

IBM Security Identity Governance and Intelligence
Version 5.2.3

Installation Topics



IBM Security Identity Governance and Intelligence
Version 5.2.3

Installation Topics

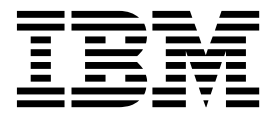


Table of contents

Table list	v	Updating the Oracle database for V5.2.3.	56
Chapter 1. Overview	1	Updating the DB2 database for V5.2.3	58
Chapter 2. Software firewall configuration in the virtual appliance	3	Synchronizing data.	60
Chapter 3. Support for FIPS 140-2 specifications	5	Loading role mining data.	60
Creating certificates for a FIPS connection with SAP	5	Building hierarchies	60
Chapter 4. Prerequisite software	9	Verify that the Rights Lookup tables have no duplicated values	61
Changing the default password for the database schemas	9	Upgrading Identity Brokerage Adapters	61
Installing the Oracle server	10	Chapter 7. Administration of the virtual appliance	63
Configuring the Oracle server	10	Appliance Dashboard	64
Installing the DB2 server	13	Viewing the notifications widget	64
Configuring the DB2 server	13	Viewing the middleware and server monitor widget	65
Installing and configuring the directory server.	18	Viewing partition information	65
Chapter 5. Installation	21	Viewing disk usage.	66
Installation of the IBM Security Identity Governance and Intelligence virtual appliance	21	Viewing IP addresses	66
VMware support	21	Viewing the server control widget.	67
XenServer support	27	Viewing the cluster status	67
Amazon EC2 support	29	Validating configuration with quick links	69
KVM support.	31	Virtual appliance administration	69
Setting up a stand-alone or primary node for IBM Security Identity Governance and Intelligence with the initial configuration wizard.	33	Viewing the event logs	69
Sample configuration response file.	35	Viewing the memory usage	70
Planning for high availability	36	Viewing the CPU usage	71
Setting up a virtual appliance cluster.	38	Viewing the storage usage	72
Recovering from a primary node failure.	46	Managing the SNMP monitoring	72
Logging on to the virtual appliance console	46	Enabling Identity Brokerage Providers in the virtual appliance	73
Logging on to the consoles from the appliance dashboard	47	Managing directory server configuration	74
Synchronizing data after the installation.	47	Authenticating users from an external user registry to the Local Management Interface.	77
Chapter 6. Upgrade or migrate the virtual appliance	49	Managing the database server configuration	81
Upgrade or migrate from IBM Security Identity Governance and Intelligence version 5.2.2 to version 5.2.3.	49	Managing the PostgreSQL database	86
Upgrading the virtual appliance from a USB Device	50	Transferring connector files to the virtual appliance from an external source	93
Upgrading the IBM Security Identity Governance and Intelligence virtual appliance with firmware update transfer utility	52	Creating a Network Files System (NFS) mount point to access connector files	95
Upgrading a virtual appliance cluster	53	Managing OpenID connect configuration	96
Verify current set of tasks and jobs for the Task Planner module	54	Managing LTPA-based single sign-on configuration	100
Closing campaigns	55	Managing the mail server configuration	102
		Managing custom files	105
		Managing certificates.	107
		Updating the JAVA security policy JAR files	110
		Managing IBM Security Directory Integrator instances	111
		Viewing the update history.	118
		Viewing the licensing.	118
		Managing the firmware settings	118
		Installing a fix pack	119
		Managing the log configuration	120
		Managing JavaCore and core dump files	124
		Viewing the About page information	125
		Managing application interfaces	126

Managing advanced tuning parameters.	128
Configuring for bidirectional languages	133
Managing hosts file	133
Configuring static routes	134
Managing a network file system (NFS)	135
Exporting or importing the configuration settings	139
Configuring the date and time settings	140
Configuring the administrator settings	141
Managing the snapshots.	141
Managing the support files.	144
Configuring system audit events	145
Restarting or shutting down	149

Virtual appliance command-line interface	149
Virtual appliance maintenance.	164
Setting up a secondary virtual appliance for active-passive configuration	164

Chapter 8. Installing and configuring Identity Brokerage Adapters 169

Installing the adapter in the virtual appliance	170
Uninstalling the adapter from the virtual appliance	171

Index 173

Table list

1. Virtual appliance administrators deployment tasks	1	15. Synchronization states table.	68
2. Port numbers	3	16. Directory server configuration details	75
3. Tags to customize the IBM Security Identity Governance and Intelligence Oracle database installation.	10	17. LMI Authentication configuration details	79
4. Database scripts for different environments and access restrictions.	12	18. Options for configuring the Identity data store	82
5. Tags to customize IBM Security Identity Governance and Intelligence DB2 installation .	14	19. PostgreSQL database action items	87
6. Database scripts for different environments and access restrictions	17	20. Necessary information for configuration	97
7. Hardware requirements	32	21. OpenID connect operations	99
8. Synchronization state table	44	22. LTPA-based Single Sign-On Configuration action items	101
9. Schema installation scripts for virtual appliance nodes in an Identity Governance and Intelligence cluster.	45	23. Mail Server Configuration	103
10. Security Identity Governance and Intelligence migration paths	49	24. File tabs and their actions	106
11. Tasks and Jobs collection for IBM Security Identity Governance and Intelligence installation.	54	25. Java Security Policy action items	110
12. Tags to customize the IBM Security Identity Governance and Intelligence Oracle database installation.	56	26. Ports that are open in the firewall.	112
13. Tags to customize the IBM Security Identity Governance and Intelligence DB2 database installation.	58	27. Security Directory Integrator action items	113
14. Virtual appliance administrators maintenance tasks	63	28. Security Directory Integrator property actions	116
		29. Security Directory Integrator adapter actions	117
		30. Available logs to help you diagnose or troubleshoot	120
		31. Core dump file management actions.	124
		32. Application Interfaces action items	127
		33. Advanced tuning parameters options	129
		34. Security protocol operations	129
		35. Security cipher suite operations	130
		36. Security cipher suite operations	131
		37. Advanced tuning parameters	132
		38. Static route actions.	135
		39. Network File System action items.	138
		40. Export or import settings actions	140
		41. Adapter package contents	170

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*, <http://www-969.ibm.com/software/reports/compatibility/clarity/softwareReqsForProduct.html>.

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: <ul style="list-style-type: none">• Installing the Oracle server• Configuring the Oracle server For DB2®: <ul style="list-style-type: none">• Installing the DB2 server• Configuring the DB2 server Installation of database schemas in a high availability environment
(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.	<ul style="list-style-type: none">• 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
<p>For high availability, set up a virtual appliance cluster.</p>	<p>Setting up a virtual appliance cluster</p> <ul style="list-style-type: none"> • Setting up a member node for IBM Security Governance and Intelligence by using the initial configuration wizard • Promoting the secondary node to the primary node • Promoting a member node to the secondary node • Enabling and disabling replication between the primary and secondary nodes • Promoting a member node to the primary node • Removing a node from the cluster • Reconnecting a node into the cluster • Synchronizing a member node with a primary node
<p>Configure the virtual appliance settings.</p>	<ul style="list-style-type: none"> • 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. Software firewall configuration in the virtual appliance

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

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

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

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

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

Table 2 describes a list of available ports that you can use to work with IBM Security Identity Governance and Intelligence virtual appliance:

Table 2. Port numbers

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

Chapter 3. Support for FIPS 140-2 specifications

Identity Governance and Intelligence provides options for using the applicable FIPS 140-2 specifications.

When in FIPS 140-2 mode, IBM Security Identity Governance and Intelligence uses the FIPS 140-2 approved cryptographic provider(s); IBMJCEFIPS (certificate 376) and/or IBMJSSEFIPS (certificate 409) and/or IBM Crypto for C (ICC (certificate 384) for cryptography. The certificates are listed on the NIST web site.

Configuring an application to support US FIPS requires that all the components of this application are in FIPS-enabled mode. To configure IBM Security Identity Governance and Intelligence for FIPS 140-2 mode, you must configure the following:

- The virtual appliance settings. Use the appliance setup wizard that runs the first time that you connect to the virtual console of an unconfigured virtual appliance. This automatically includes the embedded WebSphere® Application Server, the Java™ Runtime Environment (JRE), and the embedded PostgreSQL database. See “Setting up the initial virtual appliance” on page 23.

For the following components, be sure to select the **SSL** option when you configure the connection from the virtual appliance:

- Directory server
- Mail server
- External database server
- LMI authentication from an external user registry
- The SAP system details pane of the FIPS-enabled SAP system in the Access Risk Controls for SAP module, if you plan to work with the Access Risk Controls for SAP module.

This requires that you also create certificates to connect with the FIPS-enabled SAP system.

Important: You cannot enable the system for FIPS on an existing virtual appliance installation. You must install Identity Governance and Intelligence and its components from scratch.

Creating certificates for a FIPS connection with SAP

This section describes the steps that you need to follow to set up Identity Governance and Intelligence to connect with a SAP system over FIPS.

About this task

Before you communicate with a SAP system over FIPS, you must set up Identity Governance and Intelligence. This process involves that you create and export a client certificate and that you import the SAP server certificate into the virtual appliance. After your virtual appliance and the partner SAP system are assigned the matching certificates, you can configure the Access Risk Controls for SAP module to communicate with the SAP system.

Important: If you have a clustered environment, run the complete procedure on the primary node only, and step 7 also on the other nodes of the cluster.

Procedure

1. Follow these prerequisite steps.
 - a. Refer to your SAP administrator to obtain the `sapgenpse` tool and other required files from the SAP system. Copy these files to a temporary directory on the system that hosts your virtual appliance. The files are used to create and handle your certificates.
 - b. On the virtual appliance dashboard, select **Configure > Custom File Management** and upload the files that you saved in the previous step to folder `lib/native/crypto`.
 - c. Retrieve file `libsapcrypto.so` from the `sapgenpse` tool and select **Configure > Custom File Management** on the virtual appliance dashboard to upload it to folder `lib/native`.
 - d. Add the SAP JCO libraries to folder `lib/native` as it is described in SAP Libraries.
 - e. Restart the WebSphere Application Server from the virtual appliance dashboard.
2. Use an ssh session to access the command line interface of the virtual appliance.
3. At the command prompt, enter the following commands:
igi>utilities>arcs_configuration_snc. The **arcs_configuration_snc** command includes the commands that you are about to use to create and manage the certificates.
4. From the **arcs_configuration_snc** prompt, enter the **create_pse_file** command to create the PSE. The Personal Security Environment (PSE) file contains the information needed to create and verify digital signatures and to create or open digital envelopes.

When you enter the command, you are asked the following information:

PSE filename

A name for the file, for example `igiva.pse`. The file is created in the `../lib/native/sec` folder.

PSE PIN

A PIN or passphrase that you need to enter also in the next steps.

Distinguished name of PSE owner

The DN in the form: `CN=common name, OU=organizational unit, O=organization, C=country`.

For example,

```
igiva.example.com:arcs_configuration_snc> create_pse_file
Enter PSE filename: igiva.pse
Enter PSE PIN:
Enter Distinguished name of PSE owner: CN=igiva,ou=security,o=mycompany,c=us
Successfully created PSE file.
igiva.example.com:arcs_configuration_snc>
```

You can select **Configure > Custom File Management** in the virtual appliance dashboard to list the new PSE file in the `lib/native/sec` folder.

5. Export the client certificate of the PSE that you just created.
 - a. From the **arcs_configuration_snc** prompt, enter the **export_client_certificate** command to export to a file the client certificate of the PSE that you just created. For example,

```
igiva.example.com:arcs_configuration_snc> export_client_certificate
Enter PSE filename: igiva.pse
Enter PSE PIN:
```

```
Enter file to hold the client certificate: client_igiva.crt
Successfully exported client certificate.
igiva.example.com:arcs_configuration_snc>
```

- b. Select **Configure > Custom File Management** in the virtual appliance dashboard to download the client certificate file from the `lib/native/crypto` folder onto a temporary folder on your system.

Important: You will need to enter the contents of this file in the **X509CERT** field of the **Configure > SAP System** pane in the Access Risk Controls for SAP module. To do this, open the file with an editor and copy and paste its entire contents into the **X509CERT** field. Copy the contents as a single line with no intermediate spaces.

- c. On the SAP server, import the client certificate to the server PSE. You can use the STRUST transaction to import the client certificate.
6. Import the SAP server certificate to the client PSE on the virtual appliance.
 - a. From the SAP server, export the server certificate to a temporary folder on the system that hosts your virtual appliance. You can use the STRUST transaction to export the server certificate.
 - b. Select **Configure > Custom File Management** in the virtual appliance dashboard to upload the SAP server certificate to the `lib/native/crypto` folder.
 - c. From the **arcs_configuration_snc** prompt, enter the **import_sap_server_certificate** command to import the SAP server certificate to the client PSE on the virtual appliance . For example,

```
igiva.example.com:arcs_configuration_snc> import_sap_server_certificate
Enter PSE filename: igiva.pse
Enter PSE PIN:
Enter file containing sap server certificate: sap_server.crt
Successfully imported SAP Server Certificate to Client PSE.
igiva.example.com:arcs_configuration_snc>
```
 7. From the **arcs_configuration_snc** prompt, enter the **create_credv2_file** command to create the `cred_v2` credentials file. This file is used to securely give your PSE file (in this example `igiva.pse`) access to the Personal Security Environment without providing the PSE PIN.

For example,

```
igiva.example.com:arcs_configuration_snc> create_credv2_file
Enter PSE filename: igiva.pse
Enter PSE PIN:
Successfully created Cred_v2 file.
igiva.example.com:arcs_configuration_snc>
```

The file is saved in the `lib/native/sec` folder.

Note: If you have a clustered environment, synchronize the nodes and run this step on every node of the cluster.

8. Restart the WebSphere Application Server from the virtual appliance dashboard.
9. On the SAP server, map the x.509 certificates that were created for the user accounts for Identity Governance and Intelligence.
 - a. Start transaction SM30 and enter the VSNCSYSACL view. This view is used to restrict the SNC RFC Connections by an Access Control List (ACL). When an alert window is displayed, click the **right** symbol.
 - b. Choose **E** for the Type of ACL entry.
 - c. Enter the System ID and the SNC name for Identity Governance and Intelligence. Do not forget to insert **p:** before the Distinguished Name.

- d. Save the entry.
10. On the SAP server, map the X.509 certificate to an ABAP user for Identity Governance and Intelligence.
 - a. Start transaction SM30, enter the VUSREXTID view, and click **Maintain**. Use this view to map the Distinguished Name from the X.509 Certificate and the ABAP User.
 - b. Choose the Distinguished Name for the External ID type.
 - c. Create a new entry and activate it.

Chapter 4. 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 10 and “Configuring the DB2 server” on page 13. The default password is `ideas`.

Attention:

- Complete the procedure before you start the schema installation steps.
- Do not use any of these special characters in the password:
`$ ~ @ # () - _ { } .`

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 server, such as the `SCRIPT` directory.
`SEC_IDNTY_GVN_INTL_xxx_V5.2.3_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 V5.2.3 Database Installation Scripts file you are using.

2. Open the following file with an editor:

```
UNIX  SCRIPT/DB_INSTALLATION/IGI_5_2_3_INSTALLATION/00-COMMON/01-  
COMMON.sql
```

Windows

```
SCRIPT\DB_INSTALLATION\IGI_5_2_3_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"` The new password is enclosed within double quotation marks that are enclosed within single quotation marks on Oracle.
 - `' 'new_password' '` The new password is 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 that is 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 3.
- 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 9.
- 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 5.2.3, 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 3. 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

Table 3. Tags to customize the IBM Security Identity Governance and Intelligence Oracle database installation (continued)

Tags	Description
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>
The <password> is the administrative password that was supplied when the Oracle database was created.
2. Unpack the following compressed file from the product package image or DVD:
SEC_IDNTY_GVN_INTL_xxx_V5.2.3_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 V5.2.3 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 4. Database scripts for different environments and access restrictions.

File name	Description
01-FULL-TBLS_USER_AND_OBJ-CREATION.sql	Interactive full DB creation.
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_3_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 V5.2.3 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 install the DB2 server.
- 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 10.5.0.8.
- 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 9.
- Understand and comply with the Hardware and software requirements.

About this task

Use the following tags to customize the DB2 database.

Table 5. Tags to customize IBM Security Identity Governance and Intelligence DB2 installation

Tags	Description
DBServer	DB2 Server IP address or FQDN name
DBPort	DB2 instance port Important: Make sure that you know what the actual port number is. You can verify it at <code>/etc/services</code> .
DB_Install_Location	The folder where DB2 is installed. For example, <code>C:\DB2\IBM</code> or <code>/opt/ibm/db2/V10.5</code> .
IGI_DB	DB2 database name
INSTANCE_OWNER	DB2 instance owner of the database instance
PASSWORD	DB2 instance owner password
FQ_IGI_DB	<code><DBServer>:<DBPort>/<IGI_DB></code>
TABLESPACE_SIZE	Identity Governance and Intelligence table space size (small, medium, or large)
TABLESPACE_PATH	The location of the database

In some of the following steps, you must identify the product media type that you are using.

CMP IBM Security Identity Governance Compliance.

ANL IBM Security Identity Governance Analytics.

LFC IBM Security Identity Governance Lifecycle.

IEE IBM Security Identity Governance and Intelligence Enterprise Edition.

Procedure

1. Log in as the instance owner.

On Windows, the instance owner must be a member of the DB2ADMNS and Administrators groups. If you need to create an instance owner for IBM Security Identity Governance and Intelligence virtual appliance on Windows, take the following steps:

- a. Add the instance owner as user `igiinst` with password `ideas`. Enter the following command in a Windows command prompt:

```
net user igiinst ideas /add
```

- b. Add `igiinst` to the DB2ADMNS and Administrators groups. Enter the following commands in a Windows command prompt:

```
net localgroup "DB2ADMNS" "igiinst" /add  
net localgroup "Administrators" "igiinst" /add
```

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 one of the following commands to create a database instance.

For UNIX or Linux systems

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

For Windows systems, open the DB2 Command Window

```
DB2_Install_Location/SQLLIB/BIN/db2icrt -u igiinst igiinst
```

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

- d. Verify the actual port number of your instance. Run the **db2 get dbm cfg** command. For example,

```
db2 get dbm cfg | grep SVCENAME
-> (output) TCP/IP Service name (SVCENAME) = 50000.
```

The port is 50000. You can also look for the service name of the instance in the /etc/services directory to find the port that is associated with the instance.

- e. Run the following commands to set up the instance.

For UNIX or Linux systems

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

For Windows systems, open the DB2 Command Window

```
Set DB2INSTANCE=igiinst
db2 update dbm cfg using SVCENAME <DBPort_value>
db2set DB2COMM=tcPIP
db2set -all DB2COMM
db2start
```

Note: For Windows users, the Set DB2INSTANCE=igiinst is needed for the instance owner to have the system roles to run various commands such as **create schema**.

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_V5.2.3_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 V5.2.3 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 to remove hidden Microsoft Windows characters.
 - 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_V5.2.3_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 V5.2.3 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.

Note: To disable password policies, click **Start > Administrative Tools > Local Security Policy**. Enter the administrative password and then click **Account Policies > Password**. Disable any restrictive password policies. Then, run the **win_create_users.bat** command to create the users.

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_V5.2.3_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 V5.2.3 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'
```

If 'NO_DEFAULT' is specified as the value for **DEFINE TABLESPACE_PATH** and **DEFINE TABLESPACE_SIZE**, you are prompted for values when the scripts are run. The values for **DEFINE TABLESPACE_SIZE** are specified in the following list.

- 'M' for medium
- 'L' for large
- 'S' for small

For example,

```
--xxx.xxx.xxx.xxx - DB2 Server IP address or DNS name
--yyyyy           - DB2 Server DATABASE port
--zzz            - DB2 Server DATABASE name
DEFINE ISIG_DB = 1.23.456.123:50000/IGIDB
DEFINE TABLESPACE_PATH = '/home/db2inst1/db2inst1/NODE0000/IGIDB'
DEFINE TABLESPACE_SIZE = 'M'
```

- 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 6. Database scripts for different environments and access restrictions

File name	Description
01-FULL-TBLS_USER_AND_OBJ-CREATION.sql	Interactive full database creation.
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/sql1lib/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_3_Installation.log
```

Windows systems

```
<SCRIPT>\DB_INSTALLATION\IGI_V5_2_3_Installation.log
```

g. If 'NO_DEFAULT' is specified in the login.sql file, you are prompted for a path when the script is run. 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.

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, dcom.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 dcom.ldif
```

For example,

```
/opt/IBM/ldap/V6.4/bin/idsldapadd -h ldapserver  
-p 389 -D cn=root -w password -p port  
-f dcom.ldif
```

Chapter 5. 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` image.
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 provision at least three network interfaces to set up the virtual machine. Only two interfaces are needed for normal operations M1 and P.1. The M.2 interface is used for high availability.

First interface (eth0)

M.1 is the first management interface (LMI).

Optional: Second interface (eth1)

M.2 is the second management interface (LMI). It is used for high availability.

Third interface (eth2)

P.1 is the first application interface for the Identity Governance and Intelligence application.

- 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. Click **Next**.
9. On the Specify Advanced Options window, accept the default **Virtual Device Node**. Click **Next**.
10. Click **Finish** on the Add Hardware window.
11. Select **Connect at power on** on the Virtual Machine Properties window.
12. Click **Finish** on the Virtual Machine Properties window.
13. 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. Select the type of media that you want the virtual drive to access. For example, select **Use Datastore ISO File**.
 - e. Browse to the data store location where you uploaded the .iso file.
 - 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” on page 23.

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.”

Important: This note applies, if you are using an external database only. 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.

Note: The following languages are not supported by the appliance setup wizard:

- Arabic
- Dutch
- Hebrew
- Turkish

```
Software License Agreement
Currently selected language: English
1: Select language for license display
2: Read IBM terms
3: Read non-IBM terms
4: Proceed 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. Select whether or not to enable FIPS 140-2 mode

```
FIPS 140-2 Mode Configuration
```

You must enable FIPS mode in order to comply with FIPS 140-2 and NIST 800131a.

If you select to enable FIPS mode, appliance will be rebooted immediately to perform FIPS power-up integrity checks.

Do not choose to enable FIPS mode without reading the FIPS section in the user guide.

If you choose to enable FIPS mode now, you cannot disable it later without reinstalling the appliance.

FIPS 140-2 Mode is not enabled.

- 1: Enable FIPS 140-2 Mode
- x: Exit
- p: Previous screen
- n: Next screen

Select option: 1

```
FIPS 140-2 Configuration
```

```
Enable FIPS 140-2 mode?
```

- 1: yes
- 2: no

Enter index:

If you enter 2, the wizard proceeds to step 5. If you enter 1, the wizard asks for your confirmation.

```
You have selected to enable FIPS mode. The appliance will now reboot to perform
the FIPS integrity checks.
When appliance comes back up, you will need to login as admin user to complete
the setup.
Enter 'YES' to confirm:
```


After you enter YES to confirm, FIPS is enabled in the background and the system reboots.

After you log in, you are again prompted to accept the Software License Agreement (step 3). The wizard then proceeds to step 5.

5. 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
```

6. 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.

7. Configure network interface M.1 with the IP address, subnet mask, and default gateway. If you are creating an environment with high availability, you must also configure network interface M.2. The M.2 interface is the backup for the Local Management Interface (LMI). The procedure is similar to configuring M.1 except that the address, subnet mask, and default gateway are different.

```

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

```

8. 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

```

9. 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

```

- Review the summary of configuration details. If you chose to enable FIPS mode, check that the summary returns the following message:

FIPS 140-2 Mode is enabled.

Note: If necessary, record the details of the assigned IP address, DNS, and host name of the virtual appliance.

- 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 33.

XenServer support

The IBM Security Identity Governance and Intelligence virtual appliance can be installed on a XenServer hypervisor, Version 6.5.

When the virtual appliance is installed on XenServer, it runs in a paravirtualization (PV) mode rather than hardware assisted virtualization (HVM) mode.

The Identity Governance and Intelligence virtual appliance for XenServer is distributed as a pre-installed disk image of the appliance in Virtual Hard Disk (VHD) format. Standard installation ISO images cannot be used due to some restrictions with XenServer.

To deploy the VHD appliance image to XenServer, use the XenCenter console.

Installing the virtual appliance by using XenCenter

Import the VHD image to XenServer with XenCenter to install the virtual appliance.

Before you begin

Make sure that you have the following prerequisites:

- A functional XenServer environment, which is used as the hypervisor to host the VHD image.
- A configured XenCenter installation, which is used to deploy the VHD image.

Procedure

1. In the XenCenter console, expand the XenCenter icon on the left.
2. Right-click the attached hypervisor and select **Import**.
3. In the Import Source window, do the following steps.
 - a. Click **Browse**.
 - b. Select the VHD image to be imported and click **Open**.
 - c. Click **Next**.
4. In the VM Definition window, do the following steps.
 - a. Specify the name, number of CPUs, and memory of the virtual machine.

Note: For the detailed system requirements, see **Hardware and software requirements** in, Chapter 1, "Overview," on page 1.

- b. Click **Next**.
5. In the Location window, do the following steps.
 - a. Select the destination hypervisor from the drop-down list on the right.
 - b. Click **Next**.
 6. In the Storage window, do the following steps.
 - a. Select **Place imported virtual disks onto specified target SRs**.
 - b. Click **Next**.
 7. In the Networking window, do the following steps.
 - a. Select the network to be used for the first management interface.
 - b. Click **Next**.
 8. In the OS Fixup Settings window, do the following steps.
 - a. Select **Don't use Operating System Fixup**.
 - b. Click **Next**.
 9. In the Transfer VM Settings window, do the following steps.
 - a. Specify the settings to suit your network environment.

Note: A valid IP address, subnet, and gateway are required.

- b. Click **Next**.
10. In the Finish window, click **Finish** to start the import.

Note: The import operation might take a considerable amount of time to complete. You can click the **Logs** tab to check the progress of the import.

11. When the import is complete, run the following commands on the XenServer console to set the image to a paravirtualization mode.

```
xe vm-list (to get the uuid for the VM)
xe vm-param-set uuid=<vm uuid> HVM-boot-policy=""
xe vm-param-set uuid=<vm uuid> PV-bootloader=pygrub
xe vm-disk-list (to get the uuid for the disk - VBD entry)
xe vbd-param-set uuid=<disk uuid> bootable=true
```

For example

```
[root@xenserver ~]# xe vm-list name-label="autodeploy"
uuid ( RO)           : 6288a6a6-8577-5444-6ed5-46d2a097be54
  name-label ( RW)   : autodeploy
  power-state ( RO)  : halted
[root@xenserver ~]# xe vm-param-set uuid=6288a6a6-8577-5444-6ed5-46d2a097be54 HVM-boot-policy=""
[root@xenserver ~]# xe vm-param-set uuid=6288a6a6-8577-5444-6ed5-46d2a097be54 PV-bootloader=pygrub
[root@xenserver ~]# xe vm-disk-list vm="autodeploy"
Disk 0 VBD:
uuid ( RO)           : b0d08251-7f08-8b4e-3913-e71052dd7b13
  vm-name-label ( RO) : autodeploy
  userdevice ( RW)   : xvda

Disk 0 VDI:
uuid ( RO)           : 8dfa6027-1ef3-408b-a9ed-efa751d41720
  name-label ( RW)   : amapp-template_vdi
  sr-name-label ( RO) : Local storage
  virtual-size ( RO) : 107376279552

[root@xenserver ~]# xe vbd-param-set uuid=b0d08251-7f08-8b4e-3913-e71052dd7b13 bootable=true
```

12. Start the imported virtual machine.

Note: At least three network interfaces must be configured in order for the virtual appliance to start. Sometimes the XenCenter must be restarted before the new virtual appliance can be started correctly.

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
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.

KVM support

The IBM Security Identity Governance and Intelligence virtual appliance can be installed on a Kernel-based Virtual Machine (KVM).

The Identity Governance and Intelligence virtual appliance for KVM is distributed as a preinstalled disk image of the virtual appliance in the `.iso` format.

To deploy the `.iso` virtual appliance image to KVM, use the KVM console.

Hardware requirements

Table 7. Hardware requirements

Requirement	Value
CPU speed	3154 MHz
Disk space	500 GB hard disk space
RAM	64 GB system memory

Software requirements

- RHEL 7.0 64-bit operating system with enabled support for virtualization.
- A network bridge is required to set up network interface for the KVMs.

Installing the virtual appliance with KVM

Follow these steps to install the virtual appliance .iso image on a Kernel-based Virtual Machine.

Procedure

1. On your operating system command line, run the **virt-manager** command to open the Virtual Machine Manager.
2. Click **Create a New Virtual Machine**.
3. On the wizard, enter a name for the virtual machine.
4. Select **Local install media (ISO image or CDROM)**.
5. Click **Forward**.
6. Select **Use ISO image** and click **Browse** to select the product ISO file.
7. Select the operating system as Linux with Version Generic 2.6.x kernel.
8. Click **Forward**.
9. Enter the memory size. For example, 10240 MB.
10. Set the number of CPUs. For example, 8.
11. Click **Forward**.
12. Enter the disk size of the virtual machine. For example, 50 GB.
13. Click **Forward**.
14. Select the network bridge.
15. Select **Customize configuration before install**.
16. Click **Finish**.
17. Click **Add Hardware**.
18. Select **Network**.
19. Select the network bridge and click **Finish**.
20. Click **Add Hardware** again.
21. Select **Network**.
22. Select the network bridge and click **Finish**.
23. On the KVM console, follow the steps to complete the installation.
24. Press Enter after the disk partitioning and installation is complete. Wait for the appliance login prompt to be displayed.
25. Provide the following user credentials when the system restarts.
 - The **Unconfigured login** is admin.
 - The **Password** is admin.

What to do next

Set up the initial virtual appliance. See “Setting up the initial virtual appliance” on page 23.

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://igival.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. <ol style="list-style-type: none"> 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 35. Click response file to download the latest sample response file. 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**.
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. You can download the latest sample response file from the Mode Selection pane in the "Initial configuration" wizard. After you update the response file with the correct values, upload the response file to configure the virtual appliance in the advanced configuration mode.

For more information about advanced configuration mode, see "Setting up a stand-alone or primary node for IBM Security Identity Governance and Intelligence with the initial configuration wizard" on page 33.

```
#####
#
# 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
# 4) PG_DB          - Doesn't require any input from user.
#
igi.datastore.dbType=<IBM_DB or ORACLE_DB or ORACLE_DB_CUSTOM or PG_DB>
igi.datastore.hostName=<hostname>
igi.datastore.port=50000
igi.datastore.connection.type=<ssl or non-ssl>
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.connection.type=<ssl or non-ssl>
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
igi.mail.connection.type=<ssl or non-ssl>

#
# Application Interface configuration properties
#
igi.application.interface.FQDN=<FQDN for the interface>
igi.application.interface.gateway=<gateway 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>

```

Note: You can choose to configure SSL service for three components:

DB igi.datastore.connection.type=**ssl**

Mail Server

 igi.mail.connection.type=**ssl**

Directory Server

 igi.ldap.connection.type=**ssl**

If you choose to configure the SSL service, a confirmation panel for accepting a digital certificate is shown (for every component that is configured for SSL service).

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.

Note: If you did not configure M.2 when you set up the virtual appliance, use the **management interface set** command to configure it.

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 37.

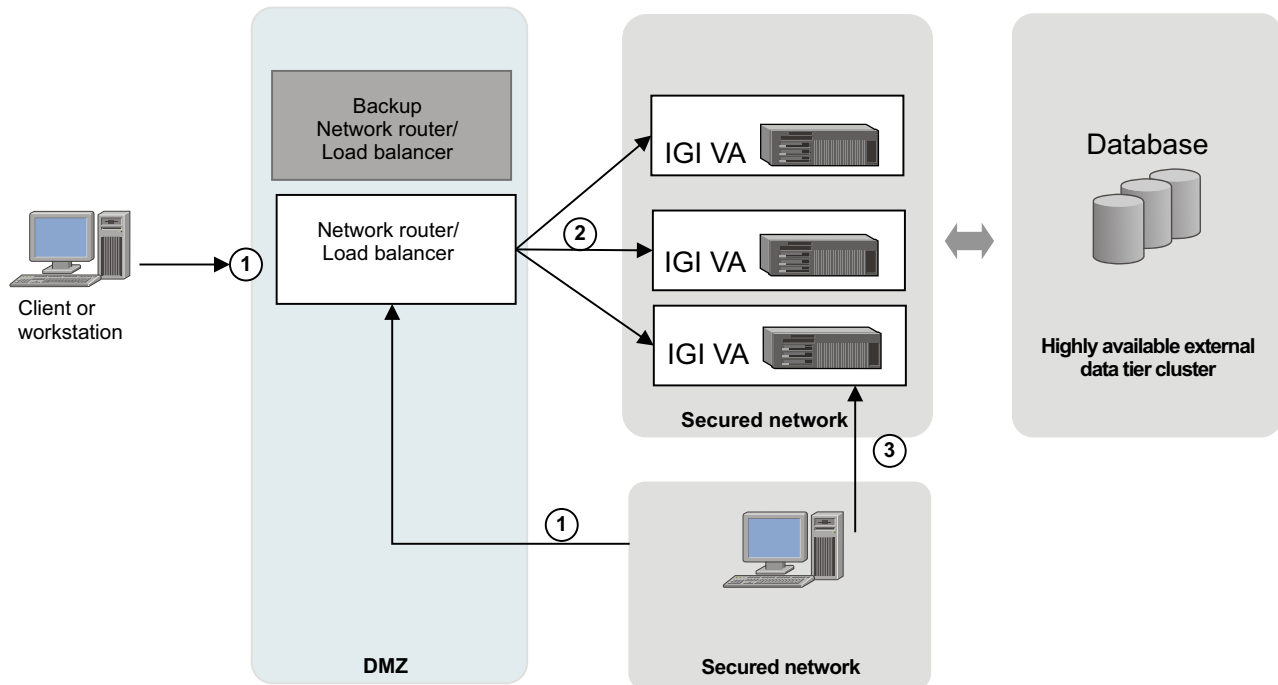


Figure 1. Deployment diagram of a typical load balancer in a customer environment

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 37, 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

“Setting up the initial virtual appliance” on page 23.

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.

Note: The first member node that you create is assigned the role of a secondary node.

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, `isigval.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@local`.
 - c. Type the password in the **Primary node administrator password** field. This is the password that you defined during the virtual appliance setup on the primary node.
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.

Note: If the connection fails, check that the ciphers and protocols on the primary and other nodes are the same. They must use the same ciphers and protocols. See “Managing advanced tuning parameters” on page 128.

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” on page 126.
8. Optional: If the primary node is configured with the internal Postgres database, you can set up replication between the primary and secondary nodes. Click the **Enable replication** check box. This option is available for the first member node only. If you do not set up replication now, you can enable it later from the Postgres Management page.
9. 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.
10. Optional: To review or edit the data in the **Connect to Primary** tab, click **Previous page**.
11. 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.
- If failures occur, click the **Click here** link to restart the configuration process.

Promoting the secondary node to the primary node

If the primary node becomes unavailable, use the Cluster Node Configuration page to change a secondary node to the 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 promote the secondary node as the primary node. You might also want to change the secondary node to the 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** on the secondary node, click **Configure > Manage Cluster > Cluster Node Configuration**.
2. Select the secondary node.
3. Click **Promote**.
4. Click **Yes** to confirm the changes.

Promoting a member node to the secondary node

The first member node that you create in the cluster is automatically created as the secondary node. If the secondary node becomes unavailable for some reason, use the Cluster Node Configuration page to promote a member node as the secondary node in the IBM Security Identity Governance and Intelligence virtual appliance.

Before you begin

No active secondary node must exist in this cluster.

About this task

The initial secondary node is the only automatic promotion. If you need to replace the secondary node, whether for maintenance or some other reason, it is a manual process.

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** on the primary node, click **Configure > Manage Cluster > Cluster Node Configuration**.
2. Select the member node.
3. Click **Promote**.

4. Click **Yes** to confirm the changes. The role of the node is change to secondary.

What to do next

Create a slave Postgres database on the secondary node. See “Enabling and disabling replication between the primary and secondary nodes.”

Enabling and disabling replication between the primary and secondary nodes

This task applies only if the cluster environment is using the internal Postgres database. You can enable replication to back up the database on the primary node with the database on the secondary node.

About this task

If you did not enable replication when you created the first member node, which was assigned the role of secondary node, you can enable it with this procedure. Replication must be initiated from the secondary node.

Procedure

1. From the top-level menu of the secondary node **Appliance Dashboard**, click **Configure > Postgres Management**. The **Postgres Management** table displays the name, the NFS enabled status, state, and role of the databases on the primary node.
2. Select the Postgres database that is on the secondary node.
3. Click **Manage > Replication > Configure replication**.
4. Click **Yes** on the confirmation window. If it was not already running, the master database is started. The secondary database is displayed with the database role of slave.
5. To stop replication, select the database that has the role of slave.
 - a. Click **Menu > Replication > Unconfigure replication**.
 - b. Click **Yes** on the confirmation window. Replication is stopped and the database is removed from the **Postgres Management** table.

Promoting a member node to the primary node

If the primary and secondary nodes become unavailable for some reason, use the Cluster Node Configuration page to promote a member node as the primary node in the IBM Security Identity Governance and Intelligence virtual appliance.

Before you begin

No active primary or secondary node must exist in this cluster.

About this task

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** on the member node that you want to promote, click **Configure > Manage Cluster > Cluster Node Configuration**.
2. Select the member node.
3. Click **Promote**.

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 “Promoting a member node to the primary node” on page 41. 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 8. 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 42.
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

- From the top-level menu of the **Appliance Dashboard**, click **Configure > Manage Cluster > Cluster Node Configuration**.
- 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.
- Optional: Click **Refresh** to display the recently updated data.

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_V5.2.2_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 9. 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 on 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 that is 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 to 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 $00n$ 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.

Recovering from a primary node failure

If the primary node becomes unavailable, use this procedure to recover your system.

About this task

Procedure

1. Remove the primary node from the cluster. See “Removing a node from the cluster” on page 42.
2. If you are using a Postgres database, promote the slave database to be the master database. This step applies to a cluster environment that uses the Postgres database only.
 - a. On the secondary node, click **Configure > Postgres Management**.
 - b. Select the slave database and click **Manage > Promote**.
 - c. Click **Yes** to confirm that you want to promote the database to master.
3. Promote the secondary node to become the primary node. See “Promoting the secondary node to the primary node” on page 40.
4. Optional: Promote a member node to be a secondary node. See “Promoting a member node to the secondary node” on page 40.
5. Optional: Enable replication between the Postgres databases. This step applies to a cluster environment that uses the Postgres database only. See “Enabling and disabling replication between the primary and secondary nodes” on page 41.

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” on page 46 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.

Synchronizing data after the installation

After the first installation, all schedulers are listed with the  **Inconsistent Task** icon.

About this task

Procedure

1. Log on to the Administration Console. If you are logging on to Administration Console 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 pane.
5. In the same pane, from the **Actions** menu, select **Synchronize**.
6. Repeat steps 4 and 5 for each scheduler that is listed.

Chapter 6. Upgrade or migrate the virtual appliance

Migration for IBM Security Identity Governance and Intelligence consists of two parts. You must first upgrade the database schema and then the product firmware. Migration must be done sequentially, from one release to the next.

Choose your installed version to determine your migration path.

Table 10. Security Identity Governance and Intelligence migration paths

From version	To version	Instructions
5.1.1	5.2	See Migrating IBM Security Identity Governance V5.1.1 Fix Pack 1 to IBM Security Identity Governance and Intelligence V5.2.0 at http://www.ibm.com/support/knowledgecenter/SSGHJR_5.2.0/com.ibm.igi.doc/installing/cpt/c_migrate_isig.html . Note: IBM Security Identity Governance Version 5.1.1 required a single IP address. For IBM Security Identity Governance and Intelligence Version 5.2, a second IP address is required. Ensure that you have two IP addresses available.
5.2	5.2.1	See Upgrade or migrate the virtual appliance to IBM Security Identity Governance and Intelligence Version 5.2.1 at http://www.ibm.com/support/knowledgecenter/SSGHJR_5.2.1/com.ibm.igi.doc/installing/cpt/c_migrate_isig.html .
5.2.1	5.2.2	See Upgrade or migrate from version 5.2.1 to 5.2.2.
5.2.2	5.2.3	See "Upgrade or migrate from IBM Security Identity Governance and Intelligence version 5.2.2 to version 5.2.3."

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 Identity Governance and Intelligence.

Important: Before you upgrade to version 5.2.3, be aware that the Target Administration Console is replaced by the Enterprise Connectors module. If you have Identity Brokerage targets, you must migrate them to the Enterprise Connectors module. Read Migrating Identity Brokerage targets to the Enterprise Connectors module before you start to upgrade.

Upgrade or migrate from IBM Security Identity Governance and Intelligence version 5.2.2 to version 5.2.3

Migration for IBM Security Identity Governance and Intelligence must be done sequentially. You can migrate directly to version 5.2.3 from version 5.2.2 only. You can use either a USB device or a firmware update transfer utility to upgrade the virtual appliance.

Ensure that your system is at version 5.2.2 before you begin migration.

If you use a DB2 or Oracle database server, you must migrate the database schema before you migrate the virtual appliance. Follow the procedure described in "Updating the DB2 database for V5.2.3" on page 58 or in "Updating the Oracle

database for V5.2.3” on page 56 to migrate the Identity Governance and Intelligence database. The PostgreSQL database is automatically migrated with the virtual appliance.

Important: Before you upgrade to version 5.2.3, be aware that the Target Administration Console is replaced by the Enterprise Connectors module. If you have Identity Brokerage targets, you must migrate them to the Enterprise Connectors module. Read Migrating Identity Brokerage targets to the Enterprise Connectors module before you start to upgrade.

There is also an impact on your previous connector configurations. See Migrating connectors to Version 5.2.3 after you run the upgrade.

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, take these steps:

- Back up your data tier, which is all the databases and the directory server.
- Migrate the database schema, if you use a DB2 or Oracle database server. See “Updating the DB2 database for V5.2.3” on page 58 or “Updating the Oracle database for V5.2.3” on page 56 for reference.

Note: JVM properties are not upgraded during the virtual appliance upgrade. Similarly, other configurations are not carried forward such as:

- Logging configuration
- Import/export settings
- Snapshots
- Support files
- Others

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 version 5.2.3 package from IBM Fix Central and extract the *.pkg build to a location of your choice on the virtual system. The package name is 5.2.3.0-ISS-SIGI-VA-FP0000.
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. Configure the application interface gateway as requested by the notification section.
9. Restart the virtual appliance to complete the upgrade process.

Note: The Event Log might list the following message:

```
The null operator, null, uploaded the igi_5.2.3.0_20170601_0222.pkg
file.
```

The message is incorrect. You can ignore it.

10. 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.

11. Optional: If you were using an LTPA key for single sign-on in the previous version, you must generate and export it again to the other systems with which you were sharing it.

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

Another option for updating the IBM Security Identity Governance and Intelligence virtual appliance is to use the firmware update transfer utility. Starting at firmware release 5.2.0.1, firmware (.pkg) files can be transferred with the Java utility. You can use this utility in place of a USB device to update the Identity Governance and Intelligence virtual appliance.

Before you begin

Migrate the database schema, if you use a DB2 or Oracle database server. See “Updating the DB2 database for V5.2.3” on page 58 or “Updating the Oracle database for V5.2.3” on page 56 for reference.

You need the appropriate compressed file, such as the 5.2.3.0-ISS-SIGI-VA-FP0000 file. Go to IBM Fix Central to determine the file name and to download the file. This compressed file contains the following files.

- The firmware update .pkg file.
- The new database schemas for DB2 and Oracle (DBupdate.zip).
- The Java Utility .jar file (File Upload.jar)
- 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 readme file.

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.

Note the location where you stored these files. You need the path for the command in the next step.

5. Run the following Java command to upload the .pkg file.

Usage

```
java -jar FileUpload.jar <Hostname:PORT> <AdminId>  
<AdminPassword> <Truststore Filepath> <Truststore Password>  
<Absolute path to pkg file> <Protocol version of lmi>
```

Hostname

The host name or the IP address of the virtual appliance host.

Port The port used to connect to the virtual appliance.

Admin ID
The administrator ID to log in to the virtual appliance.

Admin Password
The administrator's password.

Truststore Filepath
The path to the JKS file.

Truststore Password
The password for the JKS file.

AbsolutePathTo_pkg_file
The absolute path to the file that was downloaded.

Protocol version of lmi
The protocol version of LMI. You can find the protocol version in the dashboard of the virtual appliance that you are upgrading from. Go to **Manage > Advanced Tuning Parameters > lmi.security.protocol**.

Example

```
java -jar FileUpload.jar igiva.in.ibm.com:9443 admin admin /work/temptrust.jks WebAS  
/Downloads/5.2.3.0-ISS-SIGI-VA-FP0000.pkg TLS
```

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. Be sure to restart the browser session before you start the Web console.

Note: The Event Log might list the following message:

```
The null operator, null, uploaded the igi_5.2.3.0_20170601_0222.pkg  
file.
```

The message is incorrect. You can ignore it.

9. Optional: If you were using an LTPA key for single sign-on in the previous version, you must generate and export it again to the other systems with which you were sharing it.

Upgrading a virtual appliance cluster

Use this procedure to upgrade a virtual appliance cluster from IBM Security Identity Governance and Intelligence Version 5.2.2 to Version 5.2.3.

About this task

You can upgrade each node individually with either the firmware upgrade utility or a USB device. With either of these methods, the roles of the nodes remain the same. The primary node is upgraded as the primary node in the cluster. Member

nodes are upgraded as member nodes. IBM Security Identity Governance and Intelligence Version 5.2.3 supports secondary nodes. To promote a member node to a secondary node, see “Promoting a member node to the secondary node” on page 40.

Procedure

1. Select the primary node in the cluster and upgrade it to Version 5.2.3 by using the firmware upgrade utility. See “Upgrading the IBM Security Identity Governance and Intelligence virtual appliance with firmware update transfer utility” on page 52. This node becomes the primary node in the new cluster.
2. Use the same procedure to upgrade a member node.
3. Repeat Step 2 for each node that you want to upgrade to the cluster.

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 the previous version.
- The product jobs and tasks that were possibly renamed.

Product jobs and tasks must not be modified. If for some reason, you need to rename a product jobs or task, use the precautions described in Customizing system tasks and jobs.

Table 11 lists the entire set of tasks and jobs.

Table 11. Tasks and Jobs collection for IBM Security Identity Governance and Intelligence installation

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

Table 11. 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 database for V5.2.3

If IBM Security Identity Governance and Intelligence is connected to an Oracle database, you must update the database by configuring it for the new version of Identity Governance and Intelligence.

Before you begin

Before you begin, make sure that the following prerequisites are in place:

- The Oracle Server version 12c must be installed. It is the minimum version level that is required for updating to IBM Security Identity Governance and Intelligence V5.2.3.
- The migration script can be launched directly on the server that hosts the Oracle DBMS or on another computer where the Oracle Client is installed.
- You must know the common database parameters such as the IP address, server port, and SID.

About this task

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

Table 12. 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 database 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_V5.2.3_DT_IN.zip
- SEC_IDNTY_GVN_INTL_ANL_V5.2.3_DT_IN.zip
- SEC_IDNTY_GVN_INTL_LFC_V5.2.3_DT_IN.zip
- SEC_IDNTY_GVN_INTL_IEE_V5.2.3_DT_IN.zip

You find them in the DBupdate.zip file that is included in the 5.2.3.0-ISS-SIGI-VA-FP0000 package in IBM Fix Central.

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. Browse to the tnsnames.ora file. For example,
oracle_home/db/network/admin
 - b. Edit the file in a text editor such as **vi** or Notepad.
 - c. 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 database user has write permission to access the log file output:


```
chmod -R 777 *
```
3. Set the ORACLE_HOME variable in accordance with your specific Oracle client or server installation. All the next steps in the procedure assume that the sqlplus executable is located in the <ORACLE_HOME>/bin directory. Enter the following command to connect to the database and to check that the configuration works:
 - On UNIX/Linux:


```
$ORACLE_HOME/bin/sqlplus system/<password>@<IgiSID>
```
 - On Windows:


```
%ORACLE_HOME%\bin\sqlplus system/<password>@<IgiSID>
```

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

```
exit
```

4. Configure the oracle_update.sh or oracle_update.bat file.
 - a. Locate the folder that contains the oracle_update file.


```
cd <your_path>/<UPDSCRIPTDIR>/oracle/migration
```
 - b. Open the oracle_update file with a text editor.

- c. Modify the **ORACLE_BASE** and **ORACLE_HOME** variables according to your installation.
These variables are necessary for **sqlplus** to work.
 - d. Modify the **ORACLE_SERVER** variable with the value of *IgiSID* previously configured in the `tnsnames.ora` file.
 - e. If you changed the default product password from `ideas`, change it in the `sqlplus` commands as well.
5. Connect as the Oracle instance owner (for example, `oracle`), run the update script, and record the results in the log file.

On UNIX and Linux systems:

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

On Windows systems:

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

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.

Updating the DB2 database for V5.2.3

If IBM Security Identity Governance and Intelligence is connected to a DB2 database, you must update the database by configuring it for the new version of Identity Governance and Intelligence.

Before you begin

Before you begin, make sure that the following prerequisites are in place:

- The DB2 Server, Version 10.5.0, Fix Pack 8, must be installed. It is the minimum version level that is required to update to IBM Security Identity Governance and Intelligence V5.2.3.
- The DB2 Client must be installed.
- You must know the common database parameters such as the IP address, server port, and SID.

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

Tags	Description
DBServer	DB2 Server IP address or DNS name.

Table 13. Tags to customize the IBM Security Identity Governance and Intelligence DB2 database installation (continued)

Tags	Description
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_V5.2.3_DT_IN_.zip
- SEC_IDNTY_GVN_INTL_ANL_V5.2.3_DT_IN_.zip
- SEC_IDNTY_GVN_INTL_LFC_V5.2.3_DT_IN_.zip
- SEC_IDNTY_GVN_INTL_IEE_V5.2.3_DT_IN_.zip

You find them in the DBupdate.zip file that is included in the 5.2.3.0-ISS-SIGI-VA-FP0000 package in IBM Fix Central.

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 clppplus to work.
 - c. Modify the **DB2_SERVER** variable with the value of *FQ_IGI_DB*, where *FQ_IGI_DB* is:

```
<DBServer>:<DBPort>/<IGI_DB>
```
 - d. If you changed the default product password from ideas, change it in the clppplus commands as well.

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


On UNIX and Linux systems:

```
dos2unix db2_update.sh  
./db2_update.sh > upgrade.log
```

On Windows systems:

```
db2_update.bat > upgrade.log
```

Synchronizing data

After you close all the campaigns, all schedulers are listed with the  **Inconsistent Task** icon. Resynchronize the schedulers if this installation is 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 > Synchronize**.
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 **SystemHierarchyAttributeRefresh**.
4. Select **Actions > Start**.

Results

The task builds the hierarchies according to the configured schedule.

Verify that the Rights Lookup tables have no duplicated values

Before you start, or after you complete, the migration process, verify that the Rights Lookup tables contain no duplicated values.

Product versions before 5.2.2 supported the possibility of having a Rights Lookup table with duplicated values or Technical values. This option is no longer possible with version 5.2.2 and later.

Therefore, you are required to change the values or Technical values of any Rights Lookup table that are featured more than once in their respective column.

Failure to do so causes the Lookup feature in User Management requests to malfunction in the Access Requests module of Service Center.

The malfunction is because the Lookup options for User Management requests - that are configured in **Access Governance Core > Settings > Core Configurations > User Virtual Attributes** - must present univocal values when they are chosen. If the values of a Lookup option are duplicated, the product does not distinguish which is the correct one.

To verify the Rights Lookup tables, go to **Access Governance Core > Configure > Rights Lookup** and scroll the Value and Technical Value columns of each Rights Lookup table.

Upgrading Identity Brokerage Adapters

When you upgrade the product, you must upgrade the installed Identity Brokerage Adapters to their latest versions.

Upgrading the adapter requires full installation and manual import of the new adapter profile. Complete this task after the database upgrades.

See the corresponding Adapter *Installation and Configuration Guide* for the specific prerequisites, installation and configuration tasks, and issues and limitations. You can find the adapter documentation at http://www.ibm.com/support/knowledgecenter/SSIGMP_1.0.0/com.ibm.itim_pim.doc/c_adapters_intro.htm.

See the Adapters release notes for any updates to these references.

Chapter 7. 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.

Table 14. Virtual appliance administrators maintenance tasks

Tasks	Subtasks and references
Prepare for disaster recovery. Set up a secondary virtual appliance for an active-passive configuration.	<ol style="list-style-type: none"> 1. Setting up a primary virtual appliance 2. Backing up the virtual appliance 3. Reverting the virtual appliance to its backup 4. Creating a snapshot of the virtual appliance 5. Setting up a secondary virtual appliance
Monitor system event logs, memory, CPU, and storage usage, and configure the Simple Network Management Protocol.	<ul style="list-style-type: none"> • Viewing the event logs • Viewing the memory usage • Viewing the CPU usage • Viewing the storage usage • Viewing the cluster status • Managing the SNMP monitoring
Configure the directory server, database server, OpenID connect providers, and mail server.	<ul style="list-style-type: none"> • Managing directory server configuration • Managing the database server configuration • Managing OpenID connect configuration • Managing the mail server configuration
Configure and manage the Postgres replication, IBM Security Directory Integrator instances, and cluster nodes.	<ul style="list-style-type: none"> • Managing the Postgres database • Managing Security Directory Integrator instances • Managing LTPA-based single sign-on configuration
Manage custom files, and certificate stores.	<ul style="list-style-type: none"> • Managing custom files • Managing certificates
Manage the virtual appliance updates and licensing.	<ul style="list-style-type: none"> • Viewing the update history • Viewing the licensing • Managing the firmware settings • Installing a fix pack
Manage the virtual appliance and Identity Governance and Intelligence logs retrieval and configuration, core dumps, Identity Brokerage Providers configuration, and build information.	<ul style="list-style-type: none"> • Managing the log configuration • Managing the core dump files • Enabling Identity Brokerage Providers • Viewing the About page information

Table 14. Virtual appliance administrators maintenance tasks (continued)

Tasks	Subtasks and references
Manage network settings such as application interfaces, hosts files, static and system routes, and the network file system.	<ul style="list-style-type: none"> • Managing application interfaces • Managing hosts file • Configuring static routes • Managing a network file system (NFS)
Manage the Export and Import settings	Exporting or importing the configuration settings
Manage the virtual appliance administrator settings, and system settings such as tuning parameters, snapshots, support files, system audit events, BiDi properties, and management authentication.	<ul style="list-style-type: none"> • Configuring the date and time settings • Configuring the administrator settings • Managing advanced tuning parameters • Configuring BiDi properties • Managing the snapshots • Managing the support files • Configuring system audit events • Configuring LMI authentication for external user registry • Restarting or shutting down the appliance
Manage the virtual appliance by using the command line interface.	<ul style="list-style-type: none"> • Managing the core dump files • Tailing logs and archiving logs • Adding a JVM property • Managing the SSL certificate • Getting and setting the SIB schema names • Getting and setting the reconciliation failure threshold

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

The password that you specified when you activated the virtual appliance.

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 15. 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 42.
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 43.
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.

Table 15. Synchronization states table. (continued)

State	Description	Action
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.

- 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

- 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**
- 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

- 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.
- 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.

- 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

- From the top-level menu of the **Appliance Dashboard**, click **Monitor** > **Monitoring** > **CPU**. The System CPU Statistics page is displayed.
- 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.

- 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.
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.
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 16 on page 75.

Table 16. Directory server configuration details.

Function	Directory server options
Configure	<p>Host name Specify the name of the server that hosts the directory server.</p> <p>The acceptable formats for the host name are IPv4, FQDN, and IPv6. For example, igildap.example.com.</p> <p>Port Specify the directory server port.</p> <p>For example, 389.</p> <p>SSL Flag this check box to apply SSL encryption to the connection with this server.</p> <p>If you select this option, you are also prompted to accept the ldapcert default digital certificate.</p> <p>Principal DN Specify the principal distinguished name.</p> <p>For example, cn=root.</p> <p>Password Specify the password for the directory server.</p> <p>Organization name Specify the name of the enterprise or the organization.</p> <p>For example, JK Enterprises.</p> <p>Default organization short name Specify the abbreviation or short form of the organization name.</p> <p>For example, jke.</p> <p>DN Location Specify the directory server DN location.</p> <p>For example, dc=com.</p>

Table 16. Directory server configuration details (continued).

Function	Directory server options
Reconfigure	<p>Host name Specify the name of the server that hosts the directory server.</p> <p>The acceptable formats for the host name are IPv4, FQDN, and IPv6. For example, igildap.example.com.</p> <p>Port Specify the directory server port.</p> <p>For example, 389.</p> <p>SSL Flag this check box to apply SSL encryption to the connection with this server.</p> <p>If you select this option, you are also prompted to accept the ldapcert default digital certificate.</p> <p>Principal DN Specify the principal distinguished name.</p> <p>For example, cn=root.</p> <p>Password Specify the password for the directory server.</p>

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 16 on page 75.
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 141.
 - 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 16 on page 75.
 - 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.

The Directory Server SSL certificate

When you configure, or reconfigure, the Directory Server with the **SSL** option, the configuration pane prompts you to accept the default digital certificate for the Directory Server.

After you accept it, the certificate is created and labeled `ldapcert`.

Take these steps to view the certificate properties:

1. From the top-level menu of the Appliance Dashboard, select **Configure > Manage Server Setting > Certificates**. to display the Certificate Stores page.
2. In the **Certificate Database Name** column, select **Identity Governance and Intelligence key store**.
3. Select **Edit**.
4. Select **Signer**. The `ldapcert` certificate information is displayed.

You can also delete the selected `ldapcert` certificate and import a new one. After you delete the certificate, you can do one of the following actions to upload a new one:

- Select **Signer > Import**.
- Reconfigure the Directory Server and accept the certificate.

Alternatively, you can import your own Directory Server certificate in the **Signer** tab before you configure the Directory Server. In this case, when you select the **SSL** option in the Directory Server configuration details window, you are not prompted to accept `ldapcert`.

The `ldapcert` certificate is not automatically deleted when you unconfigure the SSL option from Directory Server.

Authenticating users from an external user registry to the Local Management Interface

You can choose to use an external user registry, in place of the default custom registry, to designate which users can authenticate to the local management interface (LMI) of the virtual appliance.

Specify users or groups of users that are defined in a directory server in the LMI Authentication Configuration details window. The directory servers that are provided by IBM Security Directory Server or by Microsoft Active Directory are supported.

This option applies only to the local management interface of the virtual appliance. It does not apply to the virtual appliance command line interface.

A disruption of the connection between the virtual appliance and the directory server might prevent the users of the external registry from being able to access the LMI. At this time, only the `admin@local` user can log into the LMI. The `admin@local` user credentials are based on the local operating system user registry. The credentials are automatically set equal to those of `admin` during the initialization process of the virtual appliance. As long as the connection is disrupted, `admin@local` is the only user who can access and manage the virtual appliance from the LMI. This applies also in a clustered environment.

In the LMI Authentication Configuration details window, you are asked to provide information about the host of the directory server, the port number, whether to use SSL encryption, the principal distinguished name, password and location, and filters for the users or user groups that can authenticate.

If you use SSL encryption, you can accept a default certificate or import your personal certificate in the Local Management Interface key store. If you delete the certificate, the users from the external registry can no longer log in to the LMI. Only the `admin@local` user can log in and either import a new certificate or reconfigure the LMI Authentication Configuration details to generate a new default certificate.

Users who are authenticated from the external registry have their actions logged by the system audit. Every event in the event log of the virtual appliance includes the ID of the user who triggered the event.

Attention: When a failback or failover recovery procedure is run on a virtual appliance with LMI Authentication configured, the event log reports `admin@local` in place of the user who actually ran the procedure.

Configuring to authenticate users from an external user registry to the Local Management Interface

Use the LMI Authentication Configuration page to configure, reconfigure, or unconfigure users from an external user registry to authenticate to the local management interface of the virtual appliance.

Before you begin

Make sure to add the required users to the external user registry on IBM Security Directory Server or Microsoft Active Directory before you work from this configuration page.

About this task

Configure, reconfigure, or unconfigure external authentication to enable users that are included in the external user registry to access the local management interface (LMI) of the virtual appliance.

Table 17. LMI Authentication configuration details

Function	LMI Authentication configuration options
Configure	<p>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.</p> <p>Port Specify the directory server port. For example, 389.</p> <p>SSL Flag this check box to apply SSL encryption to the connection with this server. If you select this option, you are also prompted to accept the default digital certificate.</p> <p>Principal DN Specify the principal distinguished name. For example, cn=root.</p> <p>Password Specify the password for the principal distinguished name.</p> <p>LMI Authentication DN Location Specify the directory server DN location. For example, dc=com.</p> <p>User filter Specify which users in the external registry can access the LMI. For example:</p> <ul style="list-style-type: none"> • For Directory Server, <code>(&(uid=%v)(objectclass=inetOrgPerson))</code> <p>utilizes user IDs (uid) and the inetOrgPerson object class to find the users. At run time, %v is replaced with the uid attribute of each user, which must be a unique key within the same object class in LDAP.</p> <ul style="list-style-type: none"> • For Active Directory, <code>(&(sAMAccountName=%v)(objectclass=organizationalPerson))</code> <p>utilizes user account names (sAMAccountName) and the organizationalPerson object class to find the users.</p> <p>Group filter Use group names to specify which users in the external registry can access the LMI. For example:</p> <ul style="list-style-type: none"> • For Directory Server, in <code>(&(cn=groupName)((objectclass=groupOfNames))</code> <p>groupName is the name of a group that is defined in Directory server. The object class can be groupOfNames, groupOfUniqueNames, or groupOfURLs. You can specify multiple object classes. For example, <code>(&(cn=groupName)((objectclass=groupOfNames) (objectclass=groupOfUniqueNames) (objectclass=groupOfURLs)))</code> • For Active Directory, in <code>(&(cn=groupName)(objectcategory=CN=Group,CN=Schema,CN=Configuration,DC=DN location of Active Directory))</code> <p>groupName is the name of a group that is defined in Directory Server.</p> </p>

Table 17. LMI Authentication configuration details (continued)

Function	LMI Authentication configuration options
Reconfigure	<p>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.</p> <p>Port Specify the directory server port. For example, 389.</p> <p>SSL Flag this check box to apply SSL encryption to the connection with this server. If you select this option, you are also prompted to accept the default digital certificate.</p> <p>Principal DN Specify the principal distinguished name. For example, cn=root.</p> <p>Password Specify the password for the principal distinguished name.</p> <p>LMI Authentication DN Location Specify the directory server DN location. For example, dc=com.</p> <p>User filter Specify which users in the external registry can access the LMI. For example:</p> <ul style="list-style-type: none"> • For Directory Server, (&(uid=%v)(objectclass=inetOrgPerson)) <p>utilizes user IDs (uid) and the inetOrgPerson object class to find the users. At run time, %v is replaced with the uid attribute of each user, which must be a unique key within the same object class in LDAP.</p> <ul style="list-style-type: none"> • For Active Directory, (&(sAMAccountName=%v)(objectclass=organizationalPerson)) <p>utilizes user account names (sAMAccountName) and the organizationalPerson object class to find the users.</p> <p>Group filter Use group names to specify which users in the external registry can access the LMI. For example:</p> <ul style="list-style-type: none"> • For Directory Server, in (&(cn=groupName)((objectclass=groupOfNames)) <p>groupName is the name of a group that is defined in Directory server. The object class can be groupOfNames, groupOfUniqueNames, or groupOfURLs. You can specify multiple object classes. For example, (&(cn=groupName)((objectclass=groupOfNames)(objectclass=groupOfUniqueNames)(objectclass=groupOfURLs)))</p> <ul style="list-style-type: none"> • For Active Directory, in (&(cn=groupName)(objectcategory=CN=Group,CN=Schema,CN=Configuration,DC=DN location of Active Directory))) <p>groupName is the name of a group that is defined in Directory Server.</p>

Procedure

1. From the top-level menu of the virtual appliance dashboard, click **Manage > System Settings > Management Authentication**.
2. In the LMI Authentication Configuration pane, select **Configure**.
3. In the LMI Authentication Configuration Details window, specify the expected variables. For more information, see Table 17 on page 79.
4. Select **Save Configuration**.
5. Optional: Reconfigure an existing LMI Authentication configuration.
 - a. From the LMI Authentication Configuration table, select the LMI Authentication configuration record.
 - b. Click **Reconfigure**.
 - c. In the Edit LMI Authentication Configuration Details window, edit the configuration variables. For more information, see Table 17 on page 79.
 - d. Click **Save Configuration**.
6. Optional: Unconfigure an existing LMI Authentication configuration.
 - a. From the LMI Authentication Configuration table, select the LMI Authentication configuration record.
 - b. Click **Unconfigure**.
 - c. Click **Yes** to confirm the deletion.

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

The following table lists the fields for configuring or reconfiguring a database as the Identity data store. The options depend on the type of database that you configure. Database types are independent of each other. If you unconfigure the database and reconfigure a different database type, the data is retained in the original database. It is not merged with the new database.

Attention:

- In a cluster environment, all nodes must use the same database. In that environment, reconfiguring, and unconfiguring can be done from the primary node only.
- For Oracle, if you change the version of the LMI security protocol, and consequently also the TLS version on the Oracle database server, you must reconfigure Database Server Configuration before users can log in to Identity Governance and Intelligence again.

Table 18. Options for configuring the Identity data store

Button	Data store options
Configure	<p>Database type Select the database type from the list. To configure the database server, select one of these options.</p> <ul style="list-style-type: none"> • IBM DB2 • Oracle (Standard) • Oracle (Custom) • PostgreSQL (Internal) If you select PostgreSQL, except for being required to change the number of minimum connections to 0, you need to enter no additional connection information. <p>Host name (FQDN, IPv4, or IPv6) Specify the name of the server that hosts the data store. For example, igidstore.example.com.</p> <p>JDBC URL Specify the JDBC URL to connect with the database. For example:</p> <ul style="list-style-type: none"> • jdbc:oracle:thin://<hostname>:<port>:<dbName> for non-SSL. • jdbc:oracle:thin:@(DESCRIPTION(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCPS)(HOST=<hostname>)(PORT=<port>))))(CONNECT_DATA=(SERVICE_NAME=<service>))) for SSL. <p>Note: Specify the JDBC URL for Oracle (Custom).</p> <p>Port Specify the data store service port. For example, 50000.</p> <p>SSL Flag the check box to configure with the database server in SSL.</p> <p>If you select this option, and you do not have a signer certificate for the database, another window prompts you to accept a default certificate. The window is not displayed if a certificate is already in place in the Identity Governance and Intelligence signer certificate store of the virtual appliance.</p> <p>Note: For a PostgreSQL database, this option is enabled by default when you configure over a FIPS-enabled virtual appliance.</p> <p>Database name Specify the Identity Governance and Intelligence database name, such as igidb.</p> <p>Database User Password Specify the password for the Identity data store user ID.</p> <p>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.</p> <p>If you select Oracle (Standard) or Oracle (Custom), configure these options.</p> <p>Oracle SID or Service name Specify the Oracle System ID (SID) or the service name to identify the database. For example, isimdb.</p> <p>Select or clear the Service name check box to manage the following aspects:</p> <ul style="list-style-type: none"> • 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. <p>Note: When you select Oracle (Custom) as the database type, you cannot configure these options:</p> <ul style="list-style-type: none"> • Port, Database name, Oracle SID or service name <p>Note: If you want to manage FIPS features with Oracle, you must be compliant with TLSv1.2 protocol (see LMI security protocol).</p>

Table 18. Options for configuring the Identity data store (continued)

Button	Data store options
Reconfigure	<p>Note: Reconfiguration does not update the database schema. It configures IBM Security Identity Governance and Intelligence with new database details.</p> <p>Host name (FQDN, IPv4, or IPv6) Specify the name of the server that hosts the data store. For example, igidstore1.example.com.</p> <p>JDBC URL Specify the JDBC URL to connect with the database. For example:</p> <ul style="list-style-type: none"> • jdbc:oracle:thin:@//<hostname>:<port>:<dbName> for non-SSL. • jdbc:oracle:thin:@(DESCRIPTION(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCPS)(HOST=<hostname>)(PORT=<port>))) (CONNECT_DATA=(SERVICE_NAME=<service>))) for SSL. <p>Note: Specify the JDBC URL for Oracle (Custom).</p> <p>Port Specify the data store service port. For example, 51000.</p> <p>SSL Flag the check box to configure with the database server in SSL.</p> <p>If you select this option, and you do not have a signer certificate for the database, another window prompts you to accept a default certificate. The window is not displayed if a certificate is already in place in the Identity Governance and Intelligence signer certificate store of the virtual appliance.</p> <p>Note: For a PostgreSQL database, this option is enabled by default when you configure over a FIPS-enabled virtual appliance.</p> <p>Database name Specify the name of the IBM Security Identity Governance and Intelligence database. Example, igidb.</p> <p>Database User Password Specify the password for the Identity data store user ID.</p> <p>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.</p> <p>If you select Oracle (Standard) or Oracle (Custom), configure these options.</p> <p>Oracle SID or Service name Specify the Oracle System ID (SID) or the service name to identify the database. For example, igidb.</p> <p>Select or clear the Service name check box to manage the following aspects:</p> <ul style="list-style-type: none"> • 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 window, specify the expected variable values. For more information, see Table 18 on page 82.
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 141.
- b. From the Database Server Configuration table, select the database configuration record, Identity data store.
- c. Click **Reconfigure**.
- d. In the Database Server Configuration window, edit the details. For more information, see Table 18 on page 82.
- 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 database connection pool settings

You can use the Database Server Configuration page to manage the data source connection pool settings.

About this task

A database connection pool is a cache of connections to the database that can be modified to improve performance. You can use this task to configure the settings for the connections.

Procedure

1. Go to the top level of the **Appliance Dashboard** click **Configure**.
2. Under **Manage External Entities**, click **Database Server Configuration**.
3. Select **Identity data store** and click either **Configure** or **Reconfigure**.
4. Click the **Connection Pool** tab in the Edit Identity data store details window.
5. Specify the values that you want to set for the connections.

Connection timeout:

Specifies the interval, in seconds, after which a connection request times out and a `ConnectionWaitTimeoutException` is thrown.

Maximum connections:

Specifies the maximum number of physical connections that you can create in this pool.

Minimum connection:

Specifies the minimum number of physical connections to maintain. The default is 5 connections.

Attention: You must set this value to 0 for PostgreSQL.

Reap time:

Specifies the interval, in seconds, between runs of the pool maintenance thread.

Unused timeout:

Specifies the interval, in seconds, after which an unused or idle connection is discarded.

Aged timeout:

Specifies the interval in seconds before a physical connection is discarded.

6. Click **Save Configuration**.

Managing DB2 automatic client reroute settings

Use the Database Server Configuration page to set up a DB2 automatic client reroute. This option is available for a DB2 datasource only.

About this task

Automatic client reroute enables an IBM® Data Server Client application to recover from a loss of communications so that the application can continue its work with minimal interruption. As the name suggests, rerouting is central to the support of continuous operations. Rerouting is only possible when an alternate location is identified to the client connection.

In an SSL configuration, for each Alternative server that you list, you need to upload a signer certificate in the Identity Governance and Intelligence signer certificate store of the virtual appliance. Note that, while a prompt to accept a default signer certificate for the database server is displayed if no user certificate is found, this is not the case for alternate servers.

Procedure

1. Go to the top level of the **Appliance Dashboard** click **Configure**.
2. Under **Manage External Entities**, click **Database Server Configuration**.
3. Select **Identity data store** and click either **Configure** or **Reconfigure**.
4. Click the **DB2 ACR** tab in the Edit Identity data store details window.
5. Specify the values that you want to set for the connections.

Retry interval for client reroute:

Specifies the amount of time, in seconds, between retries for automatic client reroute.

Maximum retries for client reroute:

If the primary connection to the server fails, it specifies the maximum number of connection retries that are attempted by the automatic client reroute function. The property is only used when Retry interval for client reroute is set.

Alternative server names:

Specifies the list of alternate server name or names for the DB2 server. If more than one alternate server name is specified, the names must be separated by commas, such as host1,host2.

Alternate port numbers:

Specifies the list of alternate server port or ports for the DB2 server. If more than one alternate server port is specified, the ports must be separated by commas, such as 50000,50001.

Note: The port number must be the same type as the port number specified on the **Connection** tab, either SSL or non-SSL.

6. Click **Save Configuration**.

The database SSL certificate

When you configure, or reconfigure, a DB2 or Oracle database server as the Identity data store, and you select the **SSL** option, a new window prompts you to accept the default digital certificate, if you do not have one in place.

The configuration process does not continue until you accept the certificate.

The window is not displayed if a certificate for the database is present in the Identity Governance and Intelligence key store.

If you run the advanced configuration process to configure the database, the existence of a certificate is verified when the response file is validated. The window that prompts you to accept the default certificate is displayed only if a certificate for the database is not found in the certificate store.

If you use the virtual appliance REST APIs to configure the database, the certificate must be in place in the certificate store. If it is not, the REST API returns an error.

If you add the database server certificate to the virtual appliance through the Database Certificate accept prompt, then the certificate is labeled `dbcert` in the Identity Governance and Intelligence signer certificate store.

The certificate is not automatically deleted when you unconfigure the database.

Managing the PostgreSQL database

IBM Security Identity Governance and Intelligence contains an internal PostgreSQL database that can store your data. If you choose to use the internal PostgreSQL database, use the following procedure to manage the database.

About this task

Important:

- If you are using the PostgreSQL database in a stand-alone node, ensure that you back up your data.
- The ID of the database administrator is `postgres`. Initially, the password is by default set to the same value of the password of the administrator of the virtual appliance. After the first time that the database administrator password is changed, the two administrator passwords follow different paths.
- The default password of DB Users (the schema users) is `ideas`.

The database administrator and the schema users passwords can be changed in the Postgres Management page.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure > Postgres Management**. The Postgres Management page displays a table with these column names.

Name Specifies the name of the internal database, *hostname*.

NFS Enabled

Indicates whether a network file system mount point is created for the database. A status of true indicates that an NFS mount point exists for the database.

State Indicates whether the instance is started or stopped.

Database Role

Specifies whether the database is a master or slave database. The role depends on whether the database is on a primary or secondary node. A PostgreSQL database on a single-server configuration or on the primary node in a cluster configuration is the master database. The PostgreSQL database on a secondary node is a slave database.

SSL Specifies whether the database runs over an SSL connection (True) or not (False). By default, the value is **True** if the database is configured on a FIPS-enabled virtual appliance.

2. On the Postgres Management page, do one of these actions. The actions that are available depend on whether you are working on the master or the slave database. The actions also depend on the node you are working from.

Table 19. PostgreSQL database action items

Action	Button	Description
Start the database	Start	This option is available on the node for the master database only. <ul style="list-style-type: none">• Select the database.• Click Start. A message indicates that the PostgreSQL server is starting. After the server is started, a system notification message is displayed that the PostgreSQL server was started successfully.
Stop the database	Stop	This option is available on the node for the master database only. <ul style="list-style-type: none">• Select the database.• Click Stop. A message indicates that the PostgreSQL server is stopping. After the server is stopped, a system notification message is displayed that the PostgreSQL server was stopped successfully.
Restart the database	Restart	This option is available for the master database only. <ul style="list-style-type: none">• Select the database.• Click Restart. A message indicates that the PostgreSQL server is restarting. After the server is restarted, a system notification message is displayed that the PostgreSQL server was restarted successfully.
Start the slave database	Resume replication	This option is available on the node for the slave database only. <ul style="list-style-type: none">• Select the database.• Click Resume replication. A message indicates that the PostgreSQL server is starting. After the server is started, a system notification message is displayed that the PostgreSQL server was started successfully.

Table 19. PostgreSQL database action items (continued)

Action	Button	Description
Stop the slave database	Pause replication	<p>This option is available on the node for the slave database only.</p> <ul style="list-style-type: none"> • Select the database. • Click Pause replication. <p>A message indicates that the PostgreSQL server is stopping. After the server is stopped, a system notification message is displayed that the PostgreSQL server was stopped successfully.</p>
Refresh the database information	Refresh	<p>Click Refresh to display the most recent version of the data, including changes that were made to the data since it was last refreshed.</p>
Create a replica of the primary node database on the secondary node	Manage	<p>This option is available for the slave database on a secondary node only.</p> <ul style="list-style-type: none"> • Select the database. • Click Manage. • Click Configure replication on the secondary node to create a backup of the master PostgreSQL database and begin replication. <p>See “Enabling and disabling replication between the primary and secondary nodes” on page 41.</p>
Remove a replica of the primary node database from the secondary node	Manage	<p>This option is available for the slave database on a secondary node only.</p> <ul style="list-style-type: none"> • Select the database. • Click Manage. • Click Unconfigure replication on the secondary node to stop replication and to remove the backup PostgreSQL database. <p>See “Enabling and disabling replication between the primary and secondary nodes” on page 41.</p>
Clear the data from the PostgreSQL database	Manage	<p>This option is available for the master database on the primary node only.</p> <ol style="list-style-type: none"> 1. Select the database. 2. Click Manage. 3. Click Reset to remove the data from the PostgreSQL database and create a new PostgreSQL database. <p>Note: If you unconfigure the PostgreSQL database as the identity data store, the data is preserved in the PostgreSQL database. To clear the database, you must use Reset.</p> <p>If you reset the master PostgreSQL database on the primary node, the slave database on the secondary node is not reset. You must force synchronization of the slave database from the secondary node to remove the data.</p>

Table 19. PostgreSQL database action items (continued)

Action	Button	Description
Change the PostgreSQL database password	Manage	This option is available for the master database on the primary node only. <ol style="list-style-type: none"> 1. Select the database. 2. Click Manage. 3. Click Change Password. <p>See "Changing the Postgres database password."</p>
Set up more storage for a PostgreSQL database	Manage	This option is available for the master database on the primary node only. <ol style="list-style-type: none"> 1. Select the database. 2. Click Manage. 3. Click Move to NFS. <p>See "Setting up external storage for the Postgres database" on page 91.</p>
Promote a slave database to a master database	Promote	This option is available for the slave database only. <ul style="list-style-type: none"> • Select the database. • Click Manage. • Click Promote. • Click Yes to confirm that you want to promote the database.
Synchronize the databases	Force Synchronization	This option is available for the slave database only. <ul style="list-style-type: none"> • Select the database. • Click Manage. • Click Force synchronization. • Click Yes to confirm that you want to force the synchronization of the database.
Change the SSL settings	Manage	<ul style="list-style-type: none"> • Select the database. • Click Manage. • Click Security. <p>The Security Setting window is displayed. The Enable SSL field displays the current status, True or False.</p> <ul style="list-style-type: none"> • Click the field and change the current value. Another window confirms that SSL is being enabled or disabled.

Changing the Postgres database password

For security reasons, you might want to change the Postgres database password from the default password.

About this task

You can change the password of the Postgres administrator and the password for the database schema users. The Postgres database passwords can be changed from the primary node only.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure > Postgres Management**.
2. Select the database to activate the management functions.
3. Click **Manage > Database > Change Password**.
4. Select the type of user that you want to change the password for from the **Users** menu.

DB Admin

Is the Postgres database administrator, whose ID is postgres. Initially, the password is by default set to the same value of the password of the administrator of the virtual appliance. After the first time that the database administrator password is changed, the two administrator passwords follow different paths.

DB Users

Are the Postgres database schema users.

Note: Changing this password, changes the password for all database schema users.

5. Type the current password for the specified user type in the **Current password** field. If you upgraded from version 5.2.1, the default Postgres database password is postgres.
6. Type the new password for the selected user type.
7. Type the password again to confirm it.
8. Click **Save Configuration**.

A message indicates that the Postgres password is being changed. A system notification message is displayed that the Postgres password was changed successfully.

Recovering from a Postgres database failure

If the master Postgres database fails, use this failover procedure to recover your system.

About this task

Although you can promote the slave Postgres database on a secondary node to the role of master, you cannot perform the master database management functions. You must either restore master Postgres database on the primary node or promote the secondary node to primary to use these management functions.

Procedure

1. Promote the slave database to be the master database.
 - a. Ensure that the master database is stopped on the primary node.
 - b. On the secondary node, click **Configure > Postgres Management**.
 - c. Select the slave database and click **Manage > Promote**.
 - d. Click **Yes** to confirm that you want to promote the database to master.

The role of the Postgres database on the secondary node is now master and the role of the database on the primary node is slave. Both databases are started as well as replication.

2. Restore the master database on the primary node.
 - a. On the secondary node, click **Configure > Postgres Management**.

- b. Select the master database and click **Stop**.
- c. On the primary node, click **Configure > Postgres Management**.
- d. Select the slave database and click **Manage > Promote**.
- e. Click **Yes** to confirm that you want to promote the database to master.

The role of the Postgres database on the primary node is now master and the role of the database on the secondary node is slave. Both databases are started as well as replication.

Results

The master Postgres database is restored on the primary server and the appropriate **Manage** options are active.

Setting up external storage for the Postgres database

If you are using the internal Postgres database and need more storage, you can use a network file system to link to external Postgres database.

Before you begin

The external directory must exist, and you must set up an NFS mount point to it. See “Managing a network file system (NFS)” on page 135. After the mount point is created, ensure that all the nodes are synchronized. See “Synchronizing a member node with a primary node” on page 43.

Take a snapshot of the virtual appliance before you move the Postgres database to a Network File System. You can use the snapshot to recover from configuration errors, or if you need to restore the internal Postgres database later.

Note: If you revert to the internal Postgres database, the snapshot does not include any data that was added to the NFS database. You must explicitly take the database backup on the NFS database and restore it to the internal database. Refer to Postgres documentation for information about how to back up and restore the database.

About this task

This task must be performed on the master Postgres database on a primary node. No business operations can take place during the move to NFS. The time that is needed for the move depends on the size of the database.

Procedure

1. Ensure that all changes are synchronized across the nodes.
2. Click **Configure > Postgres Management**.
3. Select the database to activate the options.
4. Click **Manage > Database > Move to NFS**.
5. Select the NFS mount point.
6. Click **Save Configuration**.
7. Synchronize the nodes. See “Synchronizing a member node with a primary node” on page 43.

Results

- Data is stored externally through the NFS mount point.
- Replication is disabled.

- Move to NFS is disabled.
- The slave database is removed from the Postgres Management table.

What to do next

Set up a Network File System replication server to back up your data. Refer to Postgres documentation for information about backing up and restoring the database.

Recovering the database by using a Network File System (NFS) replication server

If your Postgres database on the Network File System (NFS) becomes unavailable and you created an NFS replication server, use this procedure to recover your data.

Before you begin

An NFS replication server must exist.

About this task

For this procedure, the Postgres database that was moved to the Network File System is NFS_Server1. The NFS replication server that backs up the database is NFS_Server2.

Procedure

1. On the primary node, click **Configure > Manage Server Settings > Postgres Management**.
2. Select the database and click **Stop**.
3. Click **Manage > Network Settings > Network File System**. Take note of the remote and local directory and permission information for the Postgres database. You need them to create a new mount point.
4. Select the NFS mount point that the Postgres database was moved to and click **Delete**.
5. Create an NFS mount point to NFS_Server2. See “Managing a network file system (NFS)” on page 135. Use the same remote and local directories, and permissions, that were used for NFS_Server1.
6. Click **Save Configuration**.
7. On NFS_Server2, change the Postgres data directory permissions. Issue the following commands.


```
chown -hR 5003:5003 Postgres_Data_Directory
chmod -R 700 Postgres_Data_Directory
```
8. On the primary node, click **Configure > Manage Server Settings > Postgres Management**.
9. Select the database and click **Start**.

The PostgreSQL database SSL certificate

When you select the **SSL** option for the PostgreSQL database, or when you configure the database in a FIPS-enabled virtual appliance, a self-signed certificate is created by default.

To list the default certificate, select **Configure > Certificates** in the virtual appliance dashboard. The certificate is listed in the Certificate Stores pane with the Postgres database key store name.

If you do not want to use the default certificate, you can upload your personal certificate. In this case, you must replace the self-signed certificate with your personal certificate. You must also import your personal certificate in the Signer certificate of the Identity Governance and Intelligence key store.

To upload your personal certificate, follow these steps:

1. In the Certificate Stores pane, select Postgres database key store and click **Edit**.
2. Select dbcert and click **Update**.
The Import Certificate window is displayed.
3. In this window, enter the file name, a label, and a password, and select the type. Click **Save**.
4. In the Certificate Stores pane, select Identity Governance and Intelligence key store and click **Edit**.
5. Select the **Signer** tab and click **Import**.
The Import Certificate window is displayed.
6. In this window, enter the file name and a label, and click **Save**.

If you run a cluster and you upload your personal certificate on the secondary node where the slave database runs, you must also take these steps:

1. Import your personal certificate in the Signer certificate of the Identity Governance and Intelligence key store of the primary node.
2. Synchronize all nodes.

Backing up the PostgreSQL database

You can connect to the PostgreSQL database and use a tool of your choice to make a backup.

Enter the following parameters to connect to the master database:

Hostname

The IP address or hostname of the virtual appliance where the master database runs.

Port 5432

Username

The name of the database administrator is postgres.

Password

The password of the database administrator. Initially, the password is the same as the password of the administrator of the virtual appliance. If the password was changed, it is the latest password.

Transferring connector files to the virtual appliance from an external source

You can securely transfer subsets of files into the appliance from an external computer by using Secure Copy (scp).

About this task

A connector file can be a partition or a subset of data that is assigned to a server.

On the primary node, you can view and manage connector files through either the local management interface (LMI) or the command line interface (CLI). See “Managing custom files” on page 105 and “Virtual appliance command-line interface commands” on page 154.

On member nodes, while connector files can be viewed from the LMI, they must be managed through the command line interface. Use the command line interface to create, delete, and view connector subdirectories and files. See “Virtual appliance command-line interface commands” on page 154. You can upload files by using the following **scp** command.

Note: Connector files and subdirectories are not synchronized across nodes. In a cluster environment, you must use the command line interface to create them on each node. These folders must be managed in the `/userdata/connectors` directory. Then, upload the files by using the **scp** command.

You can transfer connector files securely by using either a password or an ssh key. To transfer the files, you must use the user name `igiuser`.

Procedure

1. Transfer files with a password.
 - a. Set up a password for `igiuser` on your IBM Security Identity Governance and Intelligence system. On the Identity Governance and Intelligence client
 - 1) Log in to the command line interface.
 - 2) Enter `igi connectors user_settings change_setting`.
 - 3) Enter the new password.
 - 4) Confirm the password.
 - 5) After the password change is confirmed, enter `exit`.
 - b. Transfer the connector file. On the external computer type

```
$scp filename igiuser@hostname:connectors
```

When prompted supply the password for `igiuser`.

2. Transfer files with an SSH key
 - a. Generate a private-public key pair. Use a program like `ssh-keygen` to generate the key pair.
 - b. Install the private key on your external computer.
 - c. Add the public key to the virtual appliance.
 - 1) Log in to the command line interface.
 - 2) Enter `igi connectors ssh_keys add`.
 - 3) Enter the public key for the **auth key**.
 - 4) Enter `exit`.
 - d. Transfer the connector file. On the external computer type

```
$scp filename igiuser@hostname:connectors
```

The file is transferred to the virtual appliance without prompting for a password.

Creating a Network File System (NFS) mount point to access connector files

If you are transferring connector files from external sources to the virtual appliance, you can use a network file system to link to those external sources directly.

Before you begin

The external connector files must exist on the remote system and be under a `connectors/` directory. You must set up an NFS mount point to it.

Take a snapshot of the virtual appliance before connect to a Network File System. You can use the snapshot to recover from configuration errors.

About this task

The connector files and subdirectories must be managed on the remote system.

Procedure

1. On the remote host system, create a user with the name `identity` with an ID of 50001. For example, on a Linux, system issue the command
`adduser -u 50001 identity`
2. Create the connector subdirectories on the remote computer that you are going to mount to. For example, on a Linux system issue the command
`mkdir -p /userdata/connectors/csvConnector1`
3. Assign the user, `identity`, the ownership of and the permissions to access the files in the remote directory `/userdata/connectors/`. For example, on a Linux system, to assign ownership and permissions, issue the commands:
`chmod -R 755 csvConnector1`
`chown -R identity:identity csvConnector1`

Repeat the commands for each of the subdirectories that contain connector files.

4. Create an NFS mount point for each connector file.
 - a. From the top-level menu of the **Appliance Dashboard**, click **Manage > Network Settings > Network File System**.
 - b. Click **New** to display the Add NFS mount point window.
 - c. Type the host name of the NFS server in FQDN, IPv4, or IPv6 format.
 - d. Specify the directory that you are accessing on the remote NFS server.
 - e. Specify the directory location on your local system where you want to access the remote server.
 - f. Optional: Specify the options to use when you connect to the remote system. You can specify multiple options that are separated by commas.
 - g. Click **Save Configuration**.

See “Managing a network file system (NFS)” on page 135.

5. Set the path for the connector files in the IBM Security Identity Governance and Intelligence application for the connector directory. For example, set the path to `/nfsmount/connectors/csvConnector1`. See Driver configuration.
6. If you are in a cluster environment, synchronize the nodes to propagate the changes. See “Synchronizing a member node with a primary node” on page 43.

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 20. Necessary information for configuration

Configuration type	Types and definitions
All configurations	<p>Provider name The service that provides your OpenID.</p> <p>Certificate Alias The label of the certificate that was uploaded to the trust store. This field is required when the signature algorithm is RS256 and the JWK URL is not provided. Otherwise, it is an optional field.</p> <p>Signature algorithm The algorithm that is used to sign the ID token that is issued by a provider. The default value is HS256.</p> <p>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.</p> <p>Client ID A publicly exposed string that is used by the service API to identify the application. It is also used to build authorization.</p> <p>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.</p> <p>Domains The domain that uses the OpenID connect as the authentication mechanism.</p>

Table 20. Necessary information for configuration (continued)

Configuration type	Types and definitions
Manual configuration	<p>Authorization URL The initial endpoint that is contacted by the relying party to begin a flow.</p> <p>Token URL The endpoint that is used to exchange an authorization code for a token.</p> <p>JWK URL The JSON web key endpoint that is used for signature verification.</p> <p>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</p> <p>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.</p>
Discovery configuration	<p>Discovery URL: Perform discovery to locate the endpoints, scope, and signature algorithm.</p>

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 21. OpenID connect operations

Operation	Steps
Use New to configure an OpenId provider.	<ol style="list-style-type: none"> 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.
Use Edit to change the provider information.	<ol style="list-style-type: none"> 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.	<ol style="list-style-type: none"> 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

- 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. 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.
- 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/en/SSPREK_9.0.0/com.ibm.isam.doc/config/concept/con_oidc_endpoints.html.
- 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 the 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 107.
- i. Restart the IBM Security Identity Governance and Intelligence server from the dashboard

Managing LTPA-based single sign-on configuration

Use the LTPA-based Single Sign-On Configuration page to generate, import, or export LTPA keys and to configure, or unconfigure the single sign-on for the IBM Security Identity Governance and Intelligence virtual appliance.

About this task

These tasks must be performed on a stand-alone node or the primary node of a cluster environment. In a cluster environment, you must synchronize the nodes to propagate the changes that you made on the primary node.

If you want to use LTPA-based single sign-on with IBM Security Identity Manager, you must export the LTPA key from IBM Security Identity Manager. Then, import the key to IBM Security Identity Governance and Intelligence.

For more information about single sign-on, see Single sign-on overview.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure > LTPA based Single Sign-On Configuration**. The Single Sign-On Configuration page displays a table with these column names.

Single Sign-On Configuration

Specifies SSO configuration as the name of the single sign-on authentication that is being used.

SSO Configured

Indicates whether single sign-on is enabled. If SSO is configured, the value is True.

LTPA Key Available

Indicates whether the LTPA key exists. After an LTPA key is generated or imported, the value is True.

- On the LTPA-based Single Sign-On Configuration page, do one of these actions. The actions that are available depend on the node you are working from.

Table 22. LTPA-based Single Sign-On Configuration action items

Action	Button	Description
Create an ltpa.key file and password	Generate	<ol style="list-style-type: none"> Click Generate. Specify a password for the LTPA key file. Confirm the password. Click Save Configuration.
Import the LTPA key file that is used by another virtual appliance	Import	<ol style="list-style-type: none"> Click Import LTPA key. Use Browse to locate the LTPA key file. Enter the password for the key file. Click Save Configuration.
Download the LTPA Key that is used by the virtual appliance	Export	<ol style="list-style-type: none"> Select the LTPA key. Click Export LTPA key. Select Save File. Click OK. <p>The LTPA key file is saved to your Downloads directory.</p>
Remove the current LTPA key	Delete	<p>This option is available if an LTPA key exists.</p> <ol style="list-style-type: none"> Click Delete. Click Yes on the confirmation message to delete the current LTPA key.
Refresh the single sign-on information	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.
Set up single sign-on authentication	Configure	<ul style="list-style-type: none"> Click Configure. Choose the domain option that you want to use. <ul style="list-style-type: none"> Use the domain from the URL that you are logged in to. Use a custom domain name. Specify the domain name in the SSO domain names: field. Type the realm name, for example myrealm.mycompany.com. Specify the URL that you want to return to when you sign off. Click Save Configuration.
Remove single sign-on configuration	Unconfigure	<p>This option is available if single sign-on is configured.</p> <ol style="list-style-type: none"> Click Unconfigure. Click Yes on the confirmation message to unconfigure single sign-on.

Managing Single Sign-On between IBM Security Identity Governance and Intelligence and IBM Security Identity Manager

Use LTPA keys to enable single sign-on among the administrative consoles and the Service Center consoles of the products.

Before you begin

To use single sign-on, you must have accounts on IBM Security Identity Governance and Intelligence and IBM Security Identity Manager with the same user IDs. IBM Security Identity Manager must be at least Version 7.0.1 with Fix Pack 4.

Procedure

1. Export the LTPA key from IBM Security Identity Manager. See *Managing the single sign-on configuration*.
2. Import the LTPA key into the primary or stand-alone node of IBM Security Identity Governance and Intelligence.
 - a. From the top-level menu of the **Appliance Dashboard**, click **Configure > LTPA based Single Sign-On Configuration**.
 - b. Click **Import LTPA key**.
 - c. Use **Browse** to locate the LTPA key file.
 - d. Enter the password for the key file.
 - e. Click **Save Configuration**.
3. Configure single sign-on on Identity Governance and Intelligence.
 - a. Click **Configure**.
 - b. Select **Use domain from url** as the domain name setting.
 - c. Type the realm name `itimCustomRealm`.
 - d. Specify the URL that you want to return to when you exit.
 - e. Click **Save Configuration**.
4. Set the domain name for the Security Identity Manager LTPA key in the Security Identity Manager virtual appliance.
 - a. Enter the command line interface of the Security Identity Manager virtual appliance.
 - b. Go to the `isim/single_sign_on_settings/domain_name/set` section.
 - c. Type the part of the fully qualified domain name that is common to the Security Identity Manager and Identity Governance and Intelligence hosts.
5. If you are working in a cluster environment, synchronize the nodes to propagate the configuration changes. See “Synchronizing a member node with a primary node” on page 43.
6. Restart the Identity Governance and Intelligence application server.
 - a. From the top-level menu of the **Appliance Dashboard**, under **Server Control**, select **Security Identity Governance and Intelligence**.
 - b. Click **Restart**.

What to do next

Log in to the Security Identity Manager Service Center UI `https://ISIM-host-FQDN:9082/itim/ui` with a user ID that is common to both products. Open another tab in your browser and go to the Identity Governance and Intelligence Service Center UI `https://IGI-host-FQDN:9343/service/?realm=IDEAS`.

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 23.

Table 23. Mail Server Configuration

Button	Mail Server options
Configure	<p>Mail server (FQDN, IPv4, or IPv6) Specify a server name that hosts the mail server. For example, mailserver.com.</p> <p>Attention: If you select the SSL option, you must specify an SMTPS server. The use of an SMTP server with the STARTTLS option is not accepted.</p> <p>Port Specify a valid service port of the mail server. By default, the port number is 25.</p> <p>SSL Flag this check box to apply SSL encryption on the email notifications that are sent from this server.</p> <p>If you select this option, you are also prompted to accept the default mailcert certificate.</p> <p>Mail from Specify an email address from which the email is sent. For example, admin@in.ibm.com.</p>
Reconfigure	<p>Mail server (FQDN, IPv4, or IPv6) Change the name of the server that hosts the mail server if necessary.</p> <p>Attention: If you select the SSL option, you must specify an SMTPS server. The use of an SMTP server with the STARTTLS option is not accepted.</p> <p>Port Change the service port of the mail server if necessary.</p> <p>SSL Flag this check box to apply SSL encryption on the email notifications that are sent from this server.</p> <p>If you select this option, you are also prompted to accept the default mailcert certificate.</p> <p>Mail from Change the address from which the email is sent if necessary.</p>

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 23 on page 103.
 - 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 23 on page 103.
 - 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.

The mail server SSL certificate

When you configure, or reconfigure, the mail server with the **SSL** option, the configuration pane prompts you to accept the digital certificate for the mail server.

After you accept it, the certificate is created and labeled mailcert.

Take these steps to view the certificate properties:

1. From the top-level menu of the Appliance Dashboard, select **Configure > Manage Server Setting > Certificates**. to display the Certificate Stores page.
2. In the Certificate Database Name column, select **Identity Governance and Intelligence key store**.
3. Select **Edit**.
4. Select **Signer**. The mailcert certificate information is displayed.

You can also delete the selected mailcert certificate and import a new one. After you delete the certificate, you can do one of the following actions to upload a new one:

- Select **Signer > Import**
- Reconfigure the mail server and accept the certificate.

Alternatively, you can import your own mail server certificate in the **Signer** tab before you configure the mail server. In this case, when you select the **SSL** option in the Mail Server Configuration Details window, you are not prompted to accept mailcert.

The mailcert certificate is not automatically deleted when you unconfigure the SSL option from the mail server.

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.

Note: On primary nodes, you can view and manage files in the Connectors directory. On member nodes in a cluster, files in the Connectors directory can be viewed only. They must be managed through the command line interface. See “Virtual appliance command-line interface commands” on page 154.

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 24 on page 106.

Your files are organized in a hierarchy of folders.

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 24 on page 106.

Table 24. File tabs and their actions

Tab	Tab Description	Actions
<p>All Files</p>	<p>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:</p> <ul style="list-style-type: none"> • Download • Upload • New Folder • Refresh <p>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.</p>	<p>Download a file.</p> <ol style="list-style-type: none"> 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.
		<p>Upload a file.</p> <p>Note: Log files and SDK files cannot be uploaded.</p> <ol style="list-style-type: none"> 1. Select a folder in the left pane. 2. Click Upload to open the File Upload window. 3. Click Browse to select the file. 4. Click Save Configuration.
		<p>Create a folder.</p> <ol style="list-style-type: none"> 1. In the left pane, select a subfolder in which you want to create another folder. <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> • 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.
		<p>Display the most recent version of the data, including changes since the last refresh.</p> <p>Click Refresh.</p>
		<p>Delete a folder.</p> <ol style="list-style-type: none"> 1. Select a folder in the left pane. 2. Click Delete Folder. 3. Click Yes to confirm the action. <p>A message indicates that the selected folder is deleted successfully.</p>

Table 24. 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: <ul style="list-style-type: none"> • Restore Default • Refresh 	Restore a file. <ol style="list-style-type: none"> 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. For example,

```

IGI key store
LMI key store
SDI key 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 the certificate store for which you want to see the certificates.

- 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 > IGI key store > Certificates**.

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

Note: Not all certificate stores have both 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.

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

Option	Description
Update	<p>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.</p> <p>In the Personal tab, do these steps.</p> <ol style="list-style-type: none"> 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. <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> • PKCS#12 • JKS • JCEKS • CMS 7. Click Save.

Option	Description
Import	In the Signer tab, do these steps. <ol style="list-style-type: none"> 1. Click Import to display the Import 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.
Export	<ol style="list-style-type: none"> 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	Note: Signer certificates can be deleted. Personal certificates cannot be deleted. <ol style="list-style-type: none"> 1. Select a certificate from the certificate store. 2. Click Delete.

Updating a personal certificate for an SSL enabled IBM Security Directory Integrator instance

If you update the personal certificate for an IBM Security Directory Integrator instance, you must use the following procedure to ensure that the instance can communicate with the target.

About this task

You can update the personal certificate of an SSL enabled directory integrator instance on any node primary, secondary, or member. The certificate must be exported and then imported to the IGI key store signer certificates of the primary node.

Procedure

1. On the node where the certificate was updated, click **Configure > Certificates**.
2. Select the key store for which the personal certificate was updated and click **Edit**.
3. Select the updated certificate and click **Export**.
4. Save the exported certificate on your local system.
5. Log in to the primary node.
6. Click **Configure > Certificates**.
7. Select **IGI key store** and click **Edit**.
8. Click **Signer**.
9. Click **Upload**.
 - a. Browse to the location of the exported certificate that you saved.
 - b. Type a label for the certificate.
 - c. Click **Save**.
10. Click **Home Appliance Dashboard**.
11. In the Server Control pane, select **Security Identity Governance and Intelligence** and click **Restart**. The nodes are placed in the **Not Synchronized** state.

- Synchronize all the member nodes. See “Synchronizing a member node with a primary node” on page 43.

Updating the JAVA security policy JAR files

The IBM® SDK, on all platforms, provides strong but limited jurisdiction policy files. By default, the key strength is 2048 bits. If you want greater security, you must create custom `US_export_policy.jar` and the `local_policy.jar` files with greater key strength and upload them to the Virtual Appliance.

About this task

Your custom Java security policy JAR files must be named

```
US_export_policy.jar
local_policy.jar
```

Remember:

- These policy JAR files apply to both application certificates and local management interface (LMI) certificates.
- In a virtual appliance cluster, upload the JAR files on every node of the cluster. If you must restore the default policy files, do so in every node.

Procedure

- From the top-level menu of the **Appliance Dashboard**, click **Configure > Java Security Policy**. The Java Security Policy page displays a table with these column names.

File name

Specifies the names of the export and import policies that are being used.

```
US_export_policy.jar
local_policy.jar
```

Modified

Indicates whether the files are the default files. If they are the default files, the **Modified** value is `False`. If the files are customized, the **Modified** values are `True`.

- On the Java Security Policy page, do one of these actions.

Table 25. Java Security Policy action items

Action	Button	Description
Replace the default Java security policy file	Upload	<ol style="list-style-type: none"> Select the Java security JAR file. Click Upload. Use Browse to locate and select the custom Java security policy file. Click OK. A status message is displayed. A system message is displayed when the upload is completed. <p>The Modified value is set to <code>True</code>.</p>

Table 25. Java Security Policy action items (continued)

Action	Button	Description
Restore the default Java security policy file	Restore Default	This option is available if the Modified value is True. <ol style="list-style-type: none"> 1. Select the Java security JAR file. 2. Click Restore Default. 3. At the confirmation prompt, click Yes. 4. A status message is displayed. The Modified value is reset to False.

Managing IBM Security Directory Integrator instances

IBM Security Identity Governance and Intelligence uses IBM Security Identity Adapters to communicate with various managed resources. These adapters are deployed and run on instances of the Security Directory Integrator. The properties of the Security Directory Integrator or Dispatcher affect all of the adapters that run on the instance. Therefore, some adapters might need to run on separate instances of the Security Directory Integrator. Use this task to create and manage multiple instances of the Security Directory Integrator.

About this task

You can configure a maximum of 10 Security Directory Integrator instances. A new instance is assigned to the first available ID and port.

Changes that you make to the Directory Integrator instance are propagated to the nodes in a cluster by the node synchronization process.

Note: For Security Directory Integrator high availability, if the instance on the primary node becomes unavailable, the failover action is for Identity Governance and Intelligence to connect to the directory integrator instance on the secondary node. If the instance is unavailable on the secondary node, Identity Governance and Intelligence continues to try to connect to the instance on member nodes.

Before the virtual appliance routes the request, it checks the connections to the host, <host:port>.

For example, the instance SDI3 crashed on the primary node. Any request that is sent to SDI3 on the primary node is routed to instance SDI3 on one of the member nodes in the cluster. If instance SDI3 crashed on member node, any request that is sent to SDI3 on the member node is routed to another instance of SDI3. The instance can be on the primary node or on one of the member nodes in the cluster.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure > SDI Management**. The Security Directory Integrator Management page displays a table with these column names.

Instance ID

Specifies the ID that was assigned to the instance when it was created. For example, the initial instance is SDI1.

Instance Name

Specifies the name of Security Directory Integrator instance. For example, SDIServer1.

State Indicates whether the instance is started or stopped.

Changes are Active

Indicates whether the adapters in the Security Directory Integrator instance are functioning.

Port Indicates the port that the instance listens on. For example, 1099. The following table shows the ports that are open in the firewall for every instance that is created.

Table 26. Ports that are open in the firewall

Instance	Ports
SDI1	1199, 1198, 1197, 1196, 1195, 1194.
SDI2	2299, 2298, 2297, 2296, 2295, 2294.
SDI3	3399, 3398, 3397, 3396, 3395, 3394.
SDI4	4499, 4498, 4497, 4496, 4495, 4494.
SDI5	5599, 5598, 5597, 5596, 5595, 5594.
SDI6	6699, 6698, 6697, 6696, 6695, 6694.
SDI7	7799, 7798, 7797, 7796, 7795, 7794.
SDI8	8899, 8898, 8897, 8896, 8895, 8894.
SDI9	9999, 9998, 9997, 9996, 9995, 9994.
SDI10	11099, 11098, 11097, 11096, 11095, 11094.

SSL Enabled

Indicates whether secure communications are enabled for the Directory Integrator instance.

The state is True if the virtual appliance is enabled for FIPS or if the **Enable SSL** check box was flagged in the Add Security Directory Integrator or Edit Security Directory Integrator windows.

2. On the Security Directory Integrator Management page, do one of these actions.

Table 27. Security Directory Integrator action items

Action	Button	Description
Add an instance	New	<ol style="list-style-type: none"> 1. Click New to display the Add Security Directory Integrator Server window. 2. Specify the name of the instance that you want to create. 3. If you want to use secure communications, click the Enable SSL check box. Note: If the virtual appliance was enabled for FIPS, the check box is already flagged and grayed out. SSL is also enabled. You cannot clear the check box, unless FIPS is disabled. If the virtual appliance was not enabled for FIPS, the check box is enabled, and you can flag it to use SSL. 4. Specify the minimum amount of memory that you want to assign to the instance in the Minimum Heapsize(MB) field. The minimum heapsize is, 256. 5. Specify the maximum amount of memory that you want to assign to the instance in the Maximum Heapsize(MB) field. The maximum heapsize is, 4,096. 6. Click Save Configuration. <p>A message indicates that a new Security Directory Integrator server is being created. After the server instance is created, a system notification message is displayed and the instance is added to the table.</p>
Edit an instance	Edit	<ol style="list-style-type: none"> 1. Select the instance. 2. Click Edit to display the Edit Security Directory Integrator Server window. 3. If you want to use secure communications, click the Enable SSL check box. If you want to disable secure communications, clear the check box. Note: If the virtual appliance was enabled for FIPS, the check box is already flagged and grayed out. SSL is also enabled. You cannot clear the check box, unless FIPS is disabled. If the virtual appliance was not enabled for FIPS, the check box is enabled, and you can flag it to use SSL. 4. Use the up and down arrows to change the minimum amount of memory that you want to assign to the instance in the Minimum Heapsize(MB) field. The minimum heapsize is, 256. 5. Use the up and down arrows to change the maximum amount of memory that you want to assign to the instance in the Maximum Heapsize(MB) field. The maximum heapsize is, 4,096. 6. Click Save Configuration. <p>A message indicates that the Security Directory Integrator server is being edited. After the server instance changes are complete, a system notification message is displayed that the instance update is successful.</p>

Table 27. Security Directory Integrator action items (continued)

Action	Button	Description
Delete an instance	Delete	<ol style="list-style-type: none"> 1. Select the instance. 2. Click Delete to display the Remove SDI Instance window. 3. A confirmation message is displayed. Click Yes to delete the instance. <p>A message indicates that the Security Directory Integrator server is being deleted. After the server instance is deleted, a system notification message is displayed that the instance is removed.</p>
Start an instance	Start	<ol style="list-style-type: none"> 1. Select the instance. 2. Click Start. <p>A message indicates that the Security Directory Integrator server is starting. After the server instance is started, a system notification message is displayed that the instance started successfully.</p>
Stop an instance	Stop	<ol style="list-style-type: none"> 1. Select the instance. 2. Click Stop. <p>A message indicates that the Security Directory Integrator server is stopping. After the server instance is stopped, a system notification message is displayed that the instance stopped successfully.</p>
Restart an instance	Restart	<ol style="list-style-type: none"> 1. Select the instance. 2. Click Restart. <p>A message indicates that the Security Directory Integrator server is restarting. After the server instance is restarted, a system notification message is displayed that the instance was restarted successfully.</p>
Refresh the instance 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.

Table 27. Security Directory Integrator action items (continued)

Action	Button	Description
Troubleshoot instance problems, configure instance properties files, install adapters, and manage the instance certificates	Manage	<ol style="list-style-type: none"> Select the instance. Click Manage. <ul style="list-style-type: none"> Click Troubleshooting > Log tracing to access and retrieve system logs. See “Managing the log configuration” on page 120. Click Troubleshooting > View log to see the Security Directory Integrator server log. Click Configuration > solution.properties to manage the Dispatcher <code>solution.properties</code> file. See “Configuring the Dispatcher properties for the Directory Integrator instance.” Click Configuration > itim_listener.properties to manage the Dispatcher <code>itim_listener.properties</code> file. See “Configuring the Dispatcher properties for the Directory Integrator instance.” Click Certificates to manage the server certificate. See “Managing certificates” on page 107. Click SDI Adapters to install, uninstall, or export adapters. See “Managing IBM Security Directory Integrator adapters” on page 116

Configuring the Dispatcher properties for the Directory Integrator instance

The Dispatcher is a Security Directory Integrator component. It enables the Identity Governance and Intelligence server to communicate with IBM Tivoli Directory Integrator-based adapters. You can modify the `solution.properties` and `itim_listener.properties` files that configure the Dispatcher.

About this task

The `solution.properties` and `itim_listener.properties` files can be modified on the primary or a stand-alone node only. In cluster environments, the nodes must be synchronized for the Directory Integrator instance configuration changes to propagate to the secondary and member nodes.

Procedure

- From the top-level menu of the **Appliance Dashboard**, click **Configure > SDI Management**.
- Select the instance for the Dispatcher that you want to manage and click **Manage > Configure**.
- Select the Dispatcher property file that you want to manage.
 - solution.properties**
 - itim_listener.properties**

The SDI Advanced Configuration window is displayed with these tabs.

ALL Displays the properties that are contained in the file and their assigned values.

Modified

Displays the properties that were changed with their new values, their default value, and indicates whether they are new properties.

4. Perform any of the following actions.

Table 28. Security Directory Integrator property actions

Action	Button	Description
Add a property.	New	<ol style="list-style-type: none"> 1. On the All tab, click New to display the Update property window. 2. Specify the name of the property that you want to create. 3. Specify the value for the property. 4. Click Save Configuration. <p>A message indicates that a new SDI property is being created. After the property is created, a system notification message is displayed and the property is added to the All and Modified table.</p>
Change a property value.	Edit	<ol style="list-style-type: none"> 1. From either tab, select the property. 2. Click Edit to display the Update property window. 3. Specify the new value for the property. 4. Click Save Configuration. <p>A message indicates that the SDI property is being updated. After the property is updated, a system notification message is displayed and the property value is updated on the All table and the property is added to the Modified table.</p>
Delete a property.	Delete	<p>Note: You can delete customer-added properties. Installed properties cannot be deleted. If you try to delete a required property, the operation fails.</p> <ol style="list-style-type: none"> 1. From the Modified tab, select the property. 2. Click Delete to display the Remove SDI Property window. 3. A confirmation message is displayed. Click Yes to delete the property. <p>A message indicates that the property server is being removed. After the property is deleted, a system notification message is displayed that the instance is deleted.</p>

5. When you are finished, click **Close**.

Managing IBM Security Directory Integrator adapters

You can install and uninstall Security Directory Integrator adapters through the virtual appliance. The adapters enable Identity Governance and Intelligence to communicate with various resources.

Before you begin

You must download the *adapter.zip* package from the IBM Passport Advantage website. Go to http://www.ibm.com/software/how-to-buy/passportadvantage/pao_customers.htm.

About this task

The virtual appliance has the UNIX and Linux adapter preinstalled.

Some adapters require third-party JAR files to be downloaded and then uploaded to virtual appliance during the adapter installation process. These jars are then added to the adapter bundle inside the virtual appliance. Use the download option

to install the complete adapter bundle that includes the third-party JAR files on another Security Directory Integrator instance.

If you have a cluster environment, adapter management tasks must be performed on the primary node. The adapter management tasks that are performed on a directory integrator instance propagate to the same instance on each node in the cluster during node synchronization. If the instance on the primary node becomes unavailable, the failover action is for Identity Governance and Intelligence to connect to the directory integrator instance on the secondary node. If the instance is unavailable on the secondary node, Identity Governance and Intelligence continues to try to connect to the instance on member nodes.

For more information about adapters, see Chapter 8, “Installing and configuring Identity Brokerage Adapters,” on page 169.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure > SDI Management**.
2. Select the instance of the Dispatcher for which you want to manage the adapters and click **Manage > SDI Adapters**. The SDI Adapters window is displayed with a table that list the name, version, and any comments about the installed adapters.
3. Perform any of the following actions.

Table 29. Security Directory Integrator adapter actions

Action	Button	Description
Add an adapter	Install	<ol style="list-style-type: none"> 1. Click Install. 2. Click Browse and navigate to the adapter package that you want to install. 3. Click OK. <p>A message indicates that a new SDI adapter is being installed. After the adapter is installed, a system notification message is displayed and the adapter is added to the SDI Adapters table.</p>
Uninstall an adapter.	Uninstall	<ol style="list-style-type: none"> 1. Select the adapter. 2. Click Uninstall to display the Remove SDI Adapter window. 3. A confirmation message is displayed. Click Yes to delete the adapter. <p>A message indicates that the adapter is being removed. After the adapter is deleted, a system notification message is displayed and the adapter is removed from the table.</p>
Download an adapter.zip bundle	Export	<ol style="list-style-type: none"> 1. Select the adapter. 2. Click Download. 3. Select to save the file. 4. Click OK. <p>The file is saved to your download directory.</p>

4. When you are finished, click **Close**.

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 122.

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

Table 30. Available logs to help you diagnose or troubleshoot

Tab	Tab description	Log file name	Description
Appliance	Helps debug any configuration failures that occur in the virtual appliance.	Server System out	Logs that trace the operation of the virtual appliance. The system out and system message files contain informational, warning, and error messages.
		Server Message	Logs that trace the operation of the virtual appliance. The system out and system message files contain informational, warning, and error messages.
		Server System trace	The system trace file contains the most detailed information. It contains all messages in the system out file as well as debug-level messages.

Table 30. Available logs to help you diagnose or troubleshoot (continued)

Tab	Tab description	Log file name	Description
Identity	Identifies issues in the Identity applications.	<ul style="list-style-type: none"> IBM Identity Governance and Intelligence Application server message IBM Identity Governance and Intelligence Application server system trace IBM Identity Governance and Intelligence trace log 	<p>Logs that trace the operation of the IBM Identity Governance and Intelligence application. The server message file contains informational, warning, and error messages. The server system trace file contains all messages in the system out file as well as debug-level messages. The server trace log contains messages of varying severity level, depending on configuration.</p>
		<ul style="list-style-type: none"> Security Directory Integrator server log Identity Brokerage Application server message Identity Brokerage Application server system trace 	<p>Logs that trace the operation of the Identity Brokerage application. The server message file contains informational, warning, and error messages. The server system trace file contains all messages in the system out file as well as debug-level messages. The Security Directory Integrator server log traces the operation of the on-board Security Directory Integrator and contains messages of varying severity level, depending on configuration.</p>

Procedure

- From the top-level menu of the **Appliance Dashboard**, select **Manage > Maintenance > Log Retrieval and Configuration**.
- 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.
- 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 30 on page 120.
- 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 file, 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 120.

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 applications.

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 application.

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 application.

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 application.

To edit the 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 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 that can be traced in the application server log.
- c. In the **Trace Level** column, select a trace level from the list to apply to the specified package.

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

To edit the existing trace configuration item, 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 packages 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 that can be traced in the IBM Security Directory Integrator log.
- c. In the **Trace Level** column, select a trace level from the list to apply to the specified package.

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

To edit the existing trace configuration item, 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 JavaCore and core dump files

Use the Core Dumps page to generate, 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.

Note: When you trigger a core dump, a system core dump is also triggered. Because of the size of the default heap, a higher CPU utilization and IO wait times occur for the system core dump. Avoid collecting core dumps when the system is in high usage, especially if you are using the embedded Postgres database.

Procedure

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

The JavaCore/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.

- Appliance management
- IBM Security Identity Governance and Intelligence Application
- Identity Brokerage Providers Application
- Security Directory Integrator (*SDI_Instance_name*)
- Others

2. In the JavaCore/Core Dumps page, do one of the following actions.

Table 31. Core dump file management actions

Action	Description
<p>Generate</p> <p>This action generates a JavaCore dump for the server type that you select. If you select the Generate core dump check box, it generates also a core dump.</p>	<ol style="list-style-type: none"> 1. Click Generate 2. Select one of the following server types in the drop-down list. <ul style="list-style-type: none"> • IBM Security Identity Governance and Intelligence Application • Identity Brokerage Providers Application • Security Directory Integrator (<i>SDI_Instance_name</i>) 3. Select the Generate core dump check box to generate also a core dump. Do not select this check box if you want to generate only a JavaCore dump. For SDI servers, both types of core dumps are generated by default. 4. Click Generate.

Table 31. Core dump file management actions (continued)

Action	Description
Delete	<ol style="list-style-type: none"> 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. Click Delete. Click Yes to confirm.
Download	<ol style="list-style-type: none"> From the File name column, select a core dump file. Note: You can select only 1 core dump file at a time for download. If you select multiple core dump files, a message is displayed. 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

- From the top-level menu of the **Appliance Dashboard**, click **Manage > Maintenance > About**.
- 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.

Interface Gateway

Indicates the address of the application interface gateway. For example, 9.122.125.1.

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 32. Application Interfaces action items

Action	Button	Description
Add an address	New	<p>Note:</p> <ul style="list-style-type: none"> • 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. <ol style="list-style-type: none"> 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. <p>IPv4</p> <p>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.</p> <p>IPv6</p> <p>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</p> 4. Specify the fully qualified domain name of the application interface in the Interface FQDN field. 5. Type the address of the interface gateway that is used by the application in the Interface Gateway field. 6. Do one of these actions. <ul style="list-style-type: none"> • For IPv4 Settings, do these steps. <ol style="list-style-type: none"> 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. <ol style="list-style-type: none"> a. Type an address value in the Address field. b. From a range of 0-64, specify a prefix value in the Prefix field. 7. Click Save. 8. If any notifications are displayed in the Notifications widget, take appropriate actions as necessary. <p>A message indicates that the application address is added successfully, and the record is listed in the Interface 1 table.</p>

Table 32. Application Interfaces action items (continued)

Action	Button	Description
Edit an address	Edit	<ol style="list-style-type: none"> 1. Select an application interface. 2. Select the address. 3. Click Edit to display the Edit Address window. 4. Modify the fully qualified domain name of the application interface in the Interface FQDN field. 5. Modify the address of the interface gateway that is used by the application in the Interface Gateway field. 6. Do one of these actions. <ul style="list-style-type: none"> • For IPv4 Settings, do these steps. <ol style="list-style-type: none"> a. Edit address value in the Address field. b. Edit net mask value in the NetMask field. • For IPv6 Settings, do these steps. <ol style="list-style-type: none"> a. Edit address value in the Address field. b. Edit prefix value in the Prefix field. 7. Click Save. <p>A message indicates that the address is updated successfully.</p>
Delete an address	Delete	<ol style="list-style-type: none"> 1. Select an application interface. 2. Select the address. 3. Click Delete to display the Confirm Action window. 4. Click Yes. <p>A message indicates that the address is deleted successfully.</p>
Test a connection	Test	<ol style="list-style-type: none"> 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. <p>A message indicates whether the test connection was successful or not.</p>
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.

Managing advanced tuning parameters

Change the advanced tuning parameter values only under the supervision of IBM Customer Support.

About this task

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage System Settings > System Settings > Advanced Tuning Parameters**
2. In the Advance Tuning Parameters pane, you can use one or more of the following commands:

Table 33. Advanced tuning parameters options

Option	Description
New	To add a new advanced tuning parameter, click New , type a key, value, and comment that describes the parameter, and then click Save Configuration .
Edit	To edit an advanced tuning parameter, select the entry, click Edit , modify the parameter information, and then click Save . Attention: <ul style="list-style-type: none"> • If you are using TLS 1.2, you must use a browser that is compatible with TLS 1.2 to access the local management interface. • When you change lmi.security.protocol from the current version (for example, from TLS to TLS 1.1 or TLS 1.2), you must switch to the same protocol version all your running external entities, if they are configured with SSL. This includes the external database server and the directory server.
Delete	To delete advanced tuning parameter, select one or more parameters, and then click Delete .

Managing local management interface security protocols for the virtual appliance

You can set the security protocols that are used with the virtual appliance.

About this task

Note: Change these advanced tuning parameter values only under the supervision of IBM® software support.

Procedure

1. Click **Manage System Settings > Advanced Tuning Parameters**.
2. Perform any of the following actions.

Table 34. Security protocol operations

Button	Procedure
New	<ol style="list-style-type: none"> 1. Click New. A dialog opens. 2. Type the name for the key such as lmi.security.protocol. 3. Type a value for the key. Valid values are <ul style="list-style-type: none"> TLS TLSv1.1 TLSv1.2 4. Type a comment that describes the protocol that you created. 5. Click Save Configuration.

Table 34. Security protocol operations (continued)

Button	Procedure
Edit	<ol style="list-style-type: none"> 1. Select a protocol key. 2. Click Edit. A dialog opens. 3. Modify then name for the key. 4. Modify the value for the key. Valid values are <ul style="list-style-type: none"> TLS TLSv1.1 TLSv1.2 5. Modify the comment that describes the key. 6. Click Save Configuration.
Delete	<ol style="list-style-type: none"> 1. Select one or more keys. If you want to delete all the keys, select the Key check box. 2. Click Delete. A confirmation message is displayed. 3. Click Yes to delete the key or No to cancel the operation.

Managing local management interface security cipher suites for the virtual appliance

You can set the security cipher suites that are used with the virtual appliance.

About this task

Note: Change these advanced tuning parameter values only under the supervision of IBM software support.

For information about advanced tuning parameters, see “Advanced tuning parameters for the virtual appliance” on page 132.

Procedure

1. Click **Manage System Settings > Advanced Tuning Parameters**.
2. Perform any of the following actions.

Table 35. Security cipher suite operations

Button	Procedure
New	<ol style="list-style-type: none"> 1. Click New. A dialog opens. 2. Type the name for the key such as <code>lmi.security.ciphers</code>. 3. Type a value for the key. Multiple values can be specified as a space-separated list. The virtual appliance supports all the cipher suites that are supported by Java 8. For a list of cipher suites that the virtual appliance supports, see https://www.ibm.com/support/knowledgecenter/SSYKE2_8.0.0/com.ibm.java.security.component.80.doc/security-component/jsse2Docs/ciphersuites.html. 4. Type a comment that describes the cipher key that you created. 5. Click Save Configuration.

Table 35. Security cipher suite operations (continued)

Button	Procedure
Edit	<ol style="list-style-type: none"> 1. Select a cipher key. 2. Click Edit. A dialog opens. 3. Modify then name for the key. 4. Modify the value for the key. Multiple values can be specified as a space-separated list. The virtual appliance supports all the cipher suites that are supported by Java 8. For a list of cipher suites that the virtual appliance supports, see https://www.ibm.com/support/knowledgecenter/SSYKE2_8.0.0/com.ibm.java.security.component.80.doc/security-component/jsse2Docs/ciphersuites.html. 5. Modify the comment that describes the key. 6. Click Save Configuration.
Delete	<ol style="list-style-type: none"> 1. Select one or more keys. If you want to delete all the keys, select the Key check box. 2. Click Delete. A confirmation message is displayed. 3. Click Yes to delete the key or No to cancel the operation.

Managing local management interface security cipher suites for Identity Governance and Intelligence

You can set the security cipher suites that are used with Identity Governance and Intelligence.

About this task

Note: Change these advanced tuning parameter values only under the supervision of IBM software support.

For information about advanced tuning parameters, see Advanced tuning parameters.

Procedure

1. Click **Manage System Settings > Advanced Tuning Parameters**.
2. Perform any of the following actions.

Table 36. Security cipher suite operations

Button	Procedure
New	<ol style="list-style-type: none"> 1. Click New. A dialog opens. 2. Type the name for the key. The name is <code>igi.security.ciphers</code>. 3. Type a value for the key. The value must be a cipher that is supported by the TLSv1.2 protocol. You can specify multiple values in a space-separated list. 4. Type a comment that describes the cipher key that you created. 5. Click Save Configuration.

Table 36. Security cipher suite operations (continued)

Button	Procedure
Edit	<ol style="list-style-type: none"> 1. Select a cipher key. 2. Click Edit. A dialog opens. 3. Modify then name for the key. 4. Modify the value for the key. The value must be a cipher that is supported by the TLSv1.2 protocol. You can specify multiple values in a space-separated list. 5. Modify the comment that describes the key. 6. Click Save Configuration.
Delete	<ol style="list-style-type: none"> 1. Select one or more keys. If you want to delete all the keys, select the Key check box. 2. Click Delete. A confirmation message is displayed. 3. Click Yes to delete the key or No to cancel the operation.

Advanced tuning parameters for the virtual appliance

Change the advanced tuning parameter values only under the supervision of IBM software support.

Local management interface (LMI)

The following table lists the advanced tuning parameters that are available.

Table 37. Advanced tuning parameters

Parameter	Description
lmi.security.ciphers	Enables specific ciphers for the local management interface. Valid values are specified as a space-separated list. The virtual appliance supports all the cipher suites that are supported by Java 8. See https://www.ibm.com/support/knowledgecenter/SSYKE2_8.0.0/com.ibm.java.security.component.80.doc/security-component/jsse2Docs/ciphersuites.html for a list of the supported cipher suites.
lmi.security.protocol	Enables specific protocols for the local management interface. Valid values are TLS , TLSv1 , and TLSv1.2 . Attention: When you change the protocol version, you must switch to the same protocol version all your running external entities, if they are configured with SSL. This includes the external database server and the directory server.
igi.security.ciphers	Enables specific ciphers for the Identity Governance and Intelligence application. The value must be a cipher that is supported by the TLSv1.2 protocol. Multiple values can be specified as a space-separated list.

Configuring for bidirectional languages

The Identity Governance and Intelligence user interfaces provide support for bidirectional languages. Use the BiDi Properties pane to adapt the bidirectional settings to your language and to your preferences.

About this task

To display the BiDi Properties pane, select **Manage > BiDi Properties** in the virtual appliance dashboard.

You can customize the following fields:

Calendar

Select one of the following values for displaying dates and time stamps in the user interfaces.

- Gregorian
- Hebrew
- Arabic-Civil
- Arabic-Religious
- Arabic-UmAlqura

The default is Gregorian. Other languages can use the default.

Numbers Shaping

Select one of the following values for displaying the numbers in numeric fields.

- None
- National
- Arabic-Indic
- Arabic-European
- Contextual

The default is National.

Base text direction

Select one of the following values for displaying the direction of user-generated text. The context is for simple input fields that are used in content authoring and certain labels.

- Contextual
- Right to left
- Left to right

The default is Contextual.

In a clustered environment, change these settings on the primary virtual appliance.

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 38. Static route actions

Field	Action
IPv4 Default Gateway	<ol style="list-style-type: none"> 1. Specify an address value. For example: 9.113.50.1. 2. Click Save. <p>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.</p>
IPv6 Default Gateway	<ol style="list-style-type: none"> 1. Specify an address value. For example: 3001:0DB9:0000:0000:02AB:00FF:FE29:9C6A. 2. Click Save. <p>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.</p>
New	<ol style="list-style-type: none"> 1. Click New to create a route. 2. In the Add Route window, define values in these fields. <ul style="list-style-type: none"> • Destination • Gateway • Metric • Interface or Segment 3. Click Save Configuration.
Edit	<ol style="list-style-type: none"> 1. Select an existing route. 2. Click Edit to change the settings. 3. In the Edit Route window, edit values in these fields. <ul style="list-style-type: none"> • Destination • Gateway • Metric • Interface or Segment 4. Click Save Configuration.
Delete	<ol style="list-style-type: none"> 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.

Managing a network file system (NFS)

To access files on a remote server, you can configure the virtual appliance as an NFS client.

Before you begin

The NFS server must exist, and all the nodes in the cluster must have the appropriate permissions on the server.

About this task

An NFS mount provides access to information and files that are on a remote server. The files that you can access and the actions that you can perform are determined by the setting on the NFS server.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > Network Settings > Network File System**. The Network File System page displays a table with these column headings.

Host Name

Indicates the system that you mounted.

Remote Directory

Indicates the directory that you are accessing on the remote server.

Local Directory

Indicates the directory on your local system that mounts to the remote directory.

Options

Indicates the access type that you are using to mount to the remote server. The default access is read-write (**rw**).

loop Ignored. Loop devices are autodetected.

sync Specifies that the server sends the information synchronously rather than asynchronously.

async Specifies that the server sends the information asynchronously rather than synchronously.

atime Enables updates to inode access times.

noatime
Disables updates to inode access times.

diratime
Enables inode access time updates on the filesystem.

nodiratime
Disables inode access time updates on the filesystem.

relatime
Enables inode access time updates in relation to modify or change times.

norelatime
Disables inode access time updates in relation to modify or change times.

dev Allows the use of special device files on the filesystem.

nodev Blocks the use of special device files on the filesystem.

exec Allows the use of executable files.

noexec Blocks the use of executable files on the mounted filesystem.

suid Allows the use of set-user-id-root programs.

nosuid Blocks the use of set-user-id-root programs.

shared Converts the subtree to a shared subtree. Mounts and unmounts within any of the mirror subtrees propagate to the other mirrors.

rshared

Converts the subtree to a shared subtree recursively. The subtree and its subtrees are shared subtrees.

slave Converts the subtree to a slave subtree. Mount and unmounts propagate from the master subtree to the slave, but not from the slave subtree to the master.

rslave Converts the subtree to a slave subtree recursively. The subtree and its subtrees are slave subtrees.

private

Converts the subtree to a private subtree. It does not propagate mounts and unmounts.

rprivate

Converts the subtree to a private subtree recursively. The subtree and its subtrees are private subtrees.

bindable

Enables the mount point to be bind mounted.

unbindable

Disables the ability of the mount point to be bind mounted.

ro Read only. The client cannot modify the files.

rw Read-write. The client can view and modify files.

Last modified on

Specifies the date and time that the mount was created or edited.

2. On any tab of the Network File System page, do one of these actions.

Table 39. Network File System action items

Action	Button	Description
Add an NFS mount point	New	<ol style="list-style-type: none"> 1. Click New to display the Add NFS mount point window. 2. Type the host name of the NFS server in FQDN, IPv4, or IPv6 format. <ul style="list-style-type: none"> FQDN Is a fully qualified domain name of the computer on the internet. It consists of a host name and a domain name. For example, <code>myserver.mycompany.com</code>. IPv4 <p>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, <code>9.122.20.250</code>.</p> IPv6 <p>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, <code>4ffe:1800:8484:3:220:f9ff:fe25:70cf</code></p> 3. Specify the directory that you are accessing on the remote NFS server 4. Specify the directory location on your local system where you want to access the remote server. 5. Specify the options to use when you connect to the remote system. You can specify multiple options that are separated by commas. For example, <code>rw, sync</code>. 6. Click Save Configuration. A status message is displayed. <p>A message indicates that the NFS mount point is added successfully, and the record is listed in the table.</p>
Edit an NFS mount point	Edit	<p>You can modify only the options that you use to mount to the remote server.</p> <ol style="list-style-type: none"> 1. Select the NFS mount point. 2. Click Edit to display the Edit NFS mount point window. 3. Specify the options that you want to use when you connect to the remote system. You can specify multiple options that are separated by commas. For example, <code>rw, sync</code>. 4. Click Save Configuration. <p>A message indicates that the NFS mount point is edited successfully.</p>
Delete an NFS mount point	Delete	<ol style="list-style-type: none"> 1. Select an NFS mount point. You can select more than one. 2. Click Delete to display the Confirm Delete window. 3. Click Yes. <p>A message indicates that the NFS mount point is deleted successfully.</p>

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 40. Export or import settings actions

Action	Button	Description
Creating a package	Create	<ol style="list-style-type: none"> 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.
Applying settings	Apply	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none">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. <p>A message indicates that the snapshot is created successfully, and it is added in the Snapshots table.</p>
Edit a snapshot	Edit	<ol style="list-style-type: none">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. <p>A message indicates that the snapshot is edited successfully.</p>
Delete a snapshot	Delete	<ol style="list-style-type: none">1. Select one or more snapshots.2. Click Delete.3. Click Yes to confirm. <p>A message indicates that the snapshot is deleted successfully.</p>

Action	Option	Description
Apply a snapshot	Apply	<p>Note:</p> <ul style="list-style-type: none"> • 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. <ol style="list-style-type: none"> 1. Select a snapshot. 2. Click Apply. 3. On the Apply Snapshot window, read the considerations. 4. Click Yes to confirm. <p>Wait until the snapshot is applied. After the snapshot is applied, a notification indicates you to restart the virtual appliance.</p> <p>Important: If you face any login problems after you apply a snapshot, do these steps.</p> <ol style="list-style-type: none"> 1. Clear the service integration bus (SIB) tables. For more information, see Clear the service integration bus. 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 67.
Download a snapshot	Download	<ol style="list-style-type: none"> 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. <p>Note: If you download multiple snapshots, the snapshots are compressed into a .zip file.</p>
Upload a snapshot	Upload	<p>Note: You can upload only 1 snapshot at a time.</p> <ol style="list-style-type: none"> 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. <ul style="list-style-type: none"> 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. <p>A message indicates that the snapshot is uploaded successfully.</p>
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	<ol style="list-style-type: none">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. <p>A message indicates that a support file is created, and it is added in the Support Files table.</p>
Edit a support file	Edit	<ol style="list-style-type: none">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. <p>A message indicates that the comment is edited.</p>
Delete a support file	Delete	<ol style="list-style-type: none">1. Select one or more support files.2. Click Delete.3. Click Yes to confirm. <p>A message indicates that the support file is deleted.</p>

Action	Option	Description
Download a support file	Download	<ol style="list-style-type: none"> 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. <p>Note: If you download multiple support files, the files are compressed into a support.zip file.</p>

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 146
 - “Configuring email objects” on page 147
 - “Configuring remote syslog objects” on page 148
 - 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	<p>On the Notification Type tab, complete these steps.</p> <ol style="list-style-type: none"> 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	<p>On the Authentication and Privacy tab, complete these steps.</p> <ol style="list-style-type: none"> 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	<p>Specifies a meaningful name for the response.</p> <p>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.</p>

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.

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:
cli                Work with the command line interface.
firmware           Work with firmware images.
fixpacks           Work with fix packs.
igi                Work with the IBM Security Identity Governance and
                  Intelligence 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.
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>
```

The following command is listed only if the virtual appliance was enabled for FIPS.

```
fips                View FIPS 140-2 state and events.
```

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 functions that are available in the graphical user interface.

Virtual appliance global commands

The IBM Security Identity Governance and Intelligence virtual appliance command-line interface (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.

cli

The function works with the command line interface.

ssh_timeout

Includes an option to view the current timeout value for the local SSH session and an option to set a new value in minutes.

fips

The function shows FIPS 140-2 state and events. The function is available only if the virtual appliance is configured in FIPS mode.

status Replies if FIPS mode is enabled and if there are any errors.

If there are no errors, the reply is:

```
igiva.example.com>fips status
FIPS 140-2 Status:OK
Appliance has enabled FIPS mode successfully.
igiva.example.com>
```

If there are errors, the reply is:

```
igiva.example.com>fips status
FIPS 140-2 Status:Error
Appliance has entered FIPS error state.
igiva.example.com>
```

view_log

Displays the FIPS log in the console.

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 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 function manages 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.

security

The function provides options to work with security settings for the local management interface.

clear_cipher_suites

Clears all the enabled security cipher suites for the local management interface.

reset_all

Resets the security protocol and security cipher suites to the default value for 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 sub-commands.

Virtual appliance command-line interface commands

Find information about the sub sections of the virtual appliance CLI command that is specific to IBM Security Identity Governance and Intelligence. 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 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.

connectors**connector_files**

Provides options to list or delete connector files that were copied to the appliance.

ssh_keys

Provides options to accept, list, or delete the keys that are used for passwordless Secure Shell (SSH).

sub_directories

Provides options to create, delete, and list subdirectories that can be used for connector files.

user_settings

Provides the option to change the igiuser password that is used transferring connector files in the virtual appliance.

jvm_property

add Adds a JVM property in the application server.

delete Deletes an existing JVM property from the application server.

update Updates an existing JVM property in the application server.

logs

clear Clears the backlog files on the system.

clear_ffdc

Clears all the FFDC log files on the system.

monitor

Provides options to monitor the log files on the system.

postgres

postgres_cmd

Provides the option to log in to the Postgres database administrator console.

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

arcs_configuration_snc

Provides the following options to enable the Access Risk Controls for SAP module to work over a FIPS connection.

create_credv2_file

Creates the cred_v2 credentials file.

create_pse_file

Creates the Personal Security Environment (PSE) file.

export_client_certificate

Creates the client certificate and exports it to a file.

import_sap_server_certificate

Imports the SAP server certificate to the PSE on the virtual appliance.

ib_settings

Provides options to work with the Identity Brokerage settings.

ib_password_reset

Resets the Identity Brokerage administrative password.

ib_recon_failure_threshold

Provides options to work with the value of the reconciliation failure threshold setting.

ib_recon_timeout

Provides options to work with the value of the reconciliation timeout setting.

ib_api Provides the status of the Identity Brokerage API, and enables or disables the Identity Brokerage API.

users Provides options to manage Identity Brokerage users.

change_password

Changes the password of an Identity Brokerage user.

create Provides options to create an Identity Brokerage user and assign a password.

deactivate

Changes the status of a user to inactive.

list Shows the Identity Brokerage users and their status.

reactivate

Changes the status of an inactive user to active.

scheduler

Provides the status of the scheduler, and enables or disables the scheduler.

session_timeout

Provides options to work with the timeout interval for desk and administrative user interfaces.

verbose_gc**disable**

Disables verbose garbage collection.

enable Enables verbose garbage collection.

status Shows whether verbose garbage collection is enabled or disabled.

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:
cli                Work with the command line interface.
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:
cli                Work with the command line interface.
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 list 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:
cli                Work with the command line interface.
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            Resart 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:
itim1002
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 `itim1003`.

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):
```
- 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
```
  - Restart the IBM Security Identity Governance and Intelligence server to apply the new settings.

## Setting a timeout for the SSH session

Use the command line of the virtual appliance to set the timeout interval for the Secure Shell (SSH) session.

### About this task

Use the **ssh\_timeout** command to set the number of minutes that the SSH session can be idle before it is closed.

The default timeout interval is 0 minutes. Use this value, if you do not want the SSH session to expire.

The minimum timeout interval is 2 minutes. The maximum interval is 9999 minutes. Choose a value between 2 and 9999, if you want to set a timeout interval.

The **ssh\_timeout** command includes the following sub-commands:

- get** Returns the value that is currently defined for **ssh\_timeout**.
- set** Sets a new value for **ssh\_timeout**. Requires the virtual appliance to be restarted to activate the new value.

The command applies to the local SSH session only.

### Procedure

- From the command line interface, log on to the IBM Security Identity Governance and Intelligence virtual appliance.
- Type the **cli** command at the `igivasrv` prompt.
- Type the **ssh\_timeout** command at the `igivasrv:cli` prompt.
- Optional: Type the **get** command at the `igivasrv:ssh_timeout` prompt to find the current timeout interval for the SSH session.  
The following message is displayed (the value is an example):  

```
Current timeout (in minutes): 0
```
- Type the **set** command at the `igivasrv:ssh_timeout` prompt to set the timeout interval for the SSH session.  
The following message is displayed (the value is an example):  
Note: The session timeout cannot be less than 2 minutes and more than 9999.  
Set 0 for no timeout.  

```
Current timeout (in minutes): 5
New timeout (in minutes):
```
- Specify the new timeout interval and press Enter. For example, specify 15.  
The following message is displayed (the values are examples):

```
Current timeout (in minutes): 5
New timeout (in minutes): 15
Session timeout updated successfully
Reboot the appliance for changes to come into effect.
```

- Restart the IBM Security Identity Governance and Intelligence server to apply the new settings.

## Resetting the Identity Brokerage administrative password

Use the command line of the virtual appliance to reset the Identity Brokerage administrative password.

### About this task

Use the **ib\_password\_reset** command to reset the Identity Brokerage administrative password on the virtual appliance.

### Procedure

To reset the password, complete these steps:

- From the command-line interface, log on to the IBM Security Identity Governance and Intelligence virtual appliance.
- Enter the **igi** command at the `igivasrv` prompt.
- Enter the **utilities** command at the `igivasrv:igi` prompt.
- Enter the **ib\_settings** command at the `igivasrv:utilities` prompt.
- Enter the **ib\_password\_reset** command at the `igivasrv:ib_settings` prompt.
- Enter YES to confirm the reset request.
- Restart the IBM Security Identity Governance and Intelligence server.

#### Related reference:

“Virtual appliance command-line interface commands” on page 154  
Find information about the sub sections of the virtual appliance CLI command that is specific to IBM Security Identity Governance and Intelligence. 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.

---

## 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:

- “Setting up a primary virtual appliance” on page 165.
- Optional: “Backing up the virtual appliance” on page 165.
- Optional: “Reverting the virtual appliance to its backup” on page 165
- “Creating a snapshot of the virtual appliance” on page 166.

5. “Setting up a secondary virtual appliance” on page 166.

## 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 21.
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 23.
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 33.
4. Log on to the applications by using the **Appliance Dashboard** console. See “Validating configuration with quick links” on page 69.
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 67.
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 67.
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 23.
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 141.

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.





---

## Chapter 8. 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 Adapters. These IBM Security Identity Adapters are sometimes referred to as Identity Brokerage Adapters in Identity Governance and Intelligence.

Identity Brokerage Adapters are the systems integration “glue” that link the Identity Governance and Intelligence to the customer’s enterprise systems and enforce identity security policies on the customer’s servers and applications. These adapters implement identity provisioning and target reconciliation.

IBM Security Identity Adapters are categorized as follows:

### **Security Directory Integrator based adapters**

These adapters are extensions to the Security Directory Integrator product and must be deployed within the Security Directory Integrator. All adapters that are deployed within a Security Directory Integrator instance are managed by that Security Directory Integrator instance as one unit. The Security Directory Integrator instance that manages a set of adapters is called Dispatcher.

### **Adapter Development Kit based adapters**

These adapters do not require the Security Directory Integrator. They require the *InstallAnywhere* wizard for deployment. These adapters use these command line configuration tools:

- agentCfg
- certTool

Some IBM Security Identity Adapters can be installed in the selected Security Directory Integrator instance on the virtual appliance: See “Installing the adapter in the virtual appliance” on page 170 for the procedure.

All Identity Governance and Intelligence supported adapters can be installed externally on the virtual appliance. Depending on the adapter, an external Security Directory Integrator may be required.

See the corresponding Adapter *Installation and Configuration Guide* for the specific prerequisites, installation and configuration tasks, and issues and limitations. See the Adapters release notes for any updates to these references.

### **Related information:**

Managing Security Directory Integrator instances

IBM Security Identity Governance and Intelligence uses IBM Security Identity Adapters to communicate with various managed resources. These adapters are deployed and run on instances of the Security Directory Integrator. The properties of the Security Directory Integrator or Dispatcher affect all of the adapters that run on the instance. Therefore, some adapters might need to run on separate instances of the Security Directory Integrator. Use this task to create and manage multiple instances of the Security Directory Integrator.

Configuring the Dispatcher properties for the Directory Integrator instance  
 The Dispatcher is a Security Directory Integrator component. It enables the Identity Governance and Intelligence server to communicate with IBM Tivoli Directory Integrator-based adapters. You can modify the `solution.properties` and `itim_listener.properties` files that configure the Dispatcher.

#### Managing IBM Security Directory Integrator adapters

You can install and uninstall Security Directory Integrator adapters through the virtual appliance. The adapters enable Identity Governance and Intelligence to communicate with various resources.

---

## Installing the adapter in the virtual appliance

For Identity Governance and Intelligence target management, you can install an Identity Brokerage Adapter or a custom adapter on the built-in IBM Security Directory Integrator in the virtual appliance instead of installing the adapter externally. As such, there is no need to manage a separate virtual machine or system.

### About this task

This procedure is applicable for a selected list of Identity Adapters. See the *Identity Adapters* product documentation at [http://www.ibm.com/support/knowledgecenter/SSIGMP\\_1.0.0/com.ibm.itim\\_pim.doc/c\\_adapters\\_intro.htm](http://www.ibm.com/support/knowledgecenter/SSIGMP_1.0.0/com.ibm.itim_pim.doc/c_adapters_intro.htm) to determine which adapters are supported in Identity Governance and Intelligence, and which can be installed on the virtual appliance.

### Procedure

1. Download the adapter package from the IBM Passport Advantage. For example, `Adapter-<Adaptename>.zip`.

The adapter package includes the following files:

*Table 41. Adapter package contents*

| Files                              | Descriptions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>bundledefinition.json</code> | The adapter definition file. It specifies the content of the package, and the adapter installation and configuration properties that are required to install and update the adapter.                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Adapter JAR profile                | <p>An IBM Security Directory Integrator adapter always include a JAR profile which contains:</p> <ul style="list-style-type: none"> <li>• <code>targetProfile.json</code> <ul style="list-style-type: none"> <li>– Service provider configuration</li> <li>– Resource type configuration</li> <li>– SCIM schema extensions</li> <li>– List of assembly lines</li> </ul> </li> <li>• A set of assembly lines in XML files</li> <li>• A set of forms in XML files</li> <li>• Custom properties that include labels and messages for supported languages.</li> </ul> <p>Use the <b>Target Administration</b> module to import the target profile.</p> |

Table 41. Adapter package contents (continued)

| Files                             | Descriptions                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Additional adapter specific files | <p>Examples of adapter specific files:</p> <ul style="list-style-type: none"> <li>• Connector jar files</li> <li>• Configuration files</li> <li>• Script files</li> <li>• Properties files</li> </ul> <p>The file names are specified in the adapter definition file along with the destination directory in the virtual appliance.</p> |

2. From the top-level menu of the **Appliance Dashboard**, click **Configure > SDI Management**.
3. Select the instance of the IBM Security Directory Integrator for which you want to manage the adapters and click **Manage > SDI Adapters**. The SDI Adapters window is displayed with a table that list the name, version, and any comments about the installed adapters.
4. On the SDI Adapters window, click **Install**.
5. On the File Upload window, click **Browse** to locate the adapter package and then click **OK**. For example, Adapter-<Adaptername>.zip.
6. Provide the missing 3rd party libraries when prompted.
  - a. On the File Upload for Pre-requisite files window, click **Select Files**. A new File Upload window is displayed.
  - b. Browse and select all the missing libraries. For example, ojdbc7.jar
  - c. Click **Open**. The selected files are listed in the File Upload for Pre-requisite files window.
  - d. Click **OK**. The missing files are uploaded and the adapter package is updated with the 3rd party libraries.

**Related tasks:**

“Managing IBM Security Directory Integrator adapters” on page 116

You can install and uninstall Security Directory Integrator adapters through the virtual appliance. The adapters enable Identity Governance and Intelligence to communicate with various resources.

---

## Uninstalling the adapter from the virtual appliance

Uninstall the adapter if you need to update the installed adapter. If a new version of the adapter is available, the only option to update it is to delete the adapter first then install the adapter. You can also uninstall the adapter if the adapter is not working as expected or it is preventing other adapters on the same instance to work as expected.

### About this task

On a cluster environment, you can only uninstall the adapter from the primary node and you must synchronize the other nodes.

### Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure > SDI Management**.

2. On the Security Directory Integrator Management page, select a IBM Security Directory Integrator instance.
3. Click **Manage > SDI Adapters**.
4. On the SDI Adapters window, select the adapter package.
5. Click **Uninstall**.
6. On the Remove SDI Adapter window, click **Yes** to confirm the request to remove the adapter from the selected IBM Security Directory Integrator instance.

---

# Index

## A

- active-passive configuration, disaster recovery 164
- advanced tuning 132
- archiving logs
  - command line interface 156

## C

- closing campaigns 55
- cluster
  - setting up 38
- cluster upgrade 53
- command line interface
  - reconciliation failure threshold 162
  - SIB schema names 161
  - tailing logs 156
- command line interface commands
  - current mode 151
  - global 150
- command-line interface 149, 154
- commands 154
- configuration
  - static routes 134
- configuration response samples 35
- configuration software firewall 3
- configuring openid 96
- core dump file
  - management 124
- current mode commands 151
- custom files
  - management 105

## D

- database
  - configuration, data store 81
  - default password
    - changing 9
  - setup in cluster 45
- database server
  - installation 10
  - SSL certificate 86
- db2 server
  - update semi-automatically 58
- DB2 server
  - installation 13
- directory server
  - configuration 74
  - installation 18
  - SSL certificate 77
- disaster recovery, active-passive configuration 164

## E

- email response objects 147
- events
  - SNMP 146

- exportimport
  - configuration settings 139
- external user registry 78

## F

- firmware settings, management 118
- fix pack, installation 119

## G

- global commands 150

## H

- hosts
  - files 133

## I

- Identity Brokerage
  - resetting password 164
- identity brokerage providers,
  - enabling 74
- installation 21

## J

- JAR files, updating 110
- Java security policy 110
- JavaCore dump file
  - management 124

## L

- LDAP
  - installation and configuration 18
  - management 74
- lmi authentication 78
  - configuration 78
- lmi\_security.protocol 132
- lmi.security.ciphers 132
- log response objects 148
- logs 148
  - configuration 122
  - configuration management 120
  - retrieval 120

## M

- mail
  - configuration 33
  - management 103
- mail server
  - SSL certificate 104
- manage certificates 107
- management
  - hosts files 133

- member node
  - wizard, initial configuration 38
- migration 49
  - rights lookup 61
  - tasks, jobs 54
  - user onboarding 61

## N

- Nodes
  - primary 40, 41
  - remove 42
  - secondary 40
- notifications 146, 147, 148

## O

- object
  - email 147
  - log 148
- objects 147, 148
- openid
  - discovery configuration 96
  - manual configuration 96
- Oracle server
  - configure 10
  - update semi-automatically 56

## P

- password reset
  - Identity Brokerage 164
- PostgreSQL database
  - backups 93
  - SSL certificate 92
- prerequisite software, installation 9

## R

- response objects
  - email 147
  - log 148
  - SNMP 146
- restart or shutdown 149
- role mining data load 60

## S

- secondary nodes 40
- server
  - configuration 33
- setting up a cluster 38
- simple network management protocol (SNMP) 146
- snapshot
  - creating, primary virtual appliance 166
- snapshots, management 142

- SSH
  - setting a timeout 163
- support files, management 144
- synchronization 47
- synchronize
  - member node 43
  - primary node 43
- synchronizing data 60
- syslog 148
- system audit events
  - configuration 145

## U

- Upgrading
  - clusters 53

## V

- virtual appliance
  - dashboard 47
  - first steps 33
  - identity brokerage providers 74
  - initial settings 23
  - installation 23
  - logging on 46, 47
  - managing 69
  - primary backup 165
  - primary, setting up 165
  - reconnect node 42
  - reverting to backup 166
  - secondary, setting up 166
  - upgrade 50, 52
  - user name and password 46
- virtual appliance dashboard 64
  - administrator settings, configure 141
  - date and time, configure 141
  - viewing about page 125
  - viewing and using quick links 69
  - viewing and using server control 67
  - viewing cluster status 67
  - viewing CPU usage 71, 72
  - viewing disk usage 66
  - viewing IP addresses 67
  - viewing licensing 118
  - viewing memory utilization 70
  - viewing middleware and server monitor widget 65
  - viewing notifications 64
  - viewing partition information 66
  - viewing update history 118
- virtual appliance installation
  - kvm 32
- virtual machine
  - system settings configuration 21

## W

- wizard
  - initial configuration 33





Printed in USA