Standard)** - **Oracle (Custom)** **Host name (FQDN, IPv4, or IPv6)** Specify the name of the server that hosts the data store. For example: `igidstore.example.com`. **JDBC URL** Specify the JDBC URL to connect with the database. For example: `jdbc:oracle:thin:@//<hostname>:<port>:<dbName>`. **Note:** Specify the JDBC URL for **Oracle (Custom)**. **Port** Specify the data store service port. For example: `50000`. **Database name** Specify the name of the IBM Security Identity Governance and Intelligence database. Example: `igidb`. **Database User Password** Specify the password for the Identity data store user ID. **Note:** All the database users must have the same password. If the password does not match for all the database users, a message indicates that the password is not correct for that user. If you select **Oracle (Standard)** or **Oracle (Custom)**, configure these options. **Oracle SID or Service name** Specify the Oracle System ID (SID) or the service name to identify the database. For example, `isimdb`. Select or clear the **Service name** check box to manage the following aspects: - If you select the check box, the value is treated as service name. - If you do not select the check box, the value is treated as SID. **Note:** When you select **Oracle (Custom)** as the database type, you cannot configure these options: - **Port** - **Database name** - **Oracle SID or service name**

Table 16. Identity data store configuration (continued)

Button	Data store options
Reconfigure	**Note:** Reconfiguration does not update the database schema. It configures only the IBM Security Identity Governance and Intelligence with new database details. **Host name (FQDN, IPv4, or IPv6)** Specify the name of the server that hosts the data store. For example: `igidstore1.example.com`. **JDBC URL** Specify the JDBC URL to connect with the database. For example: `jdbc:oracle:thin:@//<hostname>:<port>:<dbName>`. **Note:** Specify the JDBC URL for **Oracle (Custom)**. **Port** Specify the data store service port. For example: `51000`. **Database name** Specify the name of the IBM Security Identity Governance and Intelligence database. Example: `igidb`. **Database User Password** Specify the password for the Identity data store user ID. **Note:** All the database users must have the same password. If the password does not match for all the database users, a message indicates that the password is not correct for that user. If you select **Oracle (Standard)** or **Oracle (Custom)**, configure these options. **Oracle SID or Service name** Specify the Oracle System ID (SID) or the service name to identify the database. For example, `igidb`. Select or clear the **Service name** check box to manage the following aspects: • If you select the check box, the value is treated as service name. • If you do not select the check box, the value is treated as SID.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Manage External Entities** > **Database Server Configuration**. The Database Server Configuration page displays the Database Server Configuration table.
2. Click **Configure**.
3. In the Database Server Configuration Details window, specify the expected variable values. For more information, see Table 16 on page 68.
4. Click **Save Configuration** to complete this task.
5. Optional: To reconfigure an existing database server configuration, do these steps:
   a. Before you reconfigure, create a snapshot to recover from any configuration failures. See "Managing the snapshots" on page 93.
   b. From the Database Server Configuration table, select the database configuration record, `Identity data store`.
   c. Click **Reconfigure**.
   d. In the Edit Identity data store details window, edit the details. For more information, see Table 16 on page 68.
   e. Click **Save Configuration**.

Note: The database server reconfiguration takes some time. Do not refresh or close the page. Wait for the reconfiguration process to complete.

6. Optional: To unconfigure an existing identity store, do these steps:
   a. From the Database Server Configuration table, select the database configuration record, `Identity data store`.
   b. Click **Unconfigure**.
   c. Click **Yes** to confirm the deletion.

Managing OpenID connect configuration

You can use OpenID connect to access the Service Center. The OpenID connect provider must be able to authenticate the user and provide claims to a relying party about the authentication event and the user.

Before you begin

IBM Security Identity Governance and Intelligence support OpenID connect providers that meet the following requirements:

- The provider is fully OIDC-compliant.
- The user registry is managed by IBM Security Identity Governance and Intelligence.
- The relying party, IBM Security Identity Governance and Intelligence, is reachable from the provider.

Ensure that you configured an OpenID connect provider such as IBM Security Access Manager. You need the following information to perform OpenID operations.

Table 17. Necessary information for configuration

Configuration type	Information	Definition
All configurations	Provider name	The service that provides your OpenID.
	Signature algorithm	The algorithm that is used to sign the ID token that is issued by a provider. The default value is HS256.
	User ID to create subject	Sets the attribute to a claim name that is used by the vendor′s ID token that represents a user's unique identifier.
	Client ID	A publicly exposed string that is used by the service API to identify the application. It is also used to build authorization.
	Client secret	Secret is used to authenticate the identity of the application to the service API when the application requests to access a user account. It must be kept private between the application and the API.
	Domain	The domain that uses the OpenID connect as the authentication mechanism.

Table 17. Necessary information for configuration (continued)

Configuration type	Information	Definition
Manual configuration	Authorization URL	The initial endpoint that is contacted by the relying party to begin a flow.
	Token URL	The endpoint that is used to exchange an authorization code for a token.
	JWK URL	The JSON web key endpoint that is used for signature verification.
	Scope	The scopes that are associated with access tokens determine what resources are available when they are used to access OpenID connect protected endpoints. The following example is a non-normative example of scope. `scope=openid profile email phone`
	Issuer identifier	The verifiable identifier for an issuer. An issuer identifier is a case-sensitive URL that uses the HTTP scheme. It contains scheme, host, and optionally, port number and path components. It cannot contain query or fragment components.
Discovery configuration	Discovery URL	Perform discovery to locate the endpoints, scope, and signature algorithm.

About this task

You can configure one or more than one OpenID providers. However, only one provider can be used to access the Service Center at any one time.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **Manage External Entities** > **OpenID connect Configuration**. The OpenID connect Configuration page is displayed.
2. Click the tab for the operation that you want to perform.

Table 18. OpenID connect operations

Operation	Steps
Use **New** to configure an OpenId provider.	1. Click **New**. 2. Provide the information based on the type of configuration that you want to perform, either **Discovery configuration** or **Manual configuration**. 3. Click the **Service Center** check box. 4. Click **Save Configuration**.

Table 18. OpenID connect operations (continued)

Operation	Steps
Use **Edit** to change the provider information.	1. Select the provider for which you want to change the information. 2. Click **Edit**. 3. Change the information in the available fields. 4. Click **Save Configuration**.
Use Delete to remove an OpenID provider configuration.	1. Select the provider configuration that you want to remove. 2. Click **Delete**. 3. Click **Yes** on the confirmation message.
Refresh	Updates the values in the grid.

Note: You must register a redirect URI at the OpenID provider. After a successful authentication at the OpenID provider, the client is redirected to this URL. It has a specific format.

```
https://hostname:9343/oidcclient/redirect/{Provider-Name}
```

Where

- *hostname* is either the application interface IP or the application interface host name where IBM Identity Governance and Intelligence product is running.
- *Provider-Name* is the attribute value provider name that you are going to add at the time of registering OpenID connect configuration in the virtual appliance.

The OpenID provider certificate must be added to the virtual appliance truststore. You can do this task from the virtual appliance certificate page and adding the certificate to the signers. See Managing certificates.

The following example is for setting up OpenID Connect Federation between IBM Security Access Manager Version 9 and the Identity Governance and Intelligence virtual appliance.

a. Set up a federation in IBM Security Access Manager.

   Follow the directions at https://www.ibm.com/support/knowledgecenter/SSPREK_9.0.0/com.ibm.isam.doc/config/task/tsk_config_op_federation.html?lang=en

b. Create and register the client.

   Follow the instructions at https://www.ibm.com/support/knowledgecenter/SSPREK_9.0.0/com.ibm.isam.doc/config/task/tsk_config_op_partner.html?lang=en. The redirect URI is the Identity Governance and Intelligence application. The format is

   ```
   https://igiapplication:9343/oidcclient/redirect/provider-name
   ```

   Make sure that the provider name is the name of the OpenID Connect provider that you register in OpenID Connect Provider Configuration Panel in Identity Governance and Intelligence virtual appliance.

c. Configure IBM Security Access Manager as an OpenID Connect provider. See https://www.ibm.com/support/knowledgecenter/SSPREK_9.0.0/com.ibm.isam.doc/config/concept/con_oidc_auto_config_script.html?lang=en.

d. Go to https://www.ibm.com/support/knowledgecenter/SSPREK_9.0.0/com.ibm.isam.doc/config/task/ConfiguringSAML2POC.html and perform steps 3, 5, and 6.

e. Form the OpenID Connect endpoints. See https://www.ibm.com/support/knowledgecenter/SSPREK_9.0.0/com.ibm.isam.doc/config/concept/con_oidc_endpoints.html?lang=en .

f. Ensure that the IBM Security Identity Governance and Intelligence user registry is synchronized with IBM Security Access Manager.

g. Register the OpenID Connect provider in the IBM Security Identity Governance and Intelligence virtual appliance. Use the client ID, secret, and endpoints that were formed at IBM Security Access Manager. Make sure that the provider name is they same as the provider name in your redirect URL.

h. Add the IBM Security Access Manager reverse proxy certificate in the application truststore. See "Managing certificates" on page 77.

i. Restart the IBM Security Identity Governance and Intelligence server from the dashboard

Managing the mail server configuration

Use the Mail Server Configuration page to configure the email notifications for the IBM Security Identity Governance and Intelligence virtual appliance.

About this task

Configure, reconfigure, or unconfigure the mail server options. See Table 19.

Table 19. Mail Server Configuration

Button	Mail Server options
Configure	**Mail server (FQDN, IPv4, or IPv6)** Specify a server name that hosts the mail server. For example, `mailserver.com`. **Port** Specify a valid service port of the mail server. By default, the port number is `25`. **Mail from** Specify an email address from which the email is sent. For example, `admin@in.ibm.com`.
Reconfigure	**Mail server (FQDN, IPv4, or IPv6)** Change the name of the server that hosts the mail server if necessary. **Port** Change the service port of the mail server if necessary. **Mail from** Change the address from which the email is sent if necessary.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Configure** > **Manage Server Setting** > **Mail Server Configuration**. The Mail Server Configuration page displays the Mail Server Configuration table.
2. Configure a new mail server or reconfigure an existing one.
   - Configure a new server.
     a. Click **Configure**.
     b. In the Mail Server Configuration Details window, specify the expected variable values. For more information, see Table 19 on page 74.
     c. Click **Save Configuration**. A message indicates that the mail server configuration is successfully configured.
   - Reconfigure an existing server.
     a. From the Mail Server Configuration table, select a record. For example, `Mail Configuration`.
     b. Click **Reconfigure**.
     c. In the Edit Mail Configuration Details window, edit the details. For more information, see Table 19 on page 74.
     d. Click **Save Configuration**. A message indicates that the mail server configuration is successfully reconfigured.
3. Optional: To unconfigure an existing mail server, do these steps:
   a. From the Mail Server Configuration table, select a record. For example, `Mail Configuration`.
   b. Click **Unconfigure**.
   c. Click **Yes** to confirm the deletion. A message indicates that the mail server configuration is successfully unconfigured.

Managing custom files

View custom files and folders that are related to the IBM Security Identity Governance and Intelligence virtual appliance.

About this task

Manage your files from the Custom File Management page in these ways:

- Expand or collapse the directory structure to view the different files and folders, including the recently updated files.
- Download or upload any type of file.
- Create a folder for your requirements.
- Restore a selected file to the default state.

Upload all the external libraries with the Custom File Management page. You must upload the libraries into the `lib` folder. To upload a library, see Table 20 on page 76.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Configure** > **Manage Server Setting** > **Custom File Management**.
2. In the Custom File Management page, take one of these actions. See Table 20 on page 76.

Table 20. File tabs and their actions

Tab	Tab Description	Actions
All Files	Displays a directory structure in the left pane. The right pane displays a list of files in a table that is based on the folder that you selected in the left pane. You can take the following actions: • **Download** • **Upload** • **New Folder** • **Refresh** You can use the search box to find a specific property name that you want to update. Type a name or a character string for the properties file to narrow your search. Your search is in the context of the properties file that you selected. All property names that contain the string are displayed. To return to the full list of property names, clear the search box.	Download a file. 1. Select a folder in the left pane to display a list of files in the right pane. 2. Select a file. 3. Click **Download**.
		Upload a file. 1. Select a folder in the left pane. 2. Click **Upload** to open the File Upload window. 3. Click **Browse** to search and select the file. 4. Click **Save Configuration**.
		Create a folder. 1. In the left pane, select a subfolder in which you want to create another folder. **Note:** You cannot create folders under the top-level folder. **New Folder** is not enabled when you select the top level-folder. For example, `directories`. 2. Click **New Folder**. 3. In **Folder Name**, type a name. • You must use English characters for a folder name. • A folder name must be only alphanumeric. It can contain a space or an underscore. For example, `igi property`, `igi_property1` or similar patterns. You cannot name a folder with a name like `igi$property`, `igi^$^#@property`, or similar patterns. 4. Click **Save Configuration**.
		Display the most recent version of the data, including changes since the last refresh. Click **Refresh**.
		Delete a folder. 1. Select a folder in the left pane. 2. Click **Delete Folder**. 3. Click **Yes** to confirm the action. A message indicates that the selected folder is deleted successfully.

Table 20. File tabs and their actions (continued)

Tab	Tab Description	Actions
Modified Files	Displays all the modified files in a table. You can take the following actions: • **Restore Default** • **Refresh**	Restore a file. 1. Select a file from the table. 2. Click **Restore Default**. **Note:** When you click **Restore Default** for the selected file, it is deleted when it is not included with the product. Otherwise, it is restored to its original included version.
		Display the most recent version of the data, including changes since the last refresh. Click **Refresh**.

3. Optional: Restart the IBM Security Identity Governance and Intelligence server when the **Notifications** widget on the **Appliance Dashboard** indicates to do it.

Managing certificates

Administrators can update the IBM Security Identity Governance and Intelligence application server certificate.

About this task

When the certificates are added to the store, you can use them to securely connect with different endpoints.

Certificates are typically supplied to a particular computer or service. The certificate store is typically managed by virtual appliance administrators.

You can accomplish the following common certificate management tasks:

- Examining properties of certificates.
- Identifying certificates due for renewal.
- Finding certificates.
- Importing certificates.
- Exporting or backing up certificates.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Configure** > **Manage Server Setting** > **Certificates**. The Certificate Stores page displays the certificate database.

   ```
   Identity Certificate Store
   ```

   The Certificate Stores table displays these columns.

   Certificate Database Name
   The display name that is associated with the database.

   Type The type that is associated with the database. For example, JKS.
2. Select **Identity Certificate Store**.
3. Click **Edit**. When you select the database to edit it, the navigation path is displayed on the Certificates page. The navigation path identifies the keystore

that you are currently editing. For example, the path is **Certificate Stores** > **Identity Certificate Store** > **Certificates**.

On the Certificates page, the certificates are specified under these tabs.

- **Personal**
- **Signer**

These tabs display the following certificate columns.

Label The display name that is associated with the certificate.

Subject
The name of the workstation, device, or certificate authority to whom the certificate is supplied.

Issuer Information about the certificate authority that supplied the certificate.

Not Valid Before
The date and time from which the certificate is valid.

Not Valid After
The date and time after which the certificate is no longer valid.

Key Size
The key length that is associated with the certificate.

Version
The X.509 version number.

4. On the Certificates page, do one of the following actions from the toolbar.

Option	Description
Update	**Note:** When you update a certificate in the **Personal** tab, the existing certificate is replaced by the new one. The existing certificate is not available after the update action. Confirm your action before you update the certificate. You can have only a single certificate in the **Personal** tab. In the **Personal** tab, do these steps. 1. Select a certificate record. 2. Click **Update** to display the Upload Certificate window. 3. Click **Browse** to search and select the file that you want to import. The certificate information is displayed in the Files to upload table. 4. In **Label**, specify an ID for the certificate. 5. In **Password**, specify a password. 6. Select a certificate type from the **Type** list. • **PKCS#12** • **JKS** • **JCEKS** • **CMS** 7. Click **Save**.
Upload	In the **Signer** tab, do these steps. 1. Click **Upload** to display the Upload Certificate window. 2. Click **Browse** to search and select the file that you want to import. The certificate information is displayed in the Files to upload table. 3. In **Label**, specify an ID for the certificate. 4. Click **Save**. 5. Restart the server after you import a certificate.

Option	Description
Export	1. Select a certificate record. 2. Click **Export** to back up the certificate. 3. Specify a location where you want to back up the exported certificate.
Refresh	Click **Refresh** to update the list of displayed certificates.
Delete	1. Select a certificate from the certificate store. 2. Click **Delete**.

Viewing the update history

View the update history to see which firmware and security content updates are downloaded, installed, and rolled back on the IBM Security Identity Governance and Intelligence virtual appliance.

About this task

After you install an update, the update package is deleted from the IBM Security Identity Governance and Intelligence virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **Updates and Licensing** > **Update History**. The Update History page is displayed.

   The update history information is displayed in a table with the following columns:

   - **Name**
   - **Action Taken**
   - **Status**
   - **Version**
   - **Release Date**
2. Optional: Click **Refresh** to display the recently updated data.

Viewing the licensing

View the licensing to see the service agreement that you accepted when you installed the virtual appliance. You can also add a license module to manage the licensing.

About this task

A service agreement defines the agreement and formal commitments about the virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **Updates and Licensing** > **Licensing** to display the Licensing page.
2. Click **View Service Agreement** to view the service agreement in the Software License Agreement page.

Managing the firmware settings

The IBM Security Identity Governance and Intelligence virtual appliance has two partitions with separate firmware on each partition. Partitions are swapped during firmware updates so that you can roll back the firmware updates.

About this task

Either partition can be active on the virtual appliance. In the factory-installed state, partition 1 is active and contains the firmware version of the currently released product. When you apply a firmware update, the update is installed on partition 2, and your policies and settings are copied from partition 1 to partition 2. The virtual appliance restarts the system by using partition 2, which is now the active partition.

Note: The virtual appliance comes with identical firmware versions installed on both of the partitions so that you have a backup of the initial firmware configuration.

Tip: Avoid swapping partitions to restore configuration and policy settings. Use snapshots to back up and restore configuration and policy settings.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **Updates and Licensing** > **Firmware Settings**.
2. On the Firmware Settings page, do one or more of the following actions.

Option	Description
Edit	Select the partition and click **Edit** to revise the partition comment.
Create Backup	**Important:** Create a backup of your firmware only when you are installing a fix pack from IBM Customer Support. Fix packs are installed on the active partition, and you might not be able to uninstall the fix pack. **Note:** The backup process can take several minutes to complete.
Set Active	Set a partition to active when you want to use the firmware that is installed on that partition. For example, you might want to set a partition to active to use firmware that does not contain a recently applied update or fix pack.

3. Click **Yes**. If you set a partition to active, the virtual appliance restarts the system from the newly activated partition.

Installing a fix pack

Install a fix pack on the virtual appliance to address software maintenance updates for reliability and performance enhancements.

Before you begin

Restriction: You cannot uninstall a fix pack by using the local management interface. You must use the command-line interface to uninstall a fix pack.

Fix packs are applied to your active partition. You can manually create a backup of your active partition before you apply a fix pack so that you can roll back your changes.

About this task

If a fix pack is installed on your IBM Security Identity Governance and Intelligence virtual appliance, you can view information about who installed the fix pack, comments, patch size, and the installation date.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage System Settings** > **Updates and Licensing** > **Fix Packs**.
2. On the Fix Packs page, click **New**.
3. In the Add Fix Pack window, click **Browse for fix pack**.
4. Select the fix pack file and click **Open**. The Browse for fix pack table displays the fix pack details.
5. Click **Save Configuration** to install the fix pack.

Managing the log configuration

You can view component-specific and virtual appliance log files to troubleshoot virtual appliance issues. You can also configure the file size and settings of the log files in the Log Retrieval and Configuration page.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Manage** > **Maintenance** > **Log Retrieval and Configuration**.
2. On the Log Retrieval and Configuration page, select one of these tabs to view the available logs.
   - **Appliance**
   - **Identity**

   For a set of log retrieval tasks, see “Retrieving logs.”
3. Optional: Click **Configure** to configure the logs. For a set of log configuration tasks, see “Configuring logs” on page 82.

Retrieving logs

Use the Log Retrieval and Configuration page to view, save, or clear the log files. You can also use the page to configure the server log settings for the IBM Security Identity Governance and Intelligence virtual appliance.

About this task

See Table 21 for a list of available logs, which can help you to diagnose or troubleshoot the logs from the Log Retrieval and Configuration page.

Table 21. Available logs to help you diagnose or troubleshoot

Tab	Tab description	Log file name	Description
Appliance	These files help debug any configuration failures that occur in the virtual appliance.	Server System out	It is the Appliance system output log file.
		Server Message	It is the Appliance server message log file.
		Server System trace	It is the Appliance server trace log file.

Table 21. Available logs to help you diagnose or troubleshoot (continued)

Tab	Tab description	Log file name	Description
Identity	Identifies issues in the Identity applications.	IBM Identity Governance and Intelligence Application server messages IBM Identity Governance and Intelligence Application server system trace	It is the Identity application server system output log file.
		Identity Brokerage Application system messages Identity Brokerage Application server system trace Security Directory Integrator server logs IBM Identity Governance and Intelligence trace log	It is the Identity application server system error log file.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Manage** > **Maintenance** > **Log Retrieval and Configuration**.
2. On the Log Retrieval and Configuration page, do one of the following actions.
   - Click **Appliance** to open the **Appliance** tab.
   - Click **Identity** to open the **Identity** tab.
3. From the Log Retrieval and Configuration table of the **Appliance** tab, select a log file. For more information about the **Appliance** and the **Identity** log files, see Table 21 on page 81.
4. Take any of the following actions:
   - Click **View** to display the contents of the selected log file in **Log file** of the Log Content window.
   - Click **Download** to save or download a copy of the log file.
   - Click **Refresh** to display the most recent version of the log files, including changes that were made to the data since it was last refreshed.

     Note: You need not select any file to refresh the data.
   - Click **Clear** and confirm the action to remove the contents from the selected log file.

Configuring logs

Configure different options to manage the quantity and size of the log files and all other log related settings.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Manage** > **Maintenance** > **Log Retrieval and Configuration**. The Log Retrieval and Configuration page consists of two tabs.

- **Appliance**
- **Identity**

To work with these tabs, see “Retrieving logs” on page 81.

2. Click **Configure**. The Logging Configuration window consists of these tabs.

General

This tab contains information about log rollover settings, such as maximum log file rotation size and maximum number of historical log files.

Provide the following details:

Maximum size for log file rotation

The maximum size in megabytes of the log file.

Maximum number of historical log files

The maximum number of historical log files.

To edit the existing log details, specify new values.

Identity

This tab contains information about identity-specific logging details such as logging levels and whether to show SQL in logs.

Provide the following details:

Logging level

Select a logging level from the list.

The logging level is applicable only for IBM Security Identity Governance and Intelligence and Identity Brokerage Providers.

Show SQL in logs

Select an option from the list. The values are as follows.

- **True**
- **False**

The option is applicable only for IBM Security Identity Governance and Intelligence.

Date Format

Specify a format for the date that you want to display in the logs. For example, you can assign the date format as `yyyy.MM.dd`.

You can also use other date formats that you might have in your working environment.

The date format is applicable only for Identity Brokerage Providers.

Time Format

Specify a format for the time that you want to display in the logs. For example, you can assign the time format as `HH:mm:ss.SSS`.

You can also use other time formats that you might have in your working environment.

The time format is applicable only for Identity Brokerage Providers.

To edit an existing logging information, you can take any of the following actions.

- Select another logging level from the list.
- Select another value from the list.
- Change the date format.
- Change the time format.

Application Server
This tab contains information about application server-specific logging properties such as package and their trace levels.

New Do these steps:

a. Click **New** to add a package name.
b. In the **Package Name** column, click to type a package name and assign it to the application server log.
c. In the **Trace Level** column, select a trace level from the list and assign it to the application server log.

Delete Select a record and click **Delete**.

To edit an existing package name, you can take any of the following actions.

- Click a package name.
- Type another package name.
- In **Trace Level**, select another trace level from the list.

SDI This tab contains information about IBM Security Directory Integrator logging properties, such as package and their trace levels.

New Do these steps:

a. Click **New** to add a package name.
b. In the **Package Name** column, select a package name from the list and assign it to the IBM Security Directory Integrator log.
c. In the **Trace Level** column, select a trace level from the list and assign it to the IBM Security Directory Integrator log.

Delete Select a record and click **Delete**.

To edit an existing package name, you can take any of the following actions.

- Click a package name and select another package name from the list.
- In **Trace Level**, select another trace level from the list.

3. Click **Save Configuration**.

Managing the core dump files

Use the Core Dumps page to delete or download core dump files in the IBM Security Identity Governance and Intelligence virtual appliance.

About this task

A core dump file can be generated in the virtual appliance for many reasons. A core dump file stores a large amount of raw data for further examination. Use the core dump files to diagnose or debug errors in the virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, select **Manage** > **Maintenance** > **Core Dumps**.

   The Core Dumps page displays a table with a list of core dump files. The **Category** column in the table indicates the category for which the core dump file is generated. The category list is as follows.

   - Application
   - Application management
   - Others
2. On the Core Dumps page, do one of the following actions.

Table 22. Core dump file management actions

Action	Description
Delete	1. From the **File name** column, select a core dump file. **Note:** To delete multiple core dump files, select more files. To select all the core dump files, select the check box next to **File name**. 2. Click **Delete**. 3. Click **Yes** to confirm.
Download	1. From the **File name** column, select a core dump file. **Note:** You can select only 1 core dump file at a time for download. A message is displayed if you select multiple core dump files. 2. Click **Download**. **Note:** The core dump file is downloaded in an archived format such as `.zip`. **Note:** To view the contents of a core dump file, open the downloaded file.

Viewing the About page information

View the About page to learn more about the IBM Security Identity Governance and Intelligence virtual appliance and its content.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **Maintenance** > **About**.
2. View the product-specific information for the virtual appliance.

Results

The following information is displayed in the About page:

```
Product Name: IBM Security Identity Governance and Intelligence
Product Version:      5.2
Server Name:          igiva.example.com
Installed Fix Packs:  None
Build number:         20151001-0001
Build Date and Time:  Oct 1, 2015 11:24:41 AM
```

Product Name
Displays the name of product that you are using.

Product Version
Displays the version of product that you are using.

Server Name
Displays the server name.

Installed Fix Packs
Displays the last fix pack level that was installed for the version of the product that you are using.

Build number
Displays the current build number for the version of the product that you are using.

Build Date and Time
Displays the date and the exact time and the time zone on which the last build occurred.

What to do next

Read the IBM Security Identity Governance and Intelligence virtual appliance product information to determine how it can be useful in your work.

Managing application interfaces

To manage application interfaces with the management interface, use the Application Interfaces page.

About this task

An IP address and its corresponding fully qualified domain name for any application interface must have a static IP address, which must be different from the local management interface address.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **Network Settings** > **Application Interfaces**. The Application Interfaces page displays these tabs.
   - **Interface 1**
   - **Interface 2**
   - **Interface 3**
   - **Interface 4**

   Each tab displays a table with these column names.

   Type Indicates whether the type is **IPv4** or **IPv6**.

   Address
   Indicates the address of the application interface. For example, `9.122.125.175`.

   Interface FQDN
   Indicates the fully qualified domain name of the application interface. For example, `igi.example.com`.

Netmask/Prefix

Indicates the netmask or prefix of the application interface. For example, `255.255.255.0`.

A netmask is used for **IPv4**, and a prefix is used for **IPv6**.

2. On any tab of the Application Interfaces page, do one of these actions.

Table 23. Application Interfaces action items

Action	Button	Description
`Add an address`	**New**	**Note:** • You must add an address at least in **Interface 1**; adding addresses for other interfaces is not mandatory. • Make sure the IP address that you assign is not used by any other system. 1. Select the **Interface 1** tab. 2. Click **New** to display the Add Address window. 3. Select one of the following options to indicate the type of address to add. **IPv4** **IPv4** defines each interface on a network uniquely. It is a 32-bit numeric address, which is written in decimal as four sets of digits that are separated by periods with no spaces or consecutive periods. Each number can be 0 - 255. For example, `9.122.20.250`. **IPv6** **IPv6** improves the efficiency of routing and provides greater security. It is a 128-bit IP address, which is written in hexadecimal and separated by colons. For example, `4ffe:1800:8484:3:220:f9ff:fe25:70cf` 4. Specify the fully qualified domain name of the application interface in the **Interface FQDN** field. 5. Do one of these actions. • For **IPv4 Settings**, do these steps. a. Type an address value in the **Address** field. b. Type a net mask value in the **NetMask** field. • For the **IPv6 settings**, do these steps. a. Type an address value in the **Address** field. b. From a range of 0-64, specify a prefix value in the **Prefix** field. 6. Click **Save**. 7. If any notifications are displayed in the **Notifications** widget, take appropriate actions as necessary. A message indicates that the application address is added successfully, and the record is listed in the **Interface 1** table.

Table 23. Application Interfaces action items (continued)

Action	Button	Description
`Edit an address`	**Edit**	1. Select an application interface. 2. Select the address. 3. Click **Edit** to display the Edit Address window. 4. Do one of these actions. • For **IPv4 Settings**, do these steps. a. Edit address value in the **Address** field. b. Edit net mask value in the **NetMask** field. • For **IPv6 Settings**, do these steps. a. Edit address value in the **Address** field. b. Edit prefix value in the **Prefix** field. 5. Click **Save**. A message indicates that the address is updated successfully.
`Delete an address`	**Delete**	1. Select an application interface. 2. Select the address. 3. Click **Delete** to display the Confirm Action window. 4. Click **Yes**. A message indicates that the address is deleted successfully.
`Test a connection`	**Test**	1. Click **Test** to display the Ping Server window. 2. In the **Server** field, enter the IP address or name of the server to test the connection with. 3. Click **Test**. A message indicates whether the test connection was successful or not.
`Refresh the application interface data`	**Refresh**	Click **Refresh** to display the most recent version of the data, including changes that were made to the data since it was last refreshed.

3. Click **Save Configuration**.

Managing hosts file

To manage hosts file with the IBM Security Identity Governance and Intelligence virtual appliance, use the Manage Hosts File page.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage System Settings** > **Network Settings** > **Hosts File**. All current host records with their IP addresses and host names are displayed.
2. On the Manage Hosts File page, work with host records or host names.
   - `Add a host record`
     a. Select the root level **Host Records** entry or do not select any entries.
     b. Click **New**.
     c. On the Create Host record page, do these actions.

Address
Specify the IP address of the host record.

Host Name
Specify the host name of the host record.

d. Click **Save**.

- Add a host name to a host record
  a. Select a host record entry to add the host name to.
  b. Click **New**.
  c. On the Add Hostname to Host Record page, enter the host name.
  d. Click **Save**.
- Remove a host record
  a. Select a host record entry to delete.
  b. Click **Delete**.
  c. On the confirmation page, click **Yes** to confirm the deletion.
- Remove a host name from a host record
  a. Select host name entry to delete.
  b. Click **Delete**.
  c. On the confirmation page, click **Yes** to confirm the deletion.

  Note: If the removed host name is the only associated host name for the IP address, then the entire host record (the IP address and host name) is removed.
- Refresh the data

  Click **Refresh** to display the most recent version of the data since it was last refreshed.

Configuring static routes

Configure static routes to the paired protection interfaces on your virtual appliance to enable network routers to redirect users to block pages or authentication pages.

About this task

This task is only necessary for networks that contain an additional network segment between the user segment and the virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **Network Settings** > **Routes**.
2. On the Static Routes page, complete one of these steps.

Table 24. Static route actions

Field	Action
IPv4 Default Gateway	1. Specify an address value. For example: `9.113.50.1`. 2. Click **Save**. **Note:** Click **Reset** to update the displayed value back to the current default gateway. It does not make any updates to the actual default gateway value.

Table 24. Static route actions (continued)

Field	Action
IPv6 Default Gateway	1. Specify an address value. For example: `3001:0DB9:0000:0000:02AB:00FF:FE29:9C6A`. 2. Click **Save**. **Note:** Click **Reset** to update the displayed value back to the current default gateway. It does not make any updates to the actual default gateway value.
New	1. Click **New** to create a route. 2. In the Add Route window, define values in these fields. • **Destination** • **Gateway** • **Metric** • **Interface or Segment** 3. Click **Save Configuration**.
Edit	1. Select an existing route. 2. Click **Edit** to change the settings. 3. In the Edit Route window, edit values in these fields. • **Destination** • **Gateway** • **Metric** • **Interface or Segment** 4. Click **Save Configuration**.
Delete	1. Select an existing route. 2. Click **Delete**. 3. Click **Yes** to confirm your action.

Results

The new and edited system routes are displayed in the **Currently active system routes** table.

Exporting or importing the configuration settings

Export all your configuration settings from one virtual appliance into a package for use on another virtual appliance. You can configure the settings on the virtual appliance with the Export/Import Settings page. You can also view or download reports from the Export/Import Settings page.

About this task

Export the configuration settings from one virtual appliance. In another virtual appliance, import the configuration settings from the previous virtual appliance.

Note: Export and import operations work with the same build versions of the virtual appliances. You cannot export a package from a different build version and import it on a virtual appliance with a different build version. Export and import settings are available on a primary node only.

A package typically contains information about signer certificates and custom files from the virtual appliance.

The Export/Import Settings table displays these columns.

Package Name
Displays the name of the package that you created. A typical package name format is `settings_`*`hostname_timestamp`*`.vasf`. The *timestamp* format is `yyyymmddhhmmss`, which is the date and time when the package was created. For example, `settings_itimetz06.in.ibm.com_20150815023455.vasf`.

Comment
Displays the comment that you added when you created the package.

Creation Date
Displays the date and time when you created the package.

Report
View or download the reports that were created during an export or import operation.

A report is created irrespective of whether the operation was successfully completed or not.

Do one of these actions.

View Click **View** to see the report details.

Download
Click **Download** to save a copy of the report to work with your requirements.

Procedure

1. On the primary node, from the top-level menu of the **Appliance Dashboard**, select **Manage** > **Manage Export/Import** > **Export/Import Settings**.
2. On the Export/Import Settings page, do one of these actions.

Table 25. Export or import settings actions

Action	Button	Description
`Creating a package`	**Create**	1. Click **Create**. 2. On the Add Comment window, specify helpful comments in the **Comment** field so that the package is easy to identify in the Export/Import Settings table. 3. Click **Save Configuration**. A message indicates that the package is created, and it is added in the Export/Import Settings table.

Table 25. Export or import settings actions (continued)

Action	Button	Description
`Applying settings`	**Apply**	1. From the Export/Import Settings table, select a package. 2. Click **Apply** to display the Apply Settings window. 3. In **Administrator ID**, specify the administrator user ID of the virtual appliance. 4. In **Administrator Password**, specify the administrator password of the virtual appliance. 5. Click **Save Configuration**. A message indicates that the settings are applied successfully.
`Deleting a package`	**Delete**	1. From the Export/Import Settings table, select a package. 2. Click **Delete**. 3. In the Confirm Delete window, click **Yes** to confirm. A message indicates that the package is deleted. The package is removed from the Export/Import Settings table.
`Uploading a package`	**Upload**	1. Click **Upload** to display the Upload Package window. **Note:** If a package is selected in the Export/Import Settings table, the **Upload** button is not active. Make sure to clear the package selection to keep the **Upload** button active. 2. Click **Browse** to select a package that you want to upload. 3. Click **Save Configuration**. A message indicates that the package is uploaded successfully to the virtual appliance.
`Downloading a package`	**Download**	1. From the Export/Import Settings table, select a package. 2. Click **Download**. 3. Save a copy of the package to your local drive to use them for your future requirements.
`Refresh the packages`	**Refresh**	Click **Refresh** to display the most recent version of the packages since it was last refreshed.

Configuring the date and time settings

Use the Date/Time page to configure the date, time, time zone, and NTP server information of the IBM Security Identity Governance and Intelligence virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage System Settings** > **System Settings** > **Date/Time**. The Date/Time page is displayed.
2. Configure the following options on the Date/Time page.

Option	Description
Date	Specifies the day, month, and year for the IBM Security Identity Governance and Intelligence virtual appliance.
Time	Specifies the time for the IBM Security Identity Governance and Intelligence virtual appliance.
Time Zone	Specifies the time zone for the IBM Security Identity Governance and Intelligence virtual appliance.
NTP Server address	Select **Enable NTP** to list the NTP (NIST Internet Time Service) servers that the IBM Security Identity Governance and Intelligence virtual appliance uses. You can enter multiple NTP servers, which are separated by commas.

Note: You cannot set the **Time Zone** or **Date/Time** by using the system console. You can specify only NTP server addresses.

3. Click **Save Configuration**.
4. Optional: Click **Reset** to set the configuration again or differently.

Configuring the administrator settings

Use the administrator settings to change the password that you use to access your IBM Security Identity Governance and Intelligence virtual appliance. Use the settings to also access the length of idle time that is granted to pass before your session times out.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage System Settings** > **System Settings** > **Administrator Settings**. The Administrator Settings page is displayed.
2. On the Administrator Settings page, type your current password in the **Current Password** field.
3. Type your new password in the **New Password** field.
4. Type your new password in the **New Password Confirmation** field.
5. In the **Session Timeout** field, click the arrows to select the amount of time that you are allowed to be idle before you are automatically logged out.
6. Click **Save Configuration**.

Managing the snapshots

Use snapshots to restore prior configuration and policy settings to the IBM Security Identity Governance and Intelligence virtual appliance.

Before you begin

Before you create or apply a snapshot, back up your database server and the directory server.

About this task

Snapshots are stored on the IBM Security Identity Governance and Intelligence virtual appliance. However, you can download the snapshots to an external drive in case of system failure.

The Snapshots table displays these columns.

File Name
Displays the name of the snapshot that you created. A typical file name is `igi_5.2_20150815-143940.605304_igi1172.ibm.com.snapshot`.

Comment
Displays the comment that you added when you created the snapshot.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **System Settings** > **Snapshots**. The Snapshots page is displayed.
2. On the Snapshots page, do one or more of the following actions.

Action	Option	Description
`Create a snapshot`	**New**	1. Click **New**. 2. On the Add Snapshot window, specify helpful comments in the **Comments** field, so that the snapshot is easy to identify in the virtual appliance. **Note:** Read the considerations about snapshots when you create it. 3. Click **Save Configuration**. A message indicates that the snapshot is created successfully, and it is added in the Snapshots table.
`Edit a snapshot`	**Edit**	1. Select a snapshot. 2. Click **Edit**. 3. On the Edit Snapshot window, edit the existing comment in the **Comments** field. 4. Click **Save Configuration**. A message indicates that the snapshot is edited successfully.
`Delete a snapshot`	**Delete**	1. Select one or more snapshots. 2. Click **Delete**. 3. Click **Yes** to confirm. A message indicates that the snapshot is deleted successfully.

Action	Option	Description
`Apply a snapshot`	**Apply**	**Note:** - You must apply the snapshot of the same virtual appliance that you are working on. - If configuration or policy versions are newer than the firmware version, the settings are rejected. If the configuration and policy versions are older than the firmware version, the settings are moved to the current firmware version. - When you apply a snapshot, the directories that you created from the Custom File Management page are not removed. 1. Select a snapshot. 2. Click **Apply**. 3. On the Apply Snapshot window, read the considerations. 4. Click **Yes** to confirm. Wait until the snapshot is applied. After the snapshot is applied, a notification indicates you to restart the virtual appliance. **Important:** If you face any login problems after you apply a snapshot, do these steps. 1. Clear the service integration bus (SIB) tables. For more information, see Clear the SIB tables. 2. Restart the Security Directory Integrator and the IBM Security Identity Governance and Intelligence. For more information, see "Viewing the server control widget" on page 57.
`Download a snapshot`	**Download**	1. Select one or more snapshots. 2. Click **Download**. 3. Browse to the location where you want to save the snapshot. 4. Save the file. **Note:** If you download multiple snapshots, the snapshots are compressed into a `.zip` file.
`Upload a snapshot`	**Upload**	**Note:** You can upload only 1 snapshot at a time. 1. Click **Upload**. 2. In the Upload Snapshot window, click **Browse for Snapshot**. 3. Select the snapshot that you want to upload. The snapshot information is displayed in the Files to upload table. **Note:** Wait until the snapshot is uploaded. When the snapshot is uploaded, the comment, if any, is populated in the **Comments** field. 4. Click **Save Configuration**. A message indicates that the snapshot is uploaded successfully.
`Refresh the snapshot data`	**Refresh**	To display the most recent snapshot data, click **Refresh**.

Managing the support files

IBM Customer Support uses support files to help you troubleshoot problems with the IBM Security Identity Governance and Intelligence virtual appliance. Support files contain all log files, temporary and intermediate files, and command output that is needed to diagnose customer support problems.

About this task

Support files might contain customer-identifiable information, such as IP addresses, host names, user names, and policy files. Support files do not contain confidential information, such as passwords, certificates, and keys. All files inside a support file contain text that can be inspected and censored by the customer.

The support file contents are stored in a compressed file.

Tip: You can create multiple support files to track an issue over time.

The Support Files table displays these columns.

File Name
Displays the name of the support file that you created. A typical file name is `igi_5.2_20150815-143940_igi1172.ibm.com_support.zip`.

Comment
Displays the comment that you added when you created the support file.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **System Settings** > **Support Files**. The Support Files page is displayed.
2. On the Support Files page, do one or more of the following actions.

Action	Option	Description
`Create a support file`	**New**	1. Click **New**. 2. In the **Comments** field of the Create Support file window, type a comment to describe the support file. 3. Click **Save Configuration**. A message indicates that a support file is created, and it is added in the Support Files table.
`Edit a support file`	**Edit**	1. Select a support file. 2. Click **Edit**. 3. On the Edit Support file window, edit the existing comment in the **Comments** field. 4. Click **Save Configuration**. A message indicates that the comment is edited.
`Delete a support file`	**Delete**	1. Select one or more support files. 2. Click **Delete**. 3. Click **Yes** to confirm. A message indicates that the support file is deleted.

Action	Option	Description
`Download a support file`	**Download**	1. Select one or more support files. 2. Click **Download**. 3. Browse to the location where you want to save the support files. 4. Save the file. **Note:** If you download multiple support files, the files are compressed into a `support.zip` file.

Configuring system audit events

Configure where you want the IBM Security Identity Governance and Intelligence virtual appliance to send notifications about changes to system settings and problems with the virtual appliance.

About this task

Available objects include system audit events that are predefined in the virtual appliance and any system audit event objects that you created.

Important: Predefined system audit event objects cannot be deleted from the virtual appliance because they contain all the events that take place on the virtual appliance eventually. When you create objects such as SNMP, email, or syslog, you can delete these created objects.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **System Settings** > **System Audit Events**. The System Audit Events page displays the Available Objects pane and the Added Objects pane.
2. Complete one or more of the following tasks in the System Audit Events page.
   - To create a system audit event object, click **New**.

     The following system audit event objects are listed:
     - SNMP
     - Email
     - Remote Syslog

     See these related topics to configure one or more of the following system audit event objects.
     - "Configuring SNMP objects" on page 98
     - "Configuring email objects" on page 99
     - "Configuring remote syslog objects" on page 100
   - To receive notifications for problems with the system, select one or more system audit event objects from the Available Objects pane, and add or move them to the Added Objects pane.
   - To edit a system audit event object, complete the following steps:
     a. Select a system audit event object in the Added Objects pane.
     b. Click **Edit**.
     c. Change the values in these fields according to your requirement.
        - **Name**
        - **Total Event Storage Limit**

      - **NAP Events Allocation**
      - **IPS Events Allocation**
      - **System Events Allocation**
      - **Comment**
   d. Click **Save Configuration**.
3. Optional: To delete a system audit event object, do these steps.
   a. Select a system audit event object that you created.
   b. Click **Delete**.
   c. Click **Yes** to confirm.
4. Click **Save Configuration**.
5. Optional: Click **Reset** to revert to the last updated changes.

Configuring SNMP objects

Configure Simple Network Management Protocol (SNMP) objects to enable the IBM Security Identity Governance and Intelligence virtual appliance to send system audit events to an SNMP manager. The SNMP notifications identify certain values and send them to an SNMP manager.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **System Settings** > **System Audit Events**.
2. In the System Audit Events page, take one of the following actions.
   - Click **New** > **SNMP** to display the Add SNMP Object window.
   - Select an existing SNMP object and then click **Edit** to display the Edit SNMP Object window.
3. In the **General** tab, type a name for the object.
4. Select an **SNMP version** from the list.
   - V1
   - V2C
   - V3
5. In the **SNMP Governance** field, type the IP address, host name, or fully qualified domain name (FQDN) of the SNMP manager.

   Note: The SNMP host must be accessible to the virtual appliance to send SNMP traps.
6. Type the port number that the SNMP manager monitors for notifications.

   Note: The default port number is 162.
7. Type a comment to describe the SNMP object.
8. For SNMP versions V1 or V2c, type the name of the community that is used to authenticate with the SNMP agent.
9. For SNMP version 3, configure the following options.

Option	Description
Name	Type the user name to be authenticated in the SNMP database.

Option	Description
Notification Type	On the **Notification Type** tab, complete these steps. 1. Select **Inform** or **Trap** in the **Notification Type** field. 2. Specify the **SNMP Timeout** in seconds. **Note:** Specifying a timeout value is not mandatory.
Authentication and Privacy	On the **Authentication and Privacy** tab, complete these steps. 1. From the **Enable Authentication** list, select **Enabled** to enable authentication. 2. In **Authentication Passphrase**, type the relevant passphrase. 3. From the **Authentication Type** list, select a type. 4. From the **Enable Privacy** list, select **Enabled** to enable privacy. 5. In **Privacy Passphrase**, type the relevant passphrase. 6. From the **Privacy Type** list, select a type.

10. Click **Save Configuration**.

What to do next

After you configure an SNMP object, add the object to the Added Objects pane on the System Audit Events page. Add it so that the virtual appliance initiates the response when specified events occur.

Configuring email objects

You can create email objects to send an email notification to specified users or to administrators when specified events occur on your network. You can also select the event parameters to include in the message so that important information about detected events is provided.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **System Settings** > **System Audit Events**.
2. In System Audit Events page, take one of the following actions.
   - Click **New** > **Email** to display the Add Email Object window.
   - Select an existing email object and then click **Edit** to display the Edit Email Object window.
3. Configure the following options.

Option	Description
Name	Specifies a meaningful name for the response. **Note:** This name displays when you select responses for events, so give the response a name that allows users to easily identify what they are selecting.

Option	Description
From	Specifies the email address that displays in the **From** field of the email.
To	Specifies the email address or group of addresses to receive the email. **Note:** Separate individual email addresses with a comma or semicolon.
SMTP Server	Specifies the fully qualified domain name or IP address of the mail server. **Note:** The SMTP server must be accessible to the virtual appliance to send email notifications.
SMTP Port	Specifies the custom port that is used to connect to the SMTP server. The default is 25.
Comment	Type a comment to identify the email object.

4. Click **Save**.

What to do next

After you configure an email object, add the object to the Added Objects pane on the System Audit Events page. Add it so that the virtual appliance initiates the response when specified events occur.

Configuring remote syslog objects

Configure remote syslog objects to enable the system to record system events in a remote log file.

About this task

If the connection to the remote syslog server drops, the IBM Security Identity Governance and Intelligence virtual appliance generates a system audit event. If you are using TCP protocol, the virtual appliance writes the events to an auxiliary storage file. When the connection is restored, events that are stored in this file are sent to the remote syslog server. If the connection is not restored before the storage file size exceeds, any additional events are dropped. The virtual appliance generates another system audit event when the connection is reestablished.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **System Settings** > **System Audit Events**.
2. In the System Audit Events page, do one of the following steps.
   - Click **New** > **Remote Syslog** to display the Add Remote Syslog Object window.
   - Select an existing remote syslog object and then click **Edit** to display the Edit Remote Syslog Object window.
3. Configure the following options.

Option	Description
Name	Specifies a meaningful name for the response.

Option	Description
Remote Syslog Collector	Specifies the fully qualified domain name or IP address of the host on which you want to save the log. **Note:** The host must be accessible to the virtual appliance.
Remote Syslog Collector Port	Specifies the custom port that is used to connect to the syslog collector. The default is 514.
QRadar Format Enabled	Select this check box to enable the virtual appliance to send events in QRadar LEEF format instead of RFC5424 remote syslog format.
Comment	Type a comment to identify the remote syslog object.

4. Click **Save Configuration**.

What to do next

After you configure a remote syslog object, add the object to the Added Objects pane on the System Audit Events page. Add it so that the virtual appliance initiates the response when specified events occur.

Restarting or shutting down

Use the Restart or Shut down page to restart or shut down the IBM Security Identity Governance and Intelligence virtual appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage System Settings** > **System Settings** > **Restart or Shut down**. The Restart or Shut down page is displayed.
2. Do one of the following tasks.

Option	Description
Restart	Restarting the IBM Security Identity Governance and Intelligence virtual appliance takes it offline for several minutes.
Shut Down	Shutting down the IBM Security Identity Governance and Intelligence virtual appliance takes it offline and makes it inaccessible over the network until you restart it.

IBM Security Identity Governance and Intelligence virtual appliance command line interface

Access the command line interface (CLI) of the virtual appliance by using either an `ssh` session or the console.

The IBM Security Identity Governance and Intelligence virtual appliance CLI commands are broadly divided into the two sections such as current mode commands and global commands. The topic provides information about the IBM Security Identity Governance and Intelligence virtual appliance CLI commands for the following functions.

The following example shows the transcript of using an `ssh` session to access the virtual appliance.

```
usernameA@example.com> ssh -l admin igiva.example.com
admin@igiva.example.com's password:
Welcome to the IBM Security Identity Governance and Intelligence appliance
Enter "help" for a list of available commands
igiva.example.com> igi
igiva.example.com:igi> help
Current mode commands:
firmware_update     Work with the IGI firmware settings.
service_trace       Work with the IGI trace settings.
Global commands:
back                Return to the previous command mode.
exit                Log off from the appliance.
help                Display information for using the specified command.
reboot              Reboot the appliance.
shutdown            End system operation and turn off the power.
top                 Return to the top level.
igiva.example.com:igi>
```

You can also access the console by using the appropriate VMware software. For example, VMware vSphere Client.

Note: The CLI contains only a subset of the function available from the graphical user interface.

IBM Security Identity Governance and Intelligence virtual appliance global commands

The IBM Security Identity Governance and Intelligence virtual appliance CLI global commands can be used with any of the current mode commands.

Global commands

The following list gives a high-level overview of the global functions available in the command line interface commands.

`back` Returns to the previous command mode.

`exit` Logs off from the appliance.

`help` Displays information for using the specified command.

`reboot` Restarts the appliance.

`shutdown`
Ends system operations and turns off the power.

`top` Returns to the top level.

IBM Security Identity Governance and Intelligence virtual appliance current mode commands

The IBM Security Identity Governance and Intelligence virtual appliance CLI commands are broadly divided into the two sections such as current mode commands and global commands. The topic provides information about the IBM Security Identity Governance and Intelligence virtual appliance current mode commands for the following functions.

The following list gives a high-level overview of the functions available from the command line interface.

firmware

The function provides options to work with the firmware images.

backup Backs up firmware on the active partition to the inactive partition.

get_comment
Shows the comment that is associated with a firmware image.

get_info
Shows the version information that is associated with a firmware image.

list Lists information about the installed firmware images. Firmware information includes the active firmware image, a description of the firmware, the date the firmware was installed and optional backup information.

set_comment
Replaces the comment that is associated with a firmware image.

swap_active
Swaps the active firmware image. The appliance restarts the system with the inactive firmware image.

fixpacks

The function works with the fix packs. The corresponding task can be completed by using the graphical user interface. Go to **Manage** > **Updates and Licensing** > **Fix Packs**.

install
Installs the available fix packs on the inserted USB device.

list Lists the available fix packs on the inserted USB device.

rollback
Uninstalls the most recently installed fix pack.

view_history
Shows the installation history for all fix packs.

igi

The **igi** command is used to work with the IBM Security Identity Governance and Intelligence settings.

jvm_property
Provides options to work with the application server JVM properties.

logs Provides options to work with the IBM Security Identity Governance and Intelligence log files.

upgrade
Provides options to work with IBM Security Identity Governance and Intelligence firmware updates.

utilities
Provides options to work with IBM Security Identity Governance and Intelligence utilities.

license

The function provides options to work with the licenses.

install
Installs a license file from an inserted USB device.

list Lists the available license files on the inserted USB device.

show Displays the current active license information.

lmi

The function provides options to work with the local management interface.

reset_lmi_cert
Restarts the server certificate for the local management interface to a self-signed certificate.

restart
Restarts the local management interface.

trace Provides options to work with the trace settings for the local management interface.

management

dns Provides options to work with the virtual appliance DNS settings.

hostname
Provides options to work with the virtual appliance host name.

interfaces
Provides options to work with the management interface settings.

set_password
Sets the virtual appliance password.

snapshots

The function provides options to work with the snapshots. The corresponding task can be completed by using the graphical user interface. Go to **Manage** > **System Settings** > **Snapshots**.

Note: You must restart the virtual appliance after you apply the snapshot.

apply Applies a policy snapshot file to the system.

create Creates a snapshot of current policy files.

delete Deletes a policy snapshot file.

download
Downloads a policy snapshot file to a USB flash drive.

get_comment
Shows the comment that is associated with a policy snapshot file.

list Lists the policy snapshot files.

set_comment
Replaces the comment that is associated with a policy snapshot file.

upload Uploads a policy snapshot file from a USB flash drive.

`support`

The function generates the support files. The corresponding task can be completed by using the graphical user interface. Go to **Manage** > **System Settings** > **Support Files**.

`create` Creates a support information file.

`delete` Deletes a support information file.

`download`
Downloads a support information file to a USB flash drive.

`get_comment`
Shows the comment that is associated with a support information file.

`list` Lists the support information files.

`set_comment`
Replaces the comment that is associated with a support information file.

`tools`

`connect`
Tests the network connection to a certain port on a specified host.

`connections`
Displays the network connections for the appliance.

`nslookup`
Queries internet domain name servers.

`ping` Sends an `ICMP ECHO_REQUEST` to network hosts.

`traceroute`
Traces a packet from a computer to a remote destination. Shows the required number of hops for a packet that is required to reach the destination and the duration of each hop.

More information can be obtained by entering **`help`** on any of the subcommands.

IBM Security Identity Governance and Intelligence virtual appliance command line interface commands

The initial virtual appliance settings wizard runs the first time that an Administrator logs on to the command line interface (CLI) of an unconfigured virtual appliance. The topic provides information about the sub sections of the virtual appliance CLI command that is specific to IBM Security Identity Governance and Intelligence.

The IBM Security Identity Governance and Intelligence virtual appliance CLI commands are broadly divided into the following main sections:

- Current mode commands
- Global commands

In the current mode commands, the **`igi`** command is used to work with the IBM Security Identity Governance and Intelligence settings. When an Administrator or a user enters the **`igi`** command, the following sub sections are listed.

`jvm_property`

`add` Adds a JVM property in the application server.

delete Deletes an existing JVM property from the application server.

List Lists the existing JVM properties in the application server.

update Updates an existing JVM property in the application server.

logs

clear_ffdc
Clears all the FFDC log files on the system.

monitor
Provides options to monitor the log files on the system.

upgrade

The sub section provides options to work with IBM Security Identity Governance and Intelligence firmware updates.

delete Deletes firmware updates from the system.

install
Installs the available firmware update to the system.

list Lists firmware updates from a USB device.

transfer
Transfers firmware update from a USB device to the system.

utilities

ib_settings
Provides options to work with the Identity Brokerage settings.

sib_schema_name
Provides options to work with the SIB schema name.

session_timeout
Provides options to work with the timeout interval for desk and administrative user interfaces.

More information can be obtained by entering **help** on any of the subcommands.

Tailing logs and archiving logs

You can generate tailing logs and archiving logs through the command-line interface in the IBM Security Identity Governance and Intelligence virtual appliance.

About this task

To see a list of available commands, enter the `help` command at the command-line prompt. The **help** command provides detailed information about each command from the list.

Procedure

1. From the command-line interface, log on to the IBM Security Identity Governance and Intelligence virtual appliance.

   For example,

   ```
   usernameA@example.com> ssh -l admin igivasrv
   admin@igivasrv's password: admin
   ```

The following message is displayed:

```
Welcome to the IBM Security Identity Governance and Intelligence appliance
Enter "help" for a list of available commands
```

2. Enter the `help` command at the `igivasrv` prompt for a list of available commands. The following result is displayed:

```
Current mode commands:
firmware            Work with firmware images.
fixpacks            Work with fix packs.
igi                 Work with the IGI settings.
license             Work with licenses.
lmi                 Work with the local management interface.
management          Work with management settings.
snapshots           Work with policy snapshot files.
support             Work with support information files.
tools               Work with network diagnostic tools.
updates             Work with firmware and security updates.
Global commands:
back                Return to the previous command mode.
exit                Log off from the appliance.
help                Display information for using the specified command.
reboot              Reboot the appliance.
shutdown            End system operation and turn off the power.
top                 Return to the top level.
```

3. Enter the `igi` command at the `igivasrv` prompt.
4. Enter the `help` command at the `igivasrv:igi` prompt for a list of available commands. The following result is displayed:

```
Current mode commands:
jvm_property        Work with the Application Server JVM properties
logs                Work with the IBM Security Identity Governance and
                    Intelligence log files.
upgrade             Work with the IBM Security Identity Governance and
                    Intelligence upgrade.
utilities           Work with the IBM Security Identity Governance and
                    Intelligence utilities.

Global commands:
back                Return to the previous command mode.
exit                Log off from the appliance.
help                Display information for using the specified command.
reboot              Reboot the appliance.
shutdown            End system operation and turn off the power.
top                 Return to the top level.
```

5. Enter the `logs` command at the `igivasrv:igi` prompt.
6. Enter the `help` command at the `igivasrv:igi:logs` prompt for a list of available commands. The following result is displayed:

```
Current mode commands:
clear_ffdc          Clear all FFDC log files on the system.
monitor             Monitor log files on the system.
Global commands:
back                Return to the previous command mode.
exit                Log off from the appliance.
help                Display information for using the specified command.
reboot              Reboot the appliance.
shutdown            End system operation and turn off the power.
top                 Return to the top level.
```

7. Enter the `monitor` command at the `igivasrv:igi:logs` prompt.
8. Enter the `help` command at the `igivasrv:igi:logs:monitor` prompt for a list of available commands. The following result is displayed:

```
Options:
1: System
2: LMI
3: Configuration
4: IGI Application Server
5. Broker Application Server
```

   Note: Similarly, you can enter the **`clear_ffdc`** command at the `igivasrv:igi:logs` prompt to clear all FFDC log files on the system.

9. Enter the index number to view a list of logs. For example, to view the cluster manager logs, specify 4 at **Enter index**.

   The following message is displayed:

```
Options:
1: SystemErr.log
2: SystemOut.log
3: native_stderr.log
4: native_stdout.log
5: startServer.log
6: stopServer.log
```

10. Enter the index number to view the tailing logs of the cluster manager. For example, specify 1 at **Enter index**.

    The following message is displayed:

    ```
    ************ Start Display Current Environment ************
    Log file started at: [3/13/15 17:42:49:673 EDT]
    ************* End Display Current Environment *************
    ```

11. Enter the index number to view the tailing logs of the IBM Security Identity Governance and Intelligence server. For example, specify 7 at **Enter index**.

    The following message is displayed:

    ```
    1: SystemErr.log
    2: SystemOut.log
    3: SystemOut_15.03.17_02.42.19.log
    4: native_stderr.log
    5: native_stdout.log
    6: startServer.log
    7: stopServer.log
    8: SystemErr.log
    9: SystemOut.log
    10: native_stderr.log
    11: native_stdout.log
    12: startServer.log
    13: stopServer.log
    14: msg.log
    15: trace.log
    ```

12. Enter the number of lines to tail. For example, specify 1.

    The following message is displayed:

    ```
    ************ Start Display Current Environment ************
    Log file started at: [3/13/15 17:42:49:673 EDT]
    ************* End Display Current Environment*************
    ```

13. Enter the index number to view the trace logs of the IBM Security Identity Governance and Intelligence server. For example, specify 3 at **Enter index**.

    The following message is displayed:

    ```
    Options:
    1: console.log
    2: messages.log
    3: messages_16.01.22_08.52.43.0.log
    ```

14. Enter the number of lines to tail. For example, specify 5.

    The following message is displayed:

    ```
    <Time Millis="1426836005522"> 2015.03.20 03:20:05.522-04:00</Time>
    <Server Format="IP">igi1175.in.ibm.com</Server>
    <ProductId>CTGIM</ProductId>
    <Component>com.ibm.itim.pim.serviceprovider.db</Component>
    <ProductInstance>IGIVa_APP_MEMBER</ProductInstance>
    ```

Adding a JVM property

As part of configuring an application server, you might define settings that enhance the way your operating system uses of the Java virtual machine (JVM). Use the steps to add a JVM property in the Application server.

About this task

The JVM is an interpretive computing engine that is responsible for running the byte codes in a compiled Java program. The JVM translates the Java byte codes into the default instructions of the host server. The application server, being a Java process, requires a JVM to run and to support the Java applications that run on it. JVM settings are part of an application server configuration.

Access the command-line interface (CLI) of the virtual appliance by using either an `ssh` session or the console.

To see a list of available commands, enter the `help` command at the command-line prompt. The **`help`** command provides detailed information about each command from the list.

Procedure

1. From the command-line interface, log on to the IBM Security Identity Governance and Intelligence virtual appliance. The following message is displayed:

   ```
   Welcome to the IBM Security Identity Governance and Intelligence appliance
   Enter "help" for a list of available commands
   ```

2. Enter the `help` command at the `igivasrv` prompt for a list of available commands. The following result is displayed:

   ```
   Current mode commands:
   firmware            Work with firmware images.
   fixpacks            Work with fix packs.
   igi                 Work with the IGI settings.
   license             Work with licenses.
   lmi                 Work with the local management interface.
   management          Work with management settings.
   snapshots           Work with policy snapshot files.
   support             Work with support information files.
   tools               Work with network diagnostic tools.
   updates             Work with firmware and security updates.
   Global commands:
   back                Return to the previous command mode.
   exit                Log off from the appliance.
   help                Display information for using the specified command.
   reboot              Reboot the appliance.
   shutdown            End system operation and turn off the power.
   top                 Return to the top level.
   ```

3. Enter the `igi` command at the `igivasrv` prompt.
4. Enter the `help` command at the `igivasrv:igi` prompt for a list of available commands. The following result is displayed:

   ```
   Current mode commands:
   jvm_property        Work with the Application Server JVM properties
   logs                Work with the IBM Security Identity Governance and
                       Intelligence log files.
   upgrade             Work with the IBM Security Identity Governance and
                       Intelligence upgrade.
   utilities           Work with the IBM Security Identity Governance and
                       Intelligence utilities.

   Global commands:
   back                Return to the previous command mode.
   exit                Log off from the appliance.
   help                Display information for using the specified command.
   reboot              Reboot the appliance.
   shutdown            End system operation and turn off the power.
   top                 Return to the top level.
   ```

5. Enter the `jvm_property` command at the `igivasrv:igi` prompt.
6. Enter the `help` command at the `igivasrv:jvm_property` prompt for a list of available commands. The following result is displayed:

   ```
   Current mode commands:
   add                 Add a JVM Property in Application server.
   delete              Delete an existing JVM Property in Application server.
   list                List existing JVM Properties in Application
                       Server
   update              Update an existing JVM Property in Application server.
   Global commands:
   back                Return to the previous command mode.
   exit                Log off from the appliance.
   help                Display information for using the specified command.
   reboot              Reboot the appliance.
   shutdown            End system operation and turn off the power.
   top                 Return to the top level.
   ```

7. Enter the `add` command at the `igivasrv:jvm_property` prompt. The following result is displayed:

   ```
   Property name  : com.ibm.websphere.webservices.soap.enable.legacy.get.behavior
   Property value : true

   Adding JVM property
   JVM Property added successfully.
   Restart Identity Governance and Intelligence server to apply the new settings.
   ```

What to do next

Restart the IBM Security Identity Governance and Intelligence server to apply the new settings.

Managing the SSL certificate

You can use either the local management interface or web service to manage the SSL certificate.

About this task

If the certificate expires, the local management interface is not reachable. In this situation, use the reset_lmi_cert CLI command in the local management interface menu to generate a self-signed certificate so that access to the local management interface can be re-established. Then, use the restart CLI command to restart the local management interface.

Procedure

1. From the command-line interface, log on to the IBM Security Identity Governance and Intelligence virtual appliance. The following message is displayed:

   ```
   Welcome to the IBM Security Identity Governance and Intelligence appliance
   Enter "help" for a list of available commands
   ```

2. Enter the `help` command at the `igivasrv` prompt for a list of available commands. The following result is displayed:

   ```
   Current mode commands:
   firmware            Work with firmware images.
   fixpacks            Work with fix packs.
   igi                 Work with the IGI settings.
   license             Work with licenses.
   lmi                 Work with the local management interface.
   management          Work with management settings.
   snapshots           Work with policy snapshot files.
   support             Work with support information files.
   tools               Work with network diagnostic tools.
   updates             Work with firmware and security updates.
   Global commands:
   back                Return to the previous command mode.
   exit                Log off from the appliance.
   help                Display information for using the specified command.
   reboot              Reboot the appliance.
   shutdown            End system operation and turn off the power.
   top                 Return to the top level.
   ```

3. Enter the `lmi` command at the `igivasrv` prompt.
4. Enter the `help` command at the `igivasrv:lmi` prompt for a list of available commands. The following result is displayed:

   ```
   Current mode commands:
   reset_lmi_cert      Reset the server certificate for the local
                       management interface to a self signed certificate.
   restart             Restart the local management interface.
   trace               Work with the trace settings for the local management
                       interface.

   Global commands:
   back                Return to the previous command mode.
   exit                Log off from the appliance.
   ```

```
help            Display information for using the specified command.
reboot          Reboot the appliance.
shutdown        End system operation and turn off the power.
top             Return to the top level.
```

5. Enter the `reset_lmi_cert` command at the `igivasrv:lmi` prompt.
6. Enter `YES` to confirm the reset request.
7. Enter the `restart` command at the `igivasrv:lmi` prompt.

Getting and setting the SIB schema names

Get and set the correct Service Integration Bus (SIB) schema names through the command-line interface of the IBM Security Identity Governance and Intelligence virtual appliance.

About this task

When you want to set up the virtual appliance cluster, you must know the SIB schema name. You can also set the schema name to meet the requirements.

To see a list of available commands, enter the `help` command at the command-line prompt. The **`help`** command provides detailed information about each command from the list.

Procedure

1. From the command-line interface, log on to the IBM Security Identity Governance and Intelligence virtual appliance.
2. Type the **`igi`** command at the `igivasrv` prompt for a list of available commands.
3. Type the **`utilities`** command at the `igivasrv:igi` prompt for a list of available commands.
4. Type the **`sib_schema_name`** command at the `igivasrv:utilities` prompt for a list of SIB schema name mode commands.
5. Type the **`get`** command at the `igivasrv:sib_schema_name` prompt to get the SIB schema name. The following result is displayed:

   ```
   itiml002
   ```
6. Type the **`set`** command at the `igivasrv:sib_schema_name` prompt to set the SIB schema name.

   Note: The SIB schema name must be 8 characters long.
   The following result is displayed:

   ```
   Enter new SIB schema name
   ```
7. Specify the new SIB schema name and press enter. For example, specify `itiml003`.

   The following message is displayed:

   ```
   Successfully set SIB schema name.
   ```

Getting and setting the reconciliation failure threshold

Get or set the maximum number of local accounts to delete at end of reconciliation through the command-line interface of the IBM Security Identity Governance and Intelligence virtual appliance.

About this task

To see a list of available commands, enter the `help` command at the command-line prompt. The **help** command provides detailed information about each command from the list.

Procedure

1. From the command-line interface, log on to the IBM Security Identity Governance and Intelligence virtual appliance.
2. Type the **igi** command at the `igivasrv` prompt for a list of available commands.
3. Type the **utilities** command at the `igivasrv:igi` prompt for a list of available commands.
4. Type the **ib_settings** command at the `igivasrv:utilities` prompt for a list of Identity Brokerage mode commands.
5. Type the **ib_recon_failure_threshold** command at the `igivasrv:ib_settings` prompt.
6. Type the **get** command at the `igivasrv:ib_recon_failure_threshold` prompt to get the value of reconciliation failure threshold. The following result is displayed:
   ```
   15%
   ```
7. Type the **set** command at the `igivasrv:ib_recon_failure_threshold` prompt to set the reconciliation failure threshold. The following result is displayed:
   ```
   The value specifies maximum as percentage of
   total accounts to be deleted at end of reconciliation.
    Enter the value in percentage:
   ```
8. Specify the threshold and press enter. For example, specify `20`.

   The following message is displayed:
   ```
   Successfully set the value of reconciliation failure threshold.
   ```

Setting the session timeout

Use this procedure to set the timeout interval for the desk and central administration user interface.

About this task

The default timeout interval is 10 minutes. The minimum timeout interval is 2 minutes. If you do not want the sessions to expire, use `0` as the timeout setting.

To see a list of available commands, enter the `help` command at the command line prompt. The **help** command provides detailed information about each command from the list.

Procedure

1. From the command line interface, log on to the IBM Security Identity Governance and Intelligence virtual appliance.
2. Type the **igi** command at the `igivasrv` prompt.
3. Type the **utilities** command at the `igivasrv:igi` prompt.
4. Type the **session_timeout** command at the `igivasrv:utilities` prompt.
5. Type the **set** command at the `igivasrv:session_timeout` prompt to set the session timeout interval.

   The following message is displayed:

```
Current timeout (in minutes): 11
New timeout (in minutes):
```

6. Specify the new timeout interval and press Enter. For example, specify 15.

   The following message is displayed:

   ```
   Current timeout (in minutes): 11
   New timeout (in minutes): 15
   Session timeout updated successfully
   ```

7. Restart the IBM Security Identity Governance and Intelligence server to apply the new settings.

Virtual appliance maintenance

IBM Security Identity Governance and Intelligence virtual appliance provides tools for creating backups and snapshots of the virtual appliance, importing and exporting configuration files, and installing fix packs.

Setting up a secondary virtual appliance for active-passive configuration

You can provide a basic level of disaster recovery by setting up the IBM Security Identity Governance and Intelligence virtual appliance into two virtual appliances with active-passive configuration.

Complete the following tasks to deploy an active-passive configuration for the virtual appliances:

1. "Setting up a primary virtual appliance."
2. Optional: "Backing up the virtual appliance."
3. Optional: "Reverting the virtual appliance to its backup" on page 114
4. "Creating a snapshot of the virtual appliance" on page 114.
5. "Setting up a secondary virtual appliance" on page 115.

Setting up a primary virtual appliance

Set up the primary virtual appliance for the active-passive configuration.

Procedure

1. Create a virtual machine on the VMware ESXi Server by using the IBM Security Identity Governance and Intelligence virtual appliance ISO. See "Setting up the virtual machine" on page 15.
2. Complete the first steps configuration. For example, configure the host name and IP address. For more information, see "Setting up the initial virtual appliance" on page 17.
3. Complete the virtual appliance configuration. See "Setting up a stand-alone or primary node for IBM Security Identity Governance and Intelligence with the initial configuration wizard" on page 23.
4. Log on to the applications by using the **Appliance Dashboard** console. See "Validating configuration with quick links" on page 59.
5. Verify that the applications are started.
6. Verify that the user can log on to IBM Security Identity Governance and Intelligence to complete the operations.

Backing up the virtual appliance

You can back up the virtual appliance configuration.

About this task

The virtual appliance has two disk partitions, and at any time one is active and another is inactive. Backing up the virtual appliance is an optional procedure to back up the entire active partition to the inactive partition on the same virtual appliance.

Procedure

1. Stop the database instance on the external data tier.
2. On the **Appliance Dashboard**, locate the **Server Control** widget.
3. Stop the Identity Governance Service. See "Viewing the server control widget" on page 57.
4. Create a backup of the active partition on the secondary partition.
   a. On the **Appliance Dashboard**, locate the **Partition Information** widget.
   b. Under the **Partition Information** widget, click **Firmware Settings**.
   c. Select the active partition and then click **Create Backup**.

   The system restarts and backs up the primary partition.

Related tasks:

"Reverting the virtual appliance to its backup"
To revert the virtual appliance to its backup, start the virtual appliance through the inactive partition, which is the partition from where the backup was taken.

Reverting the virtual appliance to its backup

To revert the virtual appliance to its backup, start the virtual appliance through the inactive partition, which is the partition from where the backup was taken.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **Updates and Licensing** > **Firmware Settings** to display the Firmware Settings page. .
2. Select the inactive partition and click **Set Active**.

Creating a snapshot of the virtual appliance

Use the **Appliance Dashboard** to create a snapshot of the virtual appliance. A snapshot that is created from a configured virtual appliance can be applied on the same virtual appliance to restore the configuration and policy settings. A snapshot contains configuration and policy settings. It can also be used to synchronize the configuration and policy settings between virtual appliances.

Procedure

Note: Create the snapshot of the external data tier, such as the directory server and database system, at the same time to preserve the current state. The document does not describe how to create the snapshot of the external data tier systems.

1. Stop the database instance on the external data tier.
2. In the appliance dashboard, stop the Identity Governance Service. See "Viewing the server control widget" on page 57.
3. From the top-level menu of the **Appliance Dashboard**, click **Manage** > **System Settings** > **Snapshots**.
4. On the Snapshots page, click **New** to create a snapshot.

5. Under **Comments**, specify comments so that the snapshot is easy to identify from a primary virtual appliance that is synchronized with the external data tier.
6. Download and save the snapshot on the network file system.
7. Stop the primary virtual appliance. Complete one of the following tasks.
   - On the ESXi Server, suspend the virtual machine by using the VMware vSphere Client.
   - Stop the virtual appliance with the `shutdown` command-line interface command.

Setting up a secondary virtual appliance

Set up the secondary virtual appliance. The secondary virtual appliance can be configured to point to the same data tier as the primary virtual appliance for high availability configuration. It can also be configured to point to a replicated (standby) data tier for disaster recovery configuration.

Procedure

1. Create a virtual machine on the VMware ESXi Server by using the IBM Security Identity Governance and Intelligence virtual appliance ISO.
2. Set up the virtual appliance. See "Setting up the initial virtual appliance" on page 17.
3. Log on to the virtual appliance console.
4. Click the **Manage Snapshots** link in the lower-left corner of the Setup Progress pane.
5. On the Snapshots page, upload the snapshots from the primary virtual appliance. Wait until the **Comment** field is updated on the snapshot upload screen. See "Managing the snapshots" on page 93.

   When the snapshot is uploaded, the screen is refreshed, and it lists the snapshots.
6. Select the snapshot from the primary virtual appliance. Use the comments and time stamps to help you select the right snapshot.
7. Click **Apply**.
8. After you apply the snapshot, log on to the command-line interface and run the **`shutdown`** command to shut down the secondary virtual appliance.
9. Start the database instance on the external data tier.
10. Start the secondary virtual appliance from the VMware Server.
11. When the secondary virtual appliance starts, log on to the virtual appliance user interface.
12. Go to the **Appliance Dashboard**.
13. From the **Appliance Dashboard**, verify that the **Middleware Monitor** widget indicates that all middleware and applications are started.

What to do next

Only one instance of the virtual appliance can run at any time. You can start the secondary virtual appliance only when the primary virtual appliance is down.

Verify that the applications are started and that the user can log on to IBM Security Identity Governance and Intelligence.

Index

Printed in USA