

IBM Security Privileged Identity Manager
Version 2.0

Installation and Configuration Guide



IBM Security Privileged Identity Manager
Version 2.0

Installation and Configuration Guide



Note

Before using this information and the product it supports, read the information in Notices.

Edition notice

Note: This edition applies to Version 2.0 of *IBM Security Privileged Identity Manager* (product number 5725-H30) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2013, 2014.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures v

Tables vii

Chapter 1. Prerequisite software 1

Installing and configuring the database server 1
Installing and configuring the directory server 3
Setting up the directory server for SSL connection 4

Chapter 2. Installation. 7

Setting up the virtual appliance 7
 Installing the IBM Security Privileged Identity
 Manager Virtual Appliance 8
 Setting up the initial IBM Security Privileged
 Identity Manager Virtual Appliance. 8
 Selecting the virtual appliance configuration
 mode 11
 Setting up a stand-alone or primary node for
 IBM Security Privileged Identity Manager 12
Setting up a virtual appliance cluster. 14
 Setting up a member node for the IBM Security
 Privileged Identity Manager 14
 Synchronizing a Member node with a Primary
 node. 15
Setting up a load balancer for a virtual appliance
cluster 17
AccessAgent installation 18

Chapter 3. Configuration 19

Enabling the session recording feature in the virtual
appliance 19
Enabling the application identity management
feature in the virtual appliance 19
Managing the Database Server configuration 20
Managing the Directory Server configuration 22
Planning for high availability 23
Configuring the Load Balancer settings 24
Managing mail configuration 25
Managing the server properties. 25
Managing feed files. 27
Managing log configuration 28
 Retrieving logs 28
 Configuring logs 29

Chapter 4. Maintenance 31

Changing a Member node to a Primary node 31
Changing a Primary node to a Member node 31
Removing a node from the cluster. 32
Reconnecting a node into the cluster 32
Reconfiguring the data store connection 33
Reconfiguring the directory server connection 35
Setting up a secondary virtual appliance for
active-passive configuration 37
 Setting up a primary virtual appliance 37

 Backing up the primary virtual appliance 37
 Reverting the virtual appliance to its backup 38
 Creating a snapshot of the primary virtual
 appliance 38
 Setting up a secondary virtual appliance. 39
Installing a fix pack. 39
Upgrading the IBM Security Privileged Identity
Manager Virtual Appliance 40
Enhance availability by using monitoring URLs 41

Chapter 5. Reports 43

IBM Cognos reporting framework 43
 IBM Cognos Business Intelligence reporting
 components 43
 Prerequisites for IBM Cognos report server 44
Installation of IBM Cognos reporting components 45
Configuration of IBM Cognos reporting components 46
 Setting report server execution mode 47
 Setting environment variables 47
Importing the report package 48
Creating a data source. 49
Enabling the drill-through for PDF format 49
Security layer configuration around the data model
and reports 50
 Authentication and authorization for IBM
 Cognos reports 50
 User authentication setup by using LDAP 50
 Creating users in an LDAP 52
 Access control definition for the reports and
 reporting packages 54
 References for IBM Cognos report security
 configuration 56
Globalization overview 57
 Setting language preferences. 57
Enabling session recording replay from the report 58

Chapter 6. AccessProfiles 59

Creating your own privileged identity management
AccessProfiles 59
Privileged Session Recorder widgets 59
 Initializing a session recording 61
 Starting a session recording 61
 Stopping a session recording 63
 Pausing a session recording 63
 Resuming a recording session 64
Shared access widgets 64
 Choosing a shared credentials logon workflow 66
 Checking out credentials 67
 Injecting credentials 67
 Checking in credentials 70
Modifying AccessProfiles 71
 Modifying the bundled AccessProfile for the IBM
 Personal Communications application 72
 Modifying the bundled AccessProfile for the
 PuTTY application 74

Multiple AccessProfiles for the same client
application 75
 Identifying AccessProfile collision 76
 Merging AccessProfiles 76

Uploading AccessProfiles to the IMS Server 76

Notices 79

Figures

1. Deployment diagram of a typical Load Balancer in a customer environment 23
2. How the Privileged Session Recorder widgets work. 59
3. Example of a basic recording AccessProfile without check-in and check-out.. . . . 60
4. How a shared access widget is used in an AccessProfile 64
5. Example of a basic privileged identity AccessProfile that logs on with shared credentials. The check-in widget is not shown.. 65

Tables

1. Files in the /certs directory	5	9. Configure IBM Cognos reporting components	46
2. Synchronization state table	16	10. LDAP advanced mapping values	51
3. Data stores configuration options	20	11. Different application types use different parameter values for successful recordings with the Widget_PSR_Start widget.. . . .	61
4. Directory or LDAP server configuration details	22	12.	65
5. Available IBM Security Privileged Identity Manager properties in the IBM Security Privileged Identity Manager Virtual Appliance.	26	13. Injection widget parameters for different application types.	68
6. Available logs to help you diagnose or troubleshoot	28	14. Check-in widget parameters for different application types.	70
7. Software requirements for IBM Cognos report server	44	15. Capabilities of the different AccessProfiles	71
8. Installation and data synchronization process	45		

Chapter 1. Prerequisite software

Install and configure the prerequisite components before you install the IBM® Security Privileged Identity Manager Virtual Appliance.

Installing and configuring the database server

You must install and configure the database server before you can install and configure the directory server.

Procedure

1. Follow the DB2® instance creation instructions.
 - a. Access http://www.ibm.com/support/knowledgecenter/SSEPGG_10.1.0/com.ibm.db2.luw.kc.doc/welcome.html.
 - b. Search for **Creating an instance using db2icrt**.
2. Configure the database server for the IBM Security Privileged Identity Manager Virtual Appliance.
 - a. Create the database instance.
 - 1) Create an operating system user. For example, piminst.
 - 2) Add this user to the **root** group and set the **root** group as the primary group for user piminst:
useradd -g root piminst
 - 3) Change the password for user piminst:
passwd piminst
 - 4) Run the following command to create a database instance:

For Windows:

```
DB2_Install_Location\bin\db2icrt -u piminst piminst
```

DB2_Install_Location is the DB2 installation directory.

The created user piminst must be a member of these groups:

- DB2ADMNS
- DB2USERS

For Linux:

```
DB2_Install_Location/instance/db2icrt -u piminst piminst
```

- 5) Start the DB2 instance.

For Windows:

- Run **set DB2INSTANCE=piminst**, where piminst is the database instance.
- Run **db2cmd** to start the DB2 command line.
- Run **db2start**.

For Linux:

- Run **su - piminst**
- Run **db2start**.

- 6) Run the following commands to set up the DB2 instance:

- **db2 update dbm cfg using SVCENAME 50050**, where 50050 is the port on which you want your database server to listen.
- **db2set DB2COMM=tcPIP**
- **db2set -a11 DB2COMM**
- **db2stop**
- **db2start**

b. Create the database.

When you work with the IBM Security Privileged Identity Manager, use three separate databases for the three data stores: Identity, Sign-On, and Session Recording.

To create a database, take the following actions:

1) Start the DB2 instance.

For Windows:

- In the command line, run **set DB2INSTANCE=piminst**, where piminst is the database instance and owner of the database that you want to create.
- Run **db2cmd** to start the DB2 command line.
- Run **db2start**.

For Linux:

- Run **su - piminst**, where piminst is the database instance and owner of the database that you want to create.
- Run **db2start**.

2) In the DB2 command line, type the following example commands as the instance owner.

For the Identity data stores

```
db2 create db idmdb using codeset utf-8 territory us
pagesize 32 K
```

For the Single Sign-On data stores

```
db2 create db essodb using codeset utf-8 territory us
pagesize 32 K
```

For the Session Recording data stores

```
db2 create db psrdb using codeset utf-8 territory us
pagesize 32 K
```

Note: Existing Single Sign-On and Session Recording data stores with 8k or 32k page sizes are acceptable.

3) Create a temporary table space with the following command, if necessary.

```
db2 connect to psrdb
db2 create user temporary tablespace systoolstmpspace
pagesize 8 k managed by automatic storage bufferpool ibmdefaultbp
```

4) Using another Administrator or SYSADMIN account (in this case db2admin is used), run the following commands to grant certain accesses to the instance owner on the Identity data store.

```
db2 connect to idmdb user db2admin using password
db2 GRANT DBADM, SECADM ON DATABASE TO USER piminst
db2 disconnect current
db2 connect to psrdb user db2admin using password
db2 GRANT DBADM, SECADM ON DATABASE TO USER piminst
db2 disconnect current
db2stop
```

```
db2start
db2 grant execute on module sysibmadm.utl_file to user piminst with grant option
db2 grant execute on module sysibmadm.utl_dir to user piminst with grant option
```

Installing and configuring the directory server

You must install and configure the directory server before you can install the virtual appliance.

Before you begin

You must have the database server installed.

Procedure

1. For information about installing the directory server, see documentation that the directory server product provides. For example, access the documentation at <http://www.ibm.com/support/knowledgecenter/SSVJJU/welcome?lang=en> and search for **Installing and Configuring**.
2. Configure the directory server for IBM Security Privileged Identity Manager Virtual Appliance by creating and configuring the directory server instance.
 - a. Create a user.
 - Windows
In the command line, enter:
`LDAP_Install_Location\sbin\idsadduser -u ldapinst -w ldapinstpwd`
where `ldapinst` is the user name, and `ldapinstpwd` is the password.
 - UNIX and Linux
In the command line, enter:
`LDAP_Install_Location/sbin/idsadduser -u ldapinst -w ldapinstpwd -g idsldap`
where `ldapinst` is the LDAP instance name, `ldapinstpwd` is the password, and `idsldap` is the default LDAP group.
 - b. Create a directory server instance.
In the command line, enter:
`LDAP_Install_Location/sbin/idsicrt -I ldapinst -e encryptionseed -l /home/ldapinst`
where `ldapinst` is an LDAP instance name, `encryptionseed` is the encryption seed, and `/home/ldapinst` is the instance home.
 - c. Create an operating system user. For example, `db2admin`.
 - d. Add this user to the **root** and **idsldap** group and set the **idsldap** group as the primary group for user `db2admin`:
`useradd -g idsldap db2admin`
`usermod -a -G root db2admin`
 - e. Change password for user `db2admin`.
`passwd db2admin`
 - f. Create a database for the newly created LDAP instance.
In the command line, enter:
`LDAP_Install_Location/sbin/idscfgdb -I ldapinst -a db2admin -w dbadminpwd -t dbname -l /home/ldapinst/`
where `ldapinst` is an LDAP instance name, `db2admin` is the Database Administrator, `dbadminpwd` is the Database Administrator password, `dbname` is the database name, and `/home/ldapinst` is the instance home.

- g. Set the password for directory server instance Principal DN.
In the command line, enter:
`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, and `root` is the Principal DN password.
- h. Add the suffix (`dc=com`) in the directory server instance.
In the command line, enter:
`LDAP_Install_Location/sbin/idscfgsuf -I ldapinst -s dc=com`
where `ldapinst` is an LDAP instance name, and `dc=com` is the suffix.
- i. Start the directory server instance.
- Windows
In the command line, enter:
`LDAP_Install_Location/sbin/ibmslapd -I ldapinst -n`
where `ldapinst` is the LDAP instance name.
 - UNIX and Linux
In the command line, enter:
`LDAP_Install_Location/sbin/ibmslapd -I ldapinst -n -t`
where `ldapinst` is an LDAP instance name.
- j. Prepare a `ldif` file. For example, `dccom.ldif` with the following content:
`dn:dc=com`
`objectclass:domain`
Run the command:
`LDAP_Install_Location/bin/idsldapadd -h ldap_server_host`
`-p ldap_server_port -D bind_root_dn -w bind_root_password`
`-f dccom.ldif`
- For example:
`/opt/IBM/ldap/V6.3/bin/idsldapadd -D cn=root -w password -p port`
`-f dccom.ldif`

Setting up the directory server for SSL connection

Set up the directory server for an SSL connection to enable secure communication between the IBM Security Privileged Identity Manager Virtual Appliance and the directory server.

Before you begin

Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

About this task

The GSKit command-line tool will be used to create the certificate files needed to enable SSL connection on the directory server.

Note: On 32-bit platforms use the `gsk8capicmd` utility, and on 64-bit platforms use the `gsk8capicmd_64` utility.

Procedure

1. Create a certificate. Use the GSKit command-line tool to create a self-signed certificate and extract the certificate to make it available for secure communication.

- a. Find the GSKit on your system.

- For Linux: Enter `gsk8capicmd` on the command line. If anything other than an error message is returned, GSKit is installed and ready to use.
- For Windows: Open Registry Editor and look for `HKEY_LOCAL_MACHINE\SOFTWARE\IBM\gsk8\CurrentVersion\InstallPath`. This key indicates where GSKit is installed.

- b. Prepare the location of the certificate files. For example: `/certs`

- c. Go to the designated location of certificate files and create the CMS key database.

```
cd /certs
gsk8capicmd -keydb -create -db serverkey.kdb -pw serverpwd -stash
```

where, `serverkey.kdb` is the key database to be created and `serverpwd` is the password.

- d. Create a default self-signed certificate and add it to the `serverkey.kdb` key database.

```
gsk8capicmd -cert -create -db serverkey.kdb -pw serverpwd -label serverlabel -dn "cn=LDAP_Server,o=sample" -default_cert yes
```

- e. Extract the certificate from the key database to a base64-encoded ASCII data (`.arm`) file.

```
gsk8capicmd -cert -extract -db serverkey.kdb -pw serverpwd -label serverlabel -target server.arm
```

You can also extract the certificate in the binary `.der` format.

```
gsk8capicmd -cert -extract -db serverkey.kdb -pw serverpwd -label serverlabel -target server.der -format binary
```

- f. Verify that the `/certs` directory contains the following files:

Table 1. Files in the `/certs` directory

Filename	Description
<code>server.crl</code>	The file containing the certificate revocation list.
<code>server.arm</code>	The certificate.
<code>server.kdb</code>	Key database file that has the certificate.
<code>server.rdb</code>	Not used in this example.
<code>server.sth</code>	Stash file that has the password.

For more information, see:

- Topics on securing directory communications in the *IBM Security Directory Server Administration Guide* at

http://www.ibm.com/support/knowledgecenter/SSVJJU_6.3.1/com.ibm.IBMDS.doc_6.3.1/welcome.htm

- *IBM Global Security Kit GSKCapiCmd User's Guide* at

<http://www.ibm.com/support/docview.wss?uid=pub1sc22545900>

2. Enable the directory server for an SSL connection. Use an LDIF file to configure SSL on the directory server and to specify a secure port.

- a. If the directory server is not running, start the server. For example, on UNIX, type this command:

```
/opt/IBM/ldap/V6.3/sbin/ibmslapd -I itimldap
```

Where `-I` specifies the instance.

- b. Create an LDIF file, such as `ssl.ldif`, with the following data:

```
dn: cn=SSL,cn=Configuration
changetype: modify
replace: ibm-slapdSecurity
ibm-slapdSecurity: sslonly
-
replace: ibm-slapdSslKeyDatabase
ibm-slapdSslKeyDatabase: /certs/LDAPSERVER_TEST1234.kdb
-
add: ibm-slapdSslKeyDatabasePW
ibm-slapdSslKeyDatabasePW: server
```

Note: The empty lines that contain only the - (hyphen) character are expected for LDIF file formatting.

To change the secured port from the default port number 636, add these additional lines:

```
replace: ibm-slapdSecurePort
ibm-slapdSecurePort: 637
```

- c. Place the LDIF file in the following directory:

```
/opt/IBM/ldap/V6.3/bin
```

- d. Run the `idsldapmodify` command, which modifies the password policy by adding the LDIF file to the process.

```
idsldapmodify -D cn=root -w passwd -i ssl.ldif
```

-D Binds to the LDAP directory, which is `cn=root` in this example.

-w Uses the *passwd* value, which is the directory server administrator password, as the password for authentication.

-i Reads the entry modification information from an LDIF file instead of from standard input. In this example, the file is named `ssl.ldif`.

A successful result produces a message similar to the following one:

```
Operation 0 modifying entry cn=SSL,cn=Configuration
```

- e. Test the directory server to confirm that it is listening on the default secure port 636. Follow these steps:

1) Stop the directory server. Type `/opt/IBM/ldap/V6.3/sbin/ibmslapd -k -I itimldap`.

2) Start the directory server. Type `/opt/IBM/ldap/V6.3/sbin/ibmslapd -I itimldap`.

Where **-I** specifies the instance.

3) Determine whether the directory server is listening on port 636.

For example, display statistics for the network interface with the directory server by typing `netstat -an |grep 636`.

A return message that indicates the port is listening might be this example:

```
tcp    0    0 9.42.62.72:636  0.0.0.0:*    LISTEN
```

Chapter 2. Installation

Install the IBM Security Privileged Identity Manager components that are required in your environment.

Setting up the virtual appliance

You must create a virtual machine to host the IBM Security Privileged Identity Manager.

Procedure

1. Download the `ispim_*.iso` build.
2. Create a virtual machine on ESXi 5.x.
 - a. Select **Custom**.
 - b. Provide a name for the virtual machine.
 - c. Choose the destination storage for this virtual machine.
 - d. Set virtual machine version to 8.
 - e. Set the guest operating system to **Linux**. Under **Version**, select **Other 2.6.x Linux (64-bit)**.
 - f. Enter the number of virtual sockets and cores per virtual sockets for the virtual machine. For example: 4 cores.
 - g. Enter the memory size. For example: 16 GB.
 - h. Set **E1000** for the network adapter.
 - i. Set the SCSI controller type to **LSI Logic Parallel**.
 - j. Select the **Create a new virtual disk** option as the type of disk to use.
 - k. Enter the disk size for virtual machine. For example: 60 GB.
 - l. Accept the default settings in the Advanced Options page.
 - m. Select **Edit the virtual machine settings before completion**.
 - n. Click **Add...** in the Virtual Machine Properties page.
 - o. Select **USB Controller** as the device type.
 - p. Select **EHCI+UHCI** as the controller type.

Note: Virtual appliance supports USB 2.0 and USB 1.1 only.
 - q. Click **Finish** on the Add Hardware page.
 - r. Click **Finish** on the Virtual Machine Properties page.
3. Mount the IBM Security Privileged Identity Manager media.
 - a. Right-click on virtual machine that you created, and then select **Edit Settings**.
 - b. Under **Hardware**, choose **CD/DVD drive 1**.
 - c. Browse for the location of the `.iso` file that is uploaded in the data store.
 - d. Select **Connect at power on**.
 - e. Click **OK**.
4. Click **Power on the virtual machine**.

What to do next

Proceed with the IBM Security Privileged Identity Manager Virtual Appliance installation.

Installing the IBM Security Privileged Identity Manager Virtual Appliance

You can install IBM Security Privileged Identity Manager Virtual Appliance after you set up the virtual machine.

Procedure

1. When you start the virtual machine for the first time, a list of available languages is displayed. Select the required language and then enter **Yes** to start the installation process.
2. When the installation process completes, press **Enter** to restart the system.

Setting up the initial IBM Security Privileged Identity Manager Virtual Appliance

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

Procedure

1. Provide the following user credentials when the system restarts after the IBM Security Privileged Identity Manager Virtual Appliance installation:
 - **Unconfigured login:** admin
 - **Password:** admin
2. Press 1 to choose the language.
Press 2 to view the IBM terms.
Press 3 to view the non-IBM terms.
Press 4 to accept the license terms.

```
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
```

3. Change the virtual appliance password. After you change the virtual appliance password, continue 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
```

```
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
```

4. Change the host name.

```
Change the Host Name
Enter the new host name: ispmva.us.example.com
```

```
Host Name Configuration
Host name: ispmva.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. In a non-cluster setup, you must use the value that is provided as the server location during AccessAgent configuration on the client system.

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

```

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

Select option: n

```

6. 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

```

7. Configure the time settings for the virtual appliance.

```

Time Configuration
Time configuration changes are applied immediately.
Time: 08:28:58
Date: 09/09/2013
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

```

8. Review the summary of configuration details.

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

9. Press 1 to accept the configuration.

Selecting the virtual appliance configuration mode

In the Mode Selection page, you can set up IBM Security Privileged Identity Manager Virtual Appliance as a stand-alone server or *Primary node*, or a *Member node*. Select an option that is based on your deployment preference.

About this task

IBM Security Privileged Identity Manager Virtual Appliance supports high availability deployment mode. A high availability deployment is a cluster of multiple servers that are active and can process requests. The virtual appliance cluster consists of one primary node, one or more member nodes, and a load balancer as a front end.

Procedure

1. In a web browser, type the host name of the IBM Security Privileged Identity Manager Virtual Appliance in the following format.

`https://host name of the IBM Security Privileged Identity Manager`

For example: `https://pim1.jk.example.com`

2. Log on to the IBM Security Privileged Identity Manager Virtual Appliance with the administrator credentials.
 - **User name:** admin
 - **Password:** admin
3. Select one of the mode options that are based on your requirement and click **Next**.

**Set up a stand-alone node for IBM Security Privileged Identity Manager Virtual Appliance or
Set up a Primary node for the IBM Security Privileged Identity Manager**

Virtual Appliance cluster

Sets up a stand-alone node or a Primary node for the IBM Security Privileged Identity Manager Virtual Appliance cluster.

Set up a Member node for the IBM Security Privileged Identity Manager Virtual Appliance cluster

Sets up a Member node for the IBM Security Privileged Identity Manager Virtual Appliance cluster.

Setting up a stand-alone or primary node for IBM Security Privileged Identity Manager

Log on to the Initial Configuration wizard from the web user interface to complete the virtual appliance setup tasks for stand-alone or primary node for IBM Security Privileged Identity Manager.

Before you begin

- Configure the initial virtual appliance settings.
- Collect the following information:
 - Setup mode selection
Choose from **Guided** or **Advanced** setup mode.
 - Session recording activation code
 - Application identity management activation code
 - Root CA or signer certificate configuration
 - Mail server configuration
 - Database server configuration. For information about database settings, see Table 3 on page 20.
 - Directory server configuration. For information about directory server, see Table 4 on page 22.

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

For example: `https://pimval.jk.example.com`
2. Log on to the IBM Security Privileged Identity Manager Virtual Appliance with the administrator credentials.
 - **Configured login:** admin
 - **Password:** admin
3. Select the **Set up a stand-alone node for IBM Security Privileged Identity Manager OR Set up a Primary node for the IBM Security Privileged Identity Manager cluster** deployment mode option.
4. Choose one of the following configuration modes and click **Next page**.

Option	Actions
Guided Configuration	<ol style="list-style-type: none">1. Follow the steps in the wizard.2. Go to step 5 on page 13.

Option	Actions
Advanced Configuration	<ol style="list-style-type: none"> 1. Use a properties response file that contains the predefined values for the configuration parameters. See Sample virtual appliance configuration response file . 2. Upload the response file to the Mode Selection page. 3. Click Next page. 4. Go to step 10.

5. On the **Session Recording Activation** and **Application Identity Management Activation** pages, take one of the following actions and click **Next page**:

- Enter the activation code.
 - To enable the session recording feature, enter the **Session Recording Activation Code**.
 - To enable the application identity feature, enter the **Application Identity Management Activation Code**

Note: If you do not enter the activation codes at this stage, you can enter the activation codes after you set up the virtual appliance. These features are not enabled until you enter the activation codes.

- If you do not plan to use these features or do not have the activation codes, skip to the next page.

6. Optional: On the **Root CA Configuration** page, take one of the following actions and click **Next page**.

- To use the default SSL certificate, review the default details that are generated by the virtual appliance.
- To define your own signer certificate, click **Update**.

Note: Use this step when you want to accomplish one of the following outcomes:

- If you want to create and use a stand-alone virtual appliance and change the own signer certificate.
- If you plan to set up a cluster of virtual appliances, you can upload the correct Root CA certificate on the Load Balancer.

7. Configure the mail server and click **Next page**.

8. Configure the database settings for the following data stores and click **Next page**.

- Identity
- Single Sign-On
- Session Recording

9. Configure the directory server and click **Next page**.

10. On the **Completion Setup** page, complete the following tasks that depend on the configuration mode you selected.

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

- **Guided Configuration:** Review the instructions and click **Complete Setup** to complete the configuration process.

- **Advanced Configuration:** Review the instructions and click **Start Configuration** to begin the configuration process.

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

11. Click the restart link.

Setting up a virtual appliance cluster

To set up a virtual appliance cluster, you must set up the virtual machine, install the IBM Security Privileged Identity Manager Virtual Appliance firmware, and complete the initial configuration.

Procedure

1. Set up a primary node.
2. Add member nodes to the cluster.

Setting up a member node for the IBM Security Privileged Identity Manager

For high availability deployment mode, you can set up a member node for the IBM Security Privileged Identity Manager cluster by using the Initial Configuration wizard.

Before you begin

Configure the initial virtual appliance settings.

About this task

In a web browser, log on to the Initial Configuration wizard from the web user interface after you complete the virtual appliance logon configuration. Complete the virtual appliance setup tasks from either the command line or the IBM Security Privileged Identity Manager Virtual Appliance management user interface.

Use the **Set up a Member node for the IBM Security Privileged Identity Manager cluster** option to set up a Member node.

Procedure

1. 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, pimval.jk.example.com.

The Primary node host name must be same that was used to create the Primary virtual appliance host name. That is, the value in the **Issued To** field of the Primary node host name must match with the value that you entered in the **Primary node host name** field of the **Connect to Primary** tab.
 - 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 Privileged Identity Manager Virtual Appliance For example, admin.
 - c. Type the password in the **Primary node administrator password** field. For example, admin.

2. Click **Test Connection** to validate the details and to verify this connection of the Member node with the Primary node. The system notifies that the connection to the Primary node was successful.
3. 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.

4. 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.
5. Optional: To review or edit the data in the **Connect to Primary** tab, click **Previous page**.
6. Click **Start Configuration** to start the initial configuration for the IBM Security Privileged Identity Manager 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 to restart the IBM Security Privileged Identity Manager Virtual Appliance. See Restarting or shutting down.
 - If the configuration is not complete or not successful, a message indicates the reason. Do one of the following actions:
 - Click the **Log files** link to open the Log Retrieval and Configuration page and check for any messages and errors in the log files.
 - Click the **Click here** link to restart the configuration process in case of failures.

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 Privileged Identity Manager 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 Privileged Identity Manager 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 2. 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 32.
Not Synchronized	Displays when the Member node is not synchronized with the Primary node.	Synchronize the Member node with the Primary node. See the following procedure.
Synchronized	Displays when the Member node is synchronized with the Primary node.	No action is required.
Synchronizing	Displays when the Member node is synchronizing with the Primary node.	Wait until the synchronization is complete. Click the Refresh icon to get the most recent status.
Not Applicable	Displays if the cluster node is a Primary node because the Primary node does not require any synchronization.	No action is required.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure > Manage Cluster > Cluster Node Configuration**.
2. Do the following actions.
 - From the Member node console, select the current Member node and click **Synchronize** to synchronize it with the Primary node.
A progress bar indicates the synchronization process. It retrieves configuration information from the Primary node for any configuration changes and synchronizes within the same node.

- From the Primary node console, select one or more Member nodes and click **Synchronize**.
A synchronization request is submitted to each of the node that was selected.

Results

The Member node is synchronized with the Primary node.

Setting up a load balancer for a virtual appliance cluster

Deploying a cluster of Privileged Identity Manager virtual appliances with a load balancer provides the required high availability for business continuity.

Before you begin

The load balancer must meet the following requirements:

- Must be a Layer-7 load balancer.
- Valid SSL certificate installed. You can install a certificate that is signed by a commercial Certificate Authority or a self-signed certificate. For a self-signed certificate, the Root CA certificate that is used to sign the load balancer certificate, must be imported into the Windows truststore to work with AccessAgent.
- AccessAgent must be configured to use the load balancer as the IMS Server. The communication between the AccessAgent and the IMS Server is over a separate SSL connection.
- `underscores_in_headers` directive is enabled.
- Session affinity is enabled.


About this task

A load balancer is a hardware or software device capable of spreading user requests between cluster member nodes. To avoid being a single point of failure, keep a backup load balancer that is ready to be swapped in. The backup load balancer is useful when the primary load balancer fails.

Procedure

1. Set up and configure the front-end load balancer. See the configuration requirements “Planning for high availability” on page 23.
2. If necessary, package the load balancer SSL certificate with the AccessAgent installation packages.
3. Configure AccessAgent to use the load balancer as the IMS Server.
4. Configure the load balancer settings on the virtual appliance. See “Configuring the Load Balancer settings” on page 24.

Related information:

 developerWorks: Configuring the appliance with a load balancer
“Planning for high availability” on page 23

IBM Security Privileged Identity Manager Virtual Appliance with a load balanced cluster provides not only the expected high availability but also provides scalability.

AccessAgent installation

Install the AccessAgent client to provide automated shared access credential check-in and check-out for IBM Security Privileged Identity Manager.

To install AccessAgent, see [Installing the AccessAgent](#).

Use the instructions to install:

- AccessAgent, Version 8.2.1 with 8.2.1-ISS-SAMESSO-AA-FP0006 or later.

Note:

- This AccessAgent version is required for text-based session recording.
- To verify the installation, configure AccessAgent to communicate with the IMS Server. To set up the IMS Server location, see [Ways of setting the IMS Server location](#).
- To enable or disable the Credential Provider, see [Response file parameters \(SetupHlp.ini\)](#) and search for the **EncentuateCredentialProviderEnabled** parameter.
- Optional: AccessStudio, Version 8.2.1 with the latest fix pack
To modify the bundled AccessProfiles, install AccessStudio on an administrative computer to develop custom AccessProfiles.

Chapter 3. Configuration

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

To manage the configured virtual appliance, log on to the **Appliance Dashboard** at `https://pimva_hostname`. For example: `https://pimval.jk.example.com`.

Enabling the session recording feature in the virtual appliance

You can enable the session recording feature in the IBM Security Privileged Identity Manager Virtual Appliance to record privileged identity sessions for auditing, security forensics, and compliance.

Before you begin

By default, session recording is not activated in the IBM Security Privileged Identity Manager Virtual Appliance. If you purchased the IBM Privileged Session Recorder feature and want to enable it, you must have the activation code to complete this task.

About this task

This task covers only how to enable the feature in the virtual appliance.

To enable the session recording for AccessAgent, modify the `pid_recorder_enabled` policy in AccessAdmin.

Procedure

1. From the top menu, click **Manage > Session Recording Activation**.
2. Enter your activation code.
3. Click **Activate** to enable session recording.

Enabling the application identity management feature in the virtual appliance

You can enable the application identity feature in the IBM Security Privileged Identity Manager Virtual Appliance to manage, automate, and track the application credentials.

Before you begin

By default, application identity is not activated in the IBM Security Privileged Identity Manager Virtual Appliance. If you purchased the IBM Security Privileged Identity Manager for Applications feature and want to enable it, you must have the activation code to complete this task.

About this task

This task covers only how to enable the feature in the virtual appliance.

Procedure

1. From the top menu, click **Manage > Application Identity Management Activation**.
2. Enter your activation code.
3. Click **Activate**.

Managing the Database Server configuration

Use the Database Server Configuration page to configure the database server for the IBM Security Privileged Identity Manager Virtual Appliance.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure > Manage External Entities > Database Server Configuration**.
2. Click the **Configure** menu to configure the Identity data store, Single Sign-On data store, or the Session Recording data store according to the order by which they are displayed.

Note: The next data store in the **Configure** menu, Single Sign-On data store, is only activated after you configure the Identity data store. Likewise, the Session Recording data store is activated in the **Configure** menu after you configure the Single Sign-On data store.

3. Specify the data store configuration details.

Table 3. Data stores configuration options

If you choose to configure the following data store:	Description
Identity data store	<p>Host name The name of the computer that hosts the data store. Example: pimidstore.example.com.</p> <p>Port The data store service port. Example: 50000.</p> <p>Database Name The name of the IBM Security Privileged Identity Manager database. Example: isimdb.</p> <p>Database Administrator ID The user with database administrator privileges. Example: piminist. Note: During the database configuration for a virtual appliance, the user must be the database owner. For example, piminist. This database owner must be the same user who created the database.</p> <p>Database Administrator Password The password for the user with database administrator privileges.</p>

Table 3. Data stores configuration options (continued)

If you choose to configure the following data store:	Description
Single Sign-On data store	<p>Host name The name of the computer that hosts the data store. Example: pimidstore.example.com.</p> <p>Port The data store service port. Example: 50000.</p> <p>Database Name The name of the IBM Security Access Manager for Enterprise Single Sign-On database. Example: essodb</p> <p>Database Administrator ID The user with database administrator privileges. Example: piminst. Note: During the database configuration for a virtual appliance, the user must be the database owner. For example, piminst. This database owner must be the same user who created the database.</p> <p>Database Administrator Password The password for the user with database administrator privileges.</p>
Session Recording data store	<p>Host name The name of the computer that hosts the data store. Example: pimidstore.example.com.</p> <p>Port The data store service port. Example: 50000.</p> <p>Database Name The name of the IBM Security Privileged Identity Manager database. Example: pimrecdb.</p> <p>Database Administrator ID The user with database administrator privileges. Example: piminst. Note: During the database configuration for a virtual appliance, the user must be the database owner. For example, piminst. This database owner must be the same user who created the database.</p> <p>Database Administrator Password The password for the user with database administrator privileges.</p>

4. Click **Save Configuration** to complete this task.

Managing the Directory Server configuration

Use the Directory Server Configuration page to configure the directory server in the IBM Security Privileged Identity Manager Virtual Appliance.

Before you begin

Complete the following tasks:

- “Installing and configuring the directory server” on page 3.
- Create the directory server DN location.

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 pane, specify the expected variables.

Table 4. Directory or LDAP server configuration details

Field name	Description and examples
Host name	The name of the computer that hosts the directory server. The acceptable formats for the host name are IPv4, FQDN, and IPv6 Example: pimldap.example.com
Port	The directory service port. Example: 389 If you opted for secure communication, use 636.
Principal DN	The principal distinguished name. Example: cn=root
Password	The password for the directory server.
Organization name	The name of the enterprise or the organization. Example: JK Enterprises
Default organization short name	The abbreviation or short form of the organization name. Example: jke
IBM Security Privileged Identity Manager DN Location	The directory server DN location. Example: dc=com

4. Click **Save Configuration** to complete this task.

Note: The Directory Server configuration takes some time. Do not refresh or close the page. Wait for the configuration process to complete.

Planning for high availability

IBM Security Privileged Identity Manager Virtual Appliance with a load balanced cluster provides not only the expected high availability but also provides scalability.

Load Balancer settings and requirements

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

Load Balancer requirements

The most common mechanism to make a highly available deployment is to add a Load Balancer that distributes user requests to underlying servers. This deployment locks down any direct access to individual servers. In addition to making a highly available deployment of the IBM Security Privileged Identity Manager Virtual Appliance, it also provides horizontal scalability. See Figure 1.

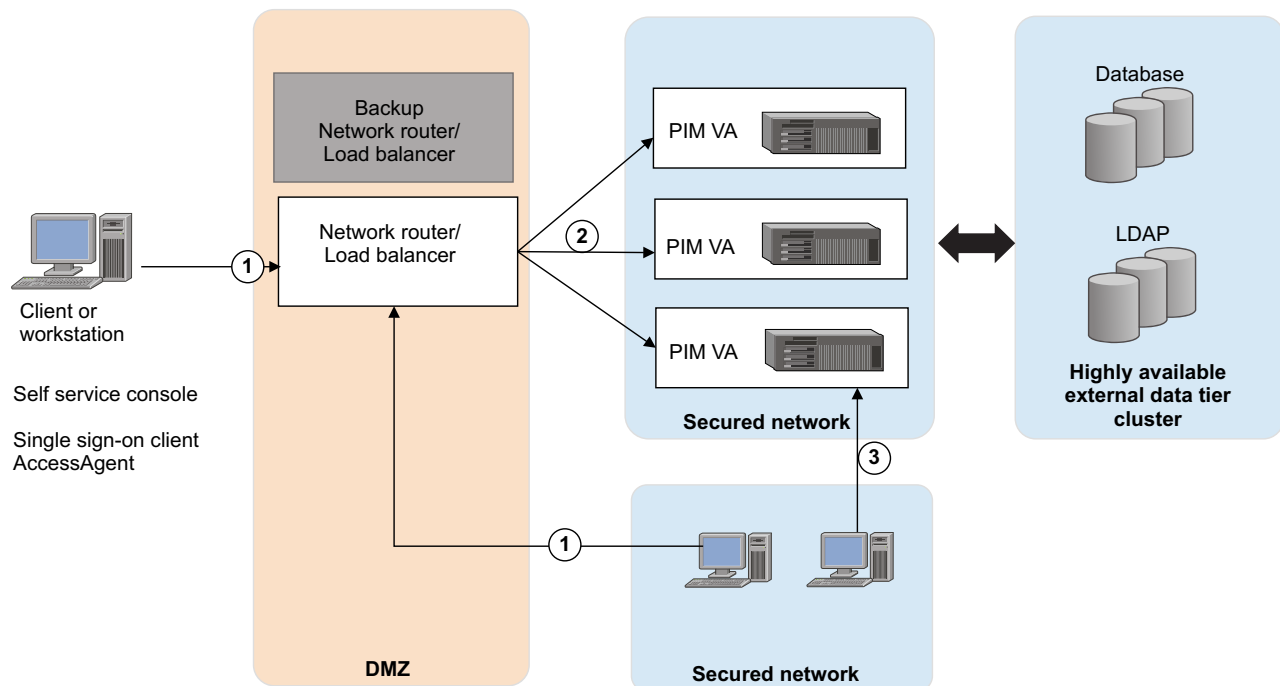


Figure 1. Deployment diagram of a typical Load Balancer in a customer environment

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 Privileged Identity Manager 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 Load Balancer for this installation. Layer-4 Load Balancers do not provide the required function and must not be used for this architecture.
- The Load Balancer must contain a valid SSL certificate for the IBM Security Access Manager for Enterprise Single Sign-On AccessAgent to connect. For a self-signed certificate, the Root CA certificate with which the Load Balancer certificate is signed must be imported in the client truststore.
- The AccessAgent must point to the Load Balancer as the IMS Server. The communication between the AccessAgent and the IMS Server is over SSL.
- 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.
- Set the client host IP into the X-Forward-For HTTP header. The IMS Server must know the client IP for its audit logs.
- The Load Balancer must detect unresponsive virtual appliances and stop directing any traffic to them.
- As shown in Figure 1 on page 23, keep one or more of the Load Balancer backups ready to avoid the Load Balancer being a single point of failure.
- Set the value of the underscores_in_headers custom header directive to on.

Related tasks:

“Configuring the Load Balancer settings”

Use the Load Balancer Configuration page to configure the Load Balancer with the IBM Security Privileged Identity Manager Virtual Appliance.

“Setting up a load balancer for a virtual appliance cluster” on page 17

Deploying a cluster of Privileged Identity Manager virtual appliances with a load balancer provides the required high availability for business continuity.

Configuring the Load Balancer settings

Use the Load Balancer Configuration page to configure the Load Balancer with the IBM Security Privileged Identity Manager Virtual Appliance.

Before you begin

You must work from the Primary node to configure or reconfigure the Load Balancer.

About this task

Configure the Load Balancer to support the working of your cluster or to distribute the workload across a cluster.

The Load Balancer Configuration page contains these columns:

Load Balancer DNS

Displays the DNS of the Load Balancer.

Last modified on

Displays the date and time when the current Load Balancer DNS was last modified.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, click **Configure > Manage External Entities > Load Balancer Configuration** to open the Load Balancer Configuration page.
2. Click **Configure** to open the Load Balancer details pane.
3. Provide the value in the **Load Balancer DNS** field. For example, enter the value as `pimval.jk.example.com`.

Note: The DNS must be a valid and a fully qualified domain name.

4. Click **Save Configuration** to complete the configuration.
5. Optional: To reconfigure the Load Balancer, do the following steps.
 - a. Select the **Load Balancer DNS** record from the Load Balancer Configuration page.
 - b. Click **Reconfigure**.
 - c. Follow steps 3 and 4.

The Load Balancer is reconfigured with the IBM Security Privileged Identity Manager Virtual Appliance.

Related information:

“Planning for high availability” on page 23

IBM Security Privileged Identity Manager Virtual Appliance with a load balanced cluster provides not only the expected high availability but also provides scalability.

Managing mail configuration

Use the Mail Server Configuration page to configure the email notifications for the IBM Security Privileged Identity Manager Virtual Appliance.

Procedure

1. From the top menu, select **Configure > E-mail Server Configuration** to configure the Mail Server.
2. Follow the instructions on the page to complete the process.

Managing the server properties

You can update the property values in the IBM Security Privileged Identity Manager Virtual Appliance to customize the IBM Security Privileged Identity Manager Server.

Before you begin

You must be familiar with the property keys and values of the IBM Security Privileged Identity Manager supplemental property files before you do this task. See the *Supplemental property files* section of the IBM Security Privileged Identity Manager documentation for details: <http://www.ibm.com/support/>

knowledgecenter/SSRMWJ_6.0.0.2/com.ibm.isim.doc_6.0.0.2/reference/ref/ref_ic_props_supp.htm.

Procedure

1. From the menu, select **Configure > Update Property**.
2. Select the property to update from the list, and click **Edit**.
3. Edit its property value and click **Save Configuration**.

You can customize following IBM Security Privileged Identity Manager properties:

Table 5. Available IBM Security Privileged Identity Manager properties in the IBM Security Privileged Identity Manager Virtual Appliance

Supplemental property files	Properties and values
adhocreporting.properties	<p>applyACIAtRuntime = false</p> <p>availableForNonAdministrators = true</p>
ReportDataSynchronization.properties	<p>accountSynchronizationStrategy = old</p> <p>accountSynchronizationStrategy = old</p> <p>authorizationOwnerSynchronizationStrategy = old</p> <p>groupSynchronizationStrategy = old</p> <p>organizationalContainerSynchronizationStrategy = old</p> <p>personSynchronizationStrategy = old</p> <p>roleSynchronizationStrategy = old</p> <p>serviceSynchronizationStrategy = old</p>
SelfServiceUI.properties	<p>enrole.ui.pageSize = 10</p> <p>enrole.ui.pageLinkMax = 100</p> <p>enrole.ui.maxSearchResults = 1000</p> <p>enrole.ui.maxSearchResults.users = 100</p>

Table 5. Available IBM Security Privileged Identity Manager properties in the IBM Security Privileged Identity Manager Virtual Appliance (continued)

Supplemental property files	Properties and values
enRole.properties	<p>enrole.connectionpool.incrementcount = 3</p> <p>enrole.connectionpool.initialpoolsize = 50</p> <p>enrole.connectionpool.maxpoolsize = 100</p> <p>enrole.connectionpool.protocol = plain ssl</p> <p>enrole.workflow.notifyoption = 1</p> <p>enrole.workflow.notifypassword = true</p> <p>enrole.workflow.notifyaccountsonwarning = false</p> <p>enrole.workflow.maxretry = 2</p> <p>enrole.workflow.retrydelay = 60000</p> <p>enrole.workflow.skipapprovalforrequester = false</p> <p>enrole.workflow.disablerequesteeapproval = false</p> <p>enrole.workflow.disablerequesterapproval = false</p> <p>enrole.workflow.skipfornoncompliantaccount = true</p> <p>enrole.reconciliation.accountcachesize = 2000</p> <p>enrole.reconciliation.threadcount = 8</p> <p>remoteservices.remotepending.restart.retry = 1440</p> <p>remoteservices.remote.pending.testing.max.duration = 1200</p> <p>enrole.CreatePassword = true</p> <p>enrole.accesscontrollist.refreshInterval = 10</p> <p>enrole.recyclebin.enable = false</p> <p>enrole.lifecyclerule.partition.size = 100</p>
ui.properties	<p>enrole.ui.customerLogo.image = ibm_banner.gif</p> <p>enrole.ui.customerLogo.url = www.ibm.com</p> <p>enrole.ui.pageSize = 50</p> <p>enrole.ui.pageLinkMax = 10</p> <p>enrole.ui.maxSearchResults = 1000</p> <p>enrole.ui.report.maxRecordsInReport = 5000</p> <p>ui.challengeResponse.showAnswers = true</p> <p>ui.userManagement.includeAccounts = true</p> <p>ui.challengeResponse.bypassChallengeResponse = true</p> <p>ui.passwordManagement.generatePassword = true</p>

Managing feed files

You can upload feed files and use them in the IBM Security Privileged Identity Manager Virtual Appliance as long as you put them in the prescribed location.

Procedure

1. From the menu, select **Configure > Upload Feed File**.
2. Click **New**.
3. Click **Browse** to search for the feed file to upload. The feed files are in /userdata/identity/feeds.
The /userdata/identity/feeds location is required while creating feed in Administrative console.

Managing log configuration

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

Procedure

1. From the menu, select **Manage > Log Retrieval and Configuration**.
2. Select the product from the tabs to view the available logs.
3. Select **Configure** to set the file size and roll over settings for the selected log file.

Retrieving logs

Use the Log Retrieval and Configuration page to view the log files. You can also use the page to configure the server log settings for the IBM Security Privileged Identity Manager Virtual Appliance.

Procedure

1. From the top menu, select **Manage > Log Retrieval and Configuration**.
2. Take any of the following actions:
 - To display a log file, click **View**.
 - To save a log file, click **Download**.
 - To remove a log file, click **Clear**.
 - To display all the log files again, click **Refresh**.

Table 6. Available logs to help you diagnose or troubleshoot

Tab	Log Files	File Name
Appliance These files help you to debug any configuration failures that occur in the virtual appliance.	Identity data store configuration log	dbConfig.stdout
	ESSO datastore configuration log	essoDbConfig.log
	Session Recording data store configuration log	sessrecConfig.log
	Directory server configuration log	ldapConfig.stdout
	Appliance system log	ispim_appliance_system.log
	Appliance Web Management Console log	messages.log

Table 6. Available logs to help you diagnose or troubleshoot (continued)

Tab	Log Files	File Name
Identity Helps you identify issues in the identity applications.	Identity Server System Out	SystemOut.log
	Identity Server System Error	SystemErr.log
	Identity Server Trace	
	Identity Application Message	msg.log
	Identity Application Trace	trace.log
	Identity Access Log	access.log
Single Sign-On Helps you identify issues in the single sign-on application.	Single Sign On Server System Out	SystemOut.log
	Single Sign On Server System Error	SystemErr.log
	Single Sign On Server Trace	
Session Recording Helps you identify issues in the session recording application.	Session Recording Server System Out	SystemOut.log
	Session Recording Server System Error	SystemErr.log
	Session Recording Server Trace	

Configuring logs

You can configure different options to manage the quantity and size of the log files.

Procedure

1. From the top menu, select **Manage > Log Retrieval and Configuration**.
2. To set the log settings, click **Configure**.
3. Provide the following details:

Maximum size for log file rotation

The size of the log file that you want to keep.

Maximum number of historical log files

The maximum number of historical log files that you want to keep.

4. Click **Save Configuration**.

Chapter 4. Maintenance

See this section for information about the IBM Security Privileged Identity Manager maintenance.

Changing a Member node to a Primary node

Use the Cluster Node Configuration page to change a Member node to Primary node in the IBM Security Privileged Identity Manager Virtual Appliance.

Before you begin

No active Primary node must exist in this cluster.

About this task

You might want to change a Member node to a Primary node in the cluster for maintenance and other tasks.

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

Procedure

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

Changing a Primary node to a Member node

Use the Cluster Node Configuration page to change a Primary node to Member node in the IBM Security Privileged Identity Manager Virtual Appliance.

Before you begin

You must work from a Primary node to change it to a Member node.

About this task

You might want to change a Primary node to a Member node due to the following reasons:

- Change the node in the cluster for maintenance and other tasks. To promote some other Member node to Primary node, you must first change the current Primary node to Member node.
- Remove a damaged or affected Primary node from the cluster configuration. You must first remove such affected node from the Load Balancer configuration.

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

Procedure

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

Before you begin

Remove the node from the Load Balancer configuration so that no user requests are routed to this node.

About this task

You can remove a Member node only from a Primary node, but you cannot remove the Primary node itself.

You might want to remove a damaged or affected Primary node from the cluster configuration. You must first remove such affected node from the Load Balancer configuration. After the node is removed, it no longer functions as part of the cluster unless you 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 Node**.
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 Privileged Identity Manager 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 Node**. The Reconnect Node pane is displayed.
4. In the Reconnect Node 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, pimval.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.

Reconfiguring the data store connection

You can reconfigure the data store if the data store configuration changes. For example, if the data store is moved to a different server host.

Procedure

1. Make a backup of the database. On the database server that runs for DB2, complete the following steps:
 - a. Log on as the instance owner. For example: db2admin.
 - b. Close all connections to the IBM Security Privileged Identity Manager database. If necessary, run the following command to force all connections to close:


```
db2 force application all
```
 - c. Back up the data store database:


```
db2 backup database IDM_DB to OLD_DB2_BACKUP_DIR
```

 where
 - IDM_DB is the name of the IBM Security Privileged Identity Manager data store database. For example: idmdb
 - OLD_DB2_BACKUP_DIR is a directory path to store the backup. For example:

Linux or UNIX systems

/tmp/db2

Windows systems

c:\temp\db2

2. Restore the backup of the database.

Install the new version of DB2. For this reconfiguration, ensure that you create the database instance and database with the same name. Users must have the same rights and privileges as those setup on the previous system.

- To create a new database instance and a database, see “Installing and configuring the database server” on page 1.
- Copy the contents of the IBM Security Privileged Identity Manager data store backup directory to the target server. For example: tmp/db2.
- Ensure that the database instance owner you create has permission to read the target directory and files within.

To restore the DB2 data on the target database server, complete the following steps:

- a. Launch DB2 command line.

Windows

- 1) Launch the Windows command line.
- 2) Run the following command:

```
set DB2INSTANCE=piminst
```

where `piminst` is the database instance.
- 3) Run **db2cmd** to launch the DB2 command line.

Linux

Run the following command:

```
su - piminst
```

where `piminst` is the database instance.

- b. In the DB2 command line, enter the following commands to restore the database by using the migrated DB2 data:

```
restore db idmdb from OLD_DB2_TEMP_DATA
```

where

- `idmdb` is the IBM Security Privileged Identity Manager data store database name.
- `OLD_DB2_TEMP_DATA` is the location of the migrated DB2 data that you copied over from the previous version. For example: `c:\temp\db2`

- c. Stop and start the DB2 server to reset the configuration.

After you create the IBM Security Privileged Identity Manager data store database, stop, and start the DB2 server to allow the changes to take effect.

Enter the following commands:

```
db2stop  
db2start
```

Note: If the `db2stop` fails and the database remains active, enter the following commands to deactivate the database:

```
db2 force application all  
db2stop
```

3. For the Identity data store, clear the **Service Integration Bus**.

For reconfiguration of the Identity data store, you must clear out the Service Integration Bus (SIB) from the restored database.

To clear out the **Service Integration Bus** on the target DB2 server, complete the following steps:

- a. Ensure that the IBM Security Privileged Identity Manager database is running (IDMDB).
- b. Launch the DB2 command line:

Windows

- 1) Launch the Windows command line.
- 2) Run the following command:
`set DB2INSTANCE=piminst`
where `piminst` is the database instance.
- 3) Run **db2cmd** to launch the DB2 command line.

Linux

Run the following command:

```
su - piminst
```

where `piminst` is the database instance.

- c. Run the following command to connect to the data store:

```
db2 connect to idmdb
```

where `idmdb` is the Identity data store.

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

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

```
db2 delete from schema_name.SIB000
db2 delete from schema_name.SIB001
db2 delete from schema_name.SIB002
db2 delete from schema_name.SIBCLASSMAP
db2 delete from schema_name.SIBKEYS
db2 delete from schema_name.SIBLISTING
db2 delete from schema_name.SIBXACTS
db2 delete from schema_name.SIBOWNER
db2 delete from schema_name.SIBOWNER0
```

where the Service Integration Bus schema, `schema_name` is `ITIML000`.

Note: The `SIMOWNER0` might not exist in all Identity data store environments. If it does not exist and the delete statement fails, you can ignore the failure.

4. Reconfigure the data store.
 - a. From the IBM Security Privileged Identity Manager administrative console, click **Menu > Database Configuration**.
 - b. Select the existing data store that you want to set up and click **Reconfigure**. Provide the details and click **Save Configuration**.
 - c. Restart the server for the corresponding data store to complete the process.

Reconfiguring the directory server connection

You can reconfigure the directory server if the directory server configuration changes.

Procedure

1. Make a backup of the directory server.

On the server running IBM Security Directory Server for IBM Security Privileged Identity Manager, complete the following steps:

- a. Log on as an Administrator with root privileges.
- b. Open a command window.

- c. Go to the `TDS_HOME/sbin` directory and type the following command:
`db2ldif -s ldap_suffix -o ldap_output_file -I ldap_instance_name`
 where:
`ldap_suffix` is the name of the suffix. For example: `dc=com`.
`ldap_output_file` is the name of the ldif output file. For example:
`old_ldif_data.ldif`.
`ldap_instance_name` is the name of the LDAP server instance, which can be obtained through the IBM Security Directory Server Instance Administration tool.
- d. Use the backup of the schema file `V3.modifiedschema` from the `OLD_ITDS_INSTANCE_HOME/etc` directory of the IBM Security Directory Server instance home directory.

2. Restore the backup of the database.

Install a version of IBM Security Directory Server that IBM Security Privileged Identity Manager supports. For this reconfiguration, ensure that you take the following actions:

- Create and use the same root suffix.
- Use the same encryption seed value as the old Directory Server instance. If not, you must export the data from the old Directory Server instance to use the seed and salt keys from the new instance.

Copy the contents of the IBM Security Privileged Identity Manager directory server backup ldif file and schema file to the target server.

To restore the directory server data on the target directory server, complete the following steps:

- a. Log on as an Administrator with root privileges.
- b. Stop the LDAP server.
- c. Copy the schema file `V3.modifiedschema` that you copied over from the previous server to the `NEW_ITDS_INSTANCE_HOME/etc` directory of the IBM Security Directory Server instance.

Note: If you customized or modified the schema files, manually merge the changes into the new schema files.

- d. From `TDS_HOME/sbin`, run the command:
`bulkload -i OLD_ITDS_TEMP_DATA\ldif_output_file -I ldap_instance_name`
 where:

`OLD_ITDS_TEMP_DATA` is the temporary directory location of the IBM Security Directory Server data you copied over from the previous server. For example, `C:\temp\51data\ids\`.

`ldif_output_file` is the name of the file that you exported in a previous task. For example, `old_ldif_data.ldif`

`ldap_instance_name` is the name of the LDAP server instance. For example, `itimldap`. You can obtain use the IBM Security Directory Server Instance Administration tool to obtain the instance name.

For more information, see Bulkload command errors.

- e. Stop and start the IBM Security Directory Server to activate the changes.

3. Reconfigure the IBM Security Directory Server.

- a. From the IBM Security Privileged Identity Manager administrative console, go to **Menu > Directory Server Configuration**.

- b. Select the directory server and click **Reconfigure**. Provide the details and click **Save Configuration**.
- c. Restart the Identity server to complete the process.

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 Privileged Identity Manager Virtual Appliance into two virtual appliances with active-passive configuration.

Complete the following tasks to deploy an active-passive configuration for the virtual appliances:

1. "Setting up a primary virtual appliance."
2. Optional: "Backing up the primary virtual appliance."
3. "Creating a snapshot of the primary virtual appliance" on page 38.
4. "Setting up a secondary virtual appliance" on page 39.

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 Privileged Identity Manager Virtual Appliance ISO.
2. Complete the first steps configuration. For example, configure the host name and IP address.
3. Complete the virtual appliance configuration.
4. Log on to the applications by using the **Appliance Dashboard** console.
5. Verify that the applications are started.
6. Verify that the user can log on to IBM Security Privileged Identity Manager, IBM Security Access Manager for Enterprise Single Sign-On and the Privileged Session Recorder console to complete operations.

Backing up the primary virtual appliance

As an optional task, you can choose to back up the primary 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 primary 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 servers from the **Appliance Dashboard**. To stop the servers, click **Stop** from the **Server Status** pane.
2. Stop the directory server instance and database instance on the external data tier.
3. From the **Appliance Dashboard**, verify that the **Middleware and Server Monitor** widget indicates that all middleware and applications are stopped.

4. Create a backup of the active partition on the secondary partition.
 - a. From the virtual appliance user interface, select **Firmware Settings**.
 - b. 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; 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; the partition from where the backup was taken.

Procedure

1. On the virtual appliance user interface, select **Firmware Settings**.
2. Select the inactive partition and click **Set Active**.

Creating a snapshot of the primary virtual appliance

Use the **Appliance Dashboard** to create a snapshot of the primary 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 the primary virtual appliance and a secondary virtual appliance.

Procedure

1. From the **Appliance Dashboard**, stop the servers.
2. On the external data tier, stop the following instances.
 - Directory server
 - Database
3. From the **Appliance Dashboard**, verify that the **Middleware and Server Monitor** widget indicates that all the middleware and applications are stopped.
4. Under **Manage System Settings**, click **Snapshots**.
5. Click **New** to create a snapshot.
6. Under the **Comments**, specify helpful comments so that the snapshot is easy to identify from a primary virtual appliance that is synchronized with the external data tier.
7. Download and save the snapshot on the network file system.
8. 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 by using the command-line interface command: `shutdown`.

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.

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 Privileged Identity Manager Virtual Appliance ISO.
2. Complete the IBM Security Privileged Identity Manager Virtual Appliance set up.
3. Select the virtual appliance configuration mode.
4. Click the **Manage Snapshots** link in the Setup Progress pane in the lower-left corner of the page.
5. Upload the snapshots that are taken from the primary appliance. Wait until the **Comment** field is updated on the snapshot upload screen.
6. When the snapshot is uploaded, the screen is refreshed and it lists the snapshots.
7. Select the snapshot, which was captured from the primary virtual appliance that is based on the comments and time stamps from the list and click **Apply**.
8. After the snapshot is applied, log on to the command-line interface and shut down the secondary virtual appliance by using the **shutdown** command.
9. Start the directory server and database instance on the external data tier.
10. Start the secondary virtual appliance from the VMware Server.
11. When the secondary virtual appliance starts, you can log on to the virtual appliance user interface.
12. Go to the **Appliance Dashboard**.
13. From the **Appliance Dashboard**, verify that the **Middleware and Server Monitor** widget indicates that all middleware and applications are started.

What to do next

Only one instance of the virtual appliance must be running at any time. As such, the secondary virtual appliance must be started only when the primary virtual appliance is down.

Verify that the applications are started and that the user can log on to IBM Security Privileged Identity Manager, IBM Security Access Manager for Enterprise Single Sign-On, and the Privileged Session Recorder console.

Installing a fix pack

Install a fix pack on the IBM Security Privileged Identity Manager 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 Privileged Identity Manager 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 > Updates and Licensing > Fix Packs**. The Fix Packs page is displayed.
2. On the Fix Packs page, click **New**.
3. In the Add Fix Pack window, click **Browse for fix pack** to locate the fix pack file.
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.

Upgrading the IBM Security Privileged Identity Manager Virtual Appliance

Install the firmware update to upgrade the IBM Security Privileged Identity Manager Virtual Appliance.

Before you begin

Before you apply the firmware update to upgrade the IBM Security Privileged Identity Manager Virtual Appliance, back up your data tier, which is all the databases and the directory server.

Important:

- When you upgrade the virtual appliance, all existing snapshots are deleted.
- The upgraded virtual appliance cannot use snapshots that are created for older versions of the virtual appliance.

About this task

The IBM Security Privileged Identity Manager 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 of the partition can be active on the IBM Security Privileged Identity Manager Virtual Appliance.

In the factory-installed state, Partition 1 is active and contains the firmware version of the current 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 Privileged Identity Manager Virtual Appliance restarts the system by using Partition 2, which is now the active partition.

The IBM Security Privileged Identity Manager Virtual Appliance version upgrade can be installed only by using the command-line interface (CLI).

Procedure

1. Download the `ispim_*.pkg` build.
2. Access the command-line interface (CLI) of the virtual appliance by using either an `ssh` session or the console.
3. Copy the `ispim_*.pkg` to a USB device.
4. Attach the USB device to your virtual system.
5. In the virtual appliance CLI, run the `ispim` command to display the `ispim` prompt.
6. At the `ispim` prompt, run the `firmware_update` command.
 - a. Run the `list_firmware` command to list the firmware updates from a USB device.
 - b. Run the `transfer_firmware` command to transfer the firmware updates from a USB device to the virtual system.

Note: To install a firmware upgrade, you must first transfer it to the virtual system.

- c. Run the `install_firmware` command.
- d. Select the index of the firmware update that you want to install to the virtual system and press **Enter**.

The results are as follows:

- 1) The upgrade process formats Partition 2 and installs the new firmware update on it.
 - 2) When you apply the firmware update, your policies and settings are copied from Partition 1 to Partition 2.
 - 3) On completion, the process indicates you to restart the virtual system.
- e. Type the `reboot` command and press **Enter** to restart the virtual system by using Partition 2. Partition 2 is now the active partition.

The results are as follows:

- 1) After the virtual appliance restarts from the Partition 2, all the configuration that were part of Partition 1, is applied to the Partition 2.
 - 2) After the configuration is applied to the virtual appliance, the process indicates you to restart the virtual appliance.
- f. Restart the virtual appliance to complete the upgrade process.
 - g. 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:

- 1) Check and fix any errors if the upgrade process failed.
- 2) Use Partition 1 to set it as the active partition and restart it.
Partition 1 now becomes the active partition.

Enhance availability by using monitoring URLs

Monitoring URLs is a facility for the customer to write scripts to monitor the uptime and the responsiveness of the IBM Security Privileged Identity Manager Virtual Appliance. It is used to monitor the health of the IBM Security Privileged Identity Manager server functions.

You do not have to authenticate to access Monitoring URI. These URIs can be used by any third-party tool to obtain data about responsiveness.

Response format

Service name: response code, Time taken in milliseconds:ms (Response code is 0 if services are down and 200 if running.)

Example: "Identity":"0", "Time taken in milliseconds":401

For Identity service -

URI: `https://appliance_hostname/monitor/response?Service=Identity`

Response: {"Identity":"0", "Time taken in milliseconds":401}

For SingleSignOn service -

URI: `https://appliance_hostname/monitor/response?Service=SingleSignOn`

Response: {"SingleSignOn":"0","Time taken in milliseconds":8}

For SessionRecorder service -

URI: `https://appliance_hostname/monitor/response?Service=SessionRecorder`

Response: {"SessionRecorder":"0","Time taken in milliseconds":2}

For All in a single request -

URI: `https://appliance_hostname/monitor/response`

Response:

{"Identity":"200","SessionRecorder":"200","SingleSignOn":"200",
"Identity Time taken in milliseconds":529,"SessionRecorder Time
taken in milliseconds":400,"SingleSignOn Time taken in
milliseconds":361}

Chapter 5. Reports

The IBM Security Privileged Identity Manager solution supports the IBM Cognos® reporting framework for report generation.

IBM Cognos reporting framework

Use the IBM Cognos reporting framework to create and analyze Privileged Identity Manager reports. With this framework, you can modify the schema and generate reports in different formats.

Note: IBM Cognos reporting does not support Microsoft SQL Server database as content store. Use DB2 database or Oracle database instead.

The IBM Cognos reporting framework includes the following items:

Reporting model

Represents the business view of the IBM Security Privileged Identity Manager and IBM Security Access Manager for Enterprise Single Sign-On data. You can use the models to customize and generate different types of Privileged Identity Manager reports that suit your requirements.

Static reports

Ready-to-use reports that are bundled with the IBM Security Privileged Identity Manager reporting package.

IBM Cognos Business Intelligence reporting components

This topic describes the IBM Cognos reporting components that you might use while you work with the Privileged Identity Manager Cognos-based report models.

Query Studio

Query Studio is the reporting tool for creating simple queries and reports in IBM Cognos Business Intelligence. To use Query Studio effectively, you must be familiar with your organization's business and its data. You might also want to be familiar with other components of IBM Cognos Business Intelligence.

Report Studio

Report Studio is a Web-based report authoring tool that professional report authors and developers use to build sophisticated, multiple-page, multiple-query reports against multiple databases. With Report Studio, you can create any reports that your organization requires, such as invoices, statements, and weekly sales and inventory reports.

Your reports can contain any number of report objects, such as charts, crosstabs, lists, and also non-BI components such as images, logos, and live embedded applications that you can link to other information.

IBM Cognos Business Intelligence Connection

IBM Cognos Business Intelligence Connection is the portal to IBM Cognos Business Intelligence software. IBM Cognos Business Intelligence Connection provides a single access point to all corporate data available in IBM Cognos Business Intelligence software.

You can use IBM Cognos Business Intelligence Connection to create and run reports and cubes and distribute reports. You can also use it to create and run agents and schedule entries.

Framework Manager

Framework Manager is a metadata modeling tool that drives query generation for IBM Cognos Business Intelligence software. A model is a collection of metadata that includes physical information and business information for one or more data sources.

IBM Cognos Business Intelligence software enables Performance Management on normalized and denormalized relational data sources and various OLAP data sources. When you add security and multilingual capabilities, one model can serve the reporting, ad hoc querying, and analysis needs of many groups of users around the globe.

Before you do anything in IBM Cognos Business Intelligence Framework Manager, you must thoroughly understand the reporting problem that you want to solve.

Prerequisites for IBM Cognos report server

To work with the Privileged Identity Manager Cognos-based reports, set up the IBM Cognos report server.

You must install the software in the following table.

Table 7. Software requirements for IBM Cognos report server

Software	For more information, see
IBM Cognos Business Intelligence Server, version 10.2.1 Fix Pack 1	<ol style="list-style-type: none"> 1. Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp. 2. Search for Business Intelligence Installation and Configuration Guide 10.2.1.1. 3. Search for the installation information and follow the procedure.
Web server	<ol style="list-style-type: none"> 1. Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp. 2. In the right pane of the home page, under Supported hardware and software section, click IBM Cognos 10.2.1 Business Intelligence software environments. 3. Click 10.2.1 tab. 4. Click Software in the Requirements by type column under the section IBM Cognos Business Intelligence 10.2.1. 5. Search for Web Servers section.

Table 7. Software requirements for IBM Cognos report server (continued)

Software	For more information, see
Data sources	<ol style="list-style-type: none"> 1. Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp. 2. In the right pane of the home page, under Supported hardware and software section, click IBM Cognos 10.2.1 Business Intelligence software environments. 3. Click 10.2.1 tab. 4. Click Software in the Requirements by type column under the section IBM Cognos Business Intelligence 10.2.1. 5. Search for Data Sources section.

Note: Optionally, you can install IBM Framework Manager, version 10.2.1 Fix Pack 1 if you want to customize the reports or models.

Installation of IBM Cognos reporting components

Installation of IBM Cognos reporting components is optional. You need these components only if you use the Privileged Identity Manager Cognos-based reports.

You must complete the installation and data synchronization process before you can access and work with Privileged Identity Manager Cognos-based reports.

Note: IBM Cognos reporting does not support Microsoft SQL Server database as content store. Use DB2 database or Oracle database instead.

The following table describes the installation and synchronization process.

Table 8. Installation and data synchronization process

Task	For more information
Install Cognos Business Intelligence 10.2.1 Fix Pack 1.	<ol style="list-style-type: none"> 1. Access http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp. 2. Search for Install Cognos BI on one computer.
Install Framework Manager 10.2.1 Fix Pack 1. Note: This task is optional. Install this component only if you want to customize the reports or models.	<ol style="list-style-type: none"> 1. Access http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp. 2. Search for Installing Framework Manager.
Complete the data synchronization.	<ol style="list-style-type: none"> 1. Access the IBM Security Privileged Identity Manager product documentation. 2. Search for Data Synchronization. <p>Note: Run the data synchronization before you generate the reports to obtain the latest report data.</p>

Cognos reporting

The Privileged Identity Manager Cognos-based reports are available at IBM Passport Advantage®:

- ISPIIMReportingModel_2.0.zip
- ISPIIMReportingPackage_2.0.zip

Note: You must set the locale to English or to any supported language before you run any of the reports. See “Setting language preferences” on page 57. Otherwise, you might encounter a “Language not supported” issue.

Configuration of IBM Cognos reporting components

After you install the prerequisites for the IBM Cognos Business Intelligence server, configure the Framework Manager, and create a content store database. Then, configure the web gateway and web server.

During the database configuration process, ensure that you complete the points in the following note.

Note:

- IBM Cognos reporting does not support Microsoft SQL Server database as content store. Use DB2 database or Oracle database instead.
- Set the JAVA_HOME environment variable to point to the JVM used by the application server.
- You must use the enterprise database as IBM Cognos content store.
- Delete the existing data source and create a new data source to enable an option of generating DDL during creation of the content store database. For information about data source creation, see “Creating a data source” on page 49.

The following table describes the configuration process.

Table 9. Configure IBM Cognos reporting components

Task	For more information
Configure Framework Manager.	<ol style="list-style-type: none">1. Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp.2. Search for Configuring Framework Manager on a 64-bit computer.
Create a content store in the database.	<ol style="list-style-type: none">1. Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp.2. Search for Start IBM Cognos Configuration and complete the steps as per your operating system.3. Search for Create a content store database.

Table 9. Configure IBM Cognos reporting components (continued)

Task	For more information
Configure the web gateway.	<ol style="list-style-type: none"> 1. Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp. 2. Search for Configure the gateway.
Configure your web server.	<ol style="list-style-type: none"> 1. Access the IBM Cognos Business Intelligence documentation at http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp. 2. Search for Configure your web server.

Setting report server execution mode

You must have a report server execution mode that is set to 32-bit mode for the report packages that do not use dynamic query mode.

Procedure

1. Start IBM Cognos Business Intelligence Configuration.
2. In the **Explorer** panel, click **Environment**.
3. Click the **Value** box for **Report server execution mode**.
4. Select **32-bit**.
5. From the **File** menu, click **Save**.

What to do next

Restart the IBM Cognos Business Intelligence service. Complete the following steps:

1. Access the IBM Cognos Business Intelligence documentation at <http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp>.
2. Search for **Restarting the IBM Cognos Business Intelligence service to apply configuration settings**.

Setting environment variables

You must set the database environment variables for a user before you start the IBM Cognos processes.

Procedure

1. Access the IBM Cognos Business Intelligence documentation at <http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp>.
2. Search for **Database environment variables**.

What to do next

Start the Cognos service from IBM Cognos Configuration to host the IBM Cognos portal. Complete the following steps:

1. Access the IBM Cognos Business Intelligence documentation at <http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp>.
2. Search for **Starting or stopping the Cognos service**.

Importing the report package

Import the report package to work with the bundled report models and the static reports.

Before you begin

- Copy the reporting package files to the directory where your deployment archives are saved. The default location is `c10_location/deployment`. For more information about the reporting packages, see “Installation of IBM Cognos reporting components” on page 45.
- To access the **Content Administration** area in IBM Cognos Administration, you must have the required permissions for the administration tasks secured feature.

Procedure

1. Access the IBM Cognos Gateway URI. For example, `https://hostname:port/ibmcognos/cgi-bin/cognos.cgi`. The *localhost* is the IP address or network host name where IBM Cognos gateway is configured. The *portnumber* is the port on which the IBM Cognos gateway is configured.
2. Go to **Launch**.
3. In the IBM Cognos Administration window, click the **Configuration** tab.
4. Click **Content Administration**.
5. Clear the history.
6. On the toolbar, click New Import icon. The New Import wizard opens.
7. In the **Deployment Archive** box, select the reporting package **ISPIMReportingPackage_2.0**.
8. Click **Next**.
9. In the **Specify a name and description** window, you can add the description and screen tip.
10. Click **Next**.
11. In the **Select the public folders and directory content** window, select the model that is displayed.
12. In the **Specify the general options** page, select whether to include access permissions and references to external namespaces, and an owner for the entries after they are imported.
13. Click **Next**. The summary information opens.
14. Review the summary information. Click **Next**.
15. In the **Select an action** page, click **Save and run once**.
16. Click **Finish**.
17. Specify the time and date for the run.
18. Click **Run**.
19. Review the run time. Click **OK**.
20. When the import file operation is submitted, click **Finish**.

Results

You can now use the report package to create reports and to run the sample reports. The sample reports are available in the reporting model on the **Public Folders** tab in the IBM Cognos portal.

Creating a data source

To work with the Privileged Identity Manager Cognos-based reports, you must create a data source.

Before you begin

- If you are working with DB2 database client, copy the file `db2cli.dll` from the DB2 client installation directory to the `<IBM Cognos installation directory>/bin` folder.
- Catalog the database if the data source is remote. Use the following commands:
 - `db2 catalog tcpip node <alias-name> remote <remote-DB-server> server <port-no>`
 - `db2 catalog database <remote-dbe> as <alias-name> at node <alias-name>`

About this task

You must use the following data source names:

- ISPIM - This data source name is used to establish connection to the IBM Security Privileged Identity Manager database.
- ISAMESSO - This data source name is used to establish connection to the IBM Security Access Manager for Enterprise Single Sign-On database.
- PSR - This data source name is used to establish connection to the Privileged Session Recording database.

Procedure

1. Access the IBM Cognos Business Intelligence product documentation at <http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp>.
2. Search for **Creating a data source** and complete the steps.

What to do next

Note: Corrupted attribute names are displayed in the reports for Arabic, Chinese, Hebrew, Japanese, Korean, and Russian languages. Double-byte character set (DBCS) characters appear to be corrupted in the reports. Edit the data source so that the data flow is in Unicode format. Complete the following steps:

1. On the Work with Reports page, click **Launch > IBM Cognos Administration**.
2. Click **Configuration** to open the data source connection.
3. Click `<data_source>`. For example: ISPIM.
4. Under the **Actions** column, click **Set properties-<data_source>**.
5. On the **Set properties-<data_source>** window, click **Connection**.
6. In the **Connection String** field, click the pencil symbol to edit the connection string.
7. In the **Collation Sequence** field, type `@UNICODE`.
8. Click **OK**.
9. Run the report to verify that the text is no longer corrupted.

Enabling the drill-through for PDF format

You must enable the drill-through functionality to run the drill-through reports in the PDF format.

Before you begin

Disable any pop-up blocking software in the browser.

Procedure

1. Open IBM Cognos Configuration.
2. Specify the fully qualified domain name for all the URIs that are defined.
3. Save the configuration.
4. Restart the IBM Cognos service. Complete the following steps:
 - a. Access the IBM Cognos Business Intelligence documentation at <http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp>.
 - b. Search for **Restarting the IBM Cognos service to apply configuration settings**.
5. In the **Explorer** window, click **Environment**.
6. In the **Group Properties** window, copy the value in the **Gateway URI** box.
7. Paste the copied **Gateway URI** value in the supported browser.
8. Run the report that you want.

Results

The drill-through report is run successfully in the PDF format.

Security layer configuration around the data model and reports

An access to the data model and reports can be restricted to a set of authorization roles. The users can create the authorization roles and associate them with the reporting entities. Only entitled users can access the data model or reports.

Authentication and authorization for IBM Cognos reports

IBM Cognos Business Intelligence administrators can set up the folders that store the reports. They can then secure those folders so that only authorized users can view, change, or perform other tasks by using the reports in the folder. To set up access control on the reports, administrators can set up the user authentication and define the access control for the set of users.

User authentication setup by using LDAP

You can configure IBM Cognos 10.2.1 Fix Pack 1 components to use an LDAP namespace for authentication when the users are in an LDAP user directory.

Configuring an LDAP Namespace for IBM Directory Server

If you configure a new LDAP namespace for use with the IBM Directory Server, you must modify the necessary settings and change the values for all properties of the IBM Directory objects.

Procedure

1. Open IBM Cognos Configuration.
2. In the Explorer window, under **Security**, right-click **Authentication**.
3. Click **New resource > Namespace**.
4. In the **Name** box, type a name for your authentication namespace.
5. In the **Type** list, click **LDAP-General default values**.

6. Click **OK**. The new authentication namespace resource appears in the Explorer window, under the **Authentication** component.
7. In the Properties window, for the **Namespace ID** property, specify a unique identifier for the namespace.

Tip: Do not use colons (:) in the Namespace ID property.

For **Host and Port**, specify <Hostname>:<port>. For example, localhost:389.

8. Specify the values for all other properties to ensure that IBM Cognos 10.2.1 Fix Pack 1 can locate and use your existing authentication namespace.

- For **Base Distinguished Name**, specify the entry for a user search.
- For **User lookup**, specify (uid=\${userID}).
- For **Bind user DN and password**, specify cn=root. For example, cn=root as a user name and secret as a password.

Note: Specify the values if you want an LDAP authentication provider to bind to the directory server by using a specific bind user DN and password. If no values are specified, an LDAP authentication namespace binds as anonymous.

9. If you do not use external identity mapping, use bind credentials to search an LDAP directory server. Complete the following items.
 - Set **Use external identity** to **False**.
 - Set **Use bind credentials for search** to **True**.
 - Specify the user ID and password for **Bind user DN and password**.
10. To configure an LDAP advanced mapping properties, see the values that are specified in the following table.

Table 10. LDAP advanced mapping values

Mappings	LDAP property	LDAP value
Folder	Object class	organizationalunit, organization, and container
	Description	description
	Name	ou, o, and cn
Group	Object class	groupofnames
	Description	description
	Member	member
Account	Name	cn
	Object class	inetorgperson

Table 10. LDAP advanced mapping values (continued)

Mappings	LDAP property	LDAP value
	Business phone	telephonenumber
	Content locale	(leave blank)
	Description	description
	Email	mail
	Fax/Phone	facsimiletelephonenumber
	Given name	givenname
	Home phone	homephone
	Mobile phone	mobile
	Name	cn
	Pager phone	pager
	Password	userPassword
	Postal address	postaladdress
	Product locale	(leave blank)
	Surname	sn
	Username	uid

If the schema is modified, you must make extra mapping changes.

11. To prevent the anonymous access, complete the following steps:
 - a. Go to **Security > Authentication > Cognos**.
 - b. Set **Allow anonymous access?** to **False**.
12. From the **File** menu, click **Save**.

Results

A new LDAP namespace is configured with the appropriate values.

What to do next

Create the users in an LDAP. See “Creating users in an LDAP.”

Creating users in an LDAP

See the example in this procedure that uses an LDAP utility to create users in LDAP.

Procedure

1. Open an LDAP utility. For example, if you are using the IBM Directory Server, the LDAP utility is `idsldapadd`.
2. Import the sample file `LdapEntries.ldif` that lists all the users who are authorized to access the reports. See the following example.

Results

After the successful import operation, you can see the users that are created in `ou=users,ou=SWG`.

Example

A sample file: `LdapEntries.ldif`

In this example, dc=com is the root entry. Specify the entry according to the schema that you use.

```
dn: ou=SWG, dc=com
ou: SWG
objectClass: top
objectClass: organizationalUnit
```

```
dn: ou=users,ou=SWG, dc=com
ou: users
objectClass: top
objectClass: organizationalUnit
```

```
dn: uid=steves,ou=users,ou=SWG, dc=com
uid: steves
userPassword:: hello123
objectClass: inetOrgPerson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: Wiley
cn: Steves
```

```
dn: uid=PortalAdmin,ou=users,ou=SWG, dc=com
userPassword:: hello123
uid: PortalAdmin
objectClass: inetOrgPerson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: Poon
cn: Chuck
```

```
dn: uid=william,ou=users,ou=SWG, dc=com
userPassword:: hello123
uid: william
objectClass: inetOrgPerson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: Hanes
cn: William
```

```
dn: uid=lucy,ou=users,ou=SWG, dc=com
userPassword:: hello123
uid: lucy
objectClass: inetOrgPerson
objectClass: top
objectClass: person
objectClass: organizationalPerson
sn: Haye
cn: Lucy
```

What to do next

Authenticate IBM Cognos Business Intelligence by using an LDAP user. Complete these steps:

1. Access the IBM Cognos Business Intelligence Gateway URI. For example, `http://localhost:portnumber/ibmcognos/cgi-bin/cognos.cgi`. The *localhost* is the IP address or network host name where IBM Cognos Business Intelligence gateway is configured. The *portnumber* is the port on which the IBM Cognos Business Intelligence gateway is configured.
2. Select the configured **Namespace**, and click **OK**.
3. Enter your LDAP user ID and password.

4. Click **OK**.

Access control definition for the reports and reporting packages

You can define the access control for the LDAP users who are the members of a role that is defined in the IBM Cognos Business Intelligence namespace. Access can be granted to those users who are the members of a defined role.

A user who has the system administrator privileges can grant the access.

Initially, all users are the members of the system administrator. Therefore, you can log in with your LDAP user authentication in IBM Cognos Business Intelligence and access the administration section before you restrict the administration access.

Restricting administration access and adding an LDAP user to system administrator role

You can restrict the IBM Cognos Business Intelligence administration access by using the system administrators role in IBM Cognos Business Intelligence namespace. You can also add an LDAP user to the system administrator role for IBM Cognos Business Intelligence report administration.

Procedure

1. Log in to IBM Cognos Business Intelligence with an LDAP user whom you want to assign the system administrator role.
2. Go to **Launch**, and click **IBM Cognos Business Intelligence Administration**.
3. Click the **Security** tab.
4. In the **Users, Groups, and Roles** section, click **Cognos**.
5. Navigate to **System Administrator** role.
6. Click the **More** link.
7. Under **Available actions**, click **Set properties**.
8. Click the **Members** tab.
9. Click the **Add** link.
10. Under **Available entries** section, click an LDAP namespace.
11. Select the **Show users in the list** check box.
12. Select the user whom you want to assign the system administrator role and make it into selected entries list.
13. Click **OK**.
14. Select **Everyone** from the members entry.
15. Click the **Remove** link to ensure that only the added users can have the system administration access.
16. Click **OK**.
17. Click the **Permissions** tab.
18. Verify that the system administrators are listed and they are provided all the permissions.
If no permissions are provided, then select the system administrators and grant all the permissions. Select the **Override the access permissions acquired from the parent entry** check box to grant the permissions.
19. Click **OK**.

Results

An LDAP user is added with the system administrator role.

What to do next

Create a role and add LDAP users as the members to that role. See “Creating a role and adding LDAP users as members.”

Creating a role and adding LDAP users as members

The topic describes the procedure to create a role in IBM Cognos and add the members from an LDAP namespace to it.

Procedure

1. Log in to IBM Cognos with an LDAP user who has the system administrator privileges. For example, PortalAdmin.
2. Go to **Launch**, and click **IBM Cognos Administration**.
3. Click the **Security** tab.
4. In the **Users, Groups, and Roles** section, click **Cognos**.
5. Click the **New Role** icon from the palette.
6. Specify the name for a role. For example, ISPIMAuditor.
7. Add the description and the screen tip.
8. Click **Next**.
9. Under **Select the members**, click **Add**.
10. Under **Available Entries Directory**, click an LDAP namespace.
11. Select the **Show users in the list** check box.
12. Select the users whom you want to add as the members to the role and make it into selected entries list.
13. Click **OK**.
14. Click **Finish**.

Results

A new role is created and LDAP users are added as the members to the new role.

Defining an access to the report by using a role

You can define an access to the report by using a role. All the members of a role can access the report or reports.

Procedure

1. Log in to IBM Cognos with an LDAP user who has the system administrator privileges. For example, PortalAdmin.
2. Under **Public Folders**, click the reporting package **ISPIMReportingPackage_2.0**.
3. Click the **More** link on the **Actions** toolbar that is associated with the report for which you want to provide the access.
4. Under **Available actions**, click **Set properties**.
5. Click the **Permissions** tab.
6. Select the **Override the access permissions acquired from the parent entry** check box.
7. Click **Add** link at the bottom of the list of entries.

8. Click **Cognos**.
9. Select the role that you want to add and make it to the selected entries.
10. Click **OK**.
11. Select the role and grant the permissions.
12. Optional: Remove other roles for which you do not want to provide the access.
13. Click **OK**.

Results

An access is defined to the report by using a role and all the members of a role can access the reports.

Defining an access to the reporting package by using a role

You can define an access to the report package by using a role. All the members of a role can access the report package.

Procedure

1. Log in to IBM Cognos with an LDAP user who has the system administrator privileges. For example, PortalAdmin.
2. Under **Public Folders**, click the **More** link on the **Actions** toolbar that is associated with the report package **ISPIMReportingPackage_2.0**.
3. Under **Available actions**, click **Set properties**.
4. Click the **Permissions** tab.
5. Select the **Override the access permissions acquired from the parent entry** check box.
6. Click the **Add** link at the bottom of the list of entries.
7. Click **Cognos**.
8. Select the role that you want to add and make it to the selected entries.
9. Click **OK**.
10. Select the role and grant the permissions.
11. Optional: Remove other roles for which you do not want to provide the access.
12. Click **OK**.

Results

An access is defined for the reporting package by using a role and the members of a role can access the reporting package.

References for IBM Cognos report security configuration

Use the following references that provide information about the topics that are related to the security configuration for the IBM Cognos reports.

Access the IBM Cognos Business Intelligence 10.2.1 documentation at <http://pic.dhe.ibm.com/infocenter/cbi/v10r2m1/index.jsp> and search for the following terms.

- **Security model.**
- **Authentication providers.**
- **Add or remove members of a cognos group or role.**

- **Create a cognos group or role.**
- **Authorization.**
- **Access permissions and credentials.**

Globalization overview

You can use the globalization features of IBM Security Privileged Identity Manager Cognos report models to produce the reports in your own language.

Language support overview

IBM Security Privileged Identity Manager Cognos reports support the following languages.

- cs=Czech
- de=German
- en=English
- es=Spanish
- fr=French
- hu=Hungarian
- it=Italian
- ja=Japanese
- ko=Korean
- pl=Polish
- pt_BR=Brazilian Portuguese
- ru=Russian
- zh_CN=Simplified Chinese
- zh_TW=Traditional Chinese

Messages or terms related to the globalization

In the reports, some of the column values might display the term Language not supported

When you select the language that is not supported by the reporting model, the value in the column is displayed as Language not supported.

Setting language preferences

You can personalize the way data appears in IBM Cognos workspace by changing your preferences. You can set the product language or content language to get the preferred output format of the reports.

Before you begin

Install and configure the IBM Cognos Business Intelligence Server version 10.2.1 Fix Pack 1.

Procedure

1. In the IBM Cognos Connection window, click **My Area Options** menu button.
2. Click **My Preferences**.
3. In the Set Preferences window, under the **Regional options** section, select **Product language**. Product language specifies the language that the IBM Cognos user interface uses.

4. In the Set Preferences window, under the **Regional options** section, select **Content language**. Content language specifies the language that is used to view and produce content in IBM Cognos such as data in the reports.
5. Click **OK**.

Results

You can view the reports or user interface in the language that you specified.

Enabling session recording replay from the report

To watch the recording of the user session on the managed resource, enable the option to replay session recording from the User Activity Audit Report. Configure the **PrivilegedIDAuditQuery** data items.

About this task

When you specify the values for the data item expressions, ensure that you put the values in single quotes.

Procedure

1. Open IBM Cognos Connection.
2. Open the Single Sign-On Privileged ID Audit Report with Report Studio. The IBM Cognos Report Studio is displayed in a new window with the Single Sign-On Privileged ID Audit Report in edit mode.
3. Open Query Explorer.
4. Double-click **PrivilegedIDAuditQuery**. The list of its corresponding data items are displayed.
5. Double-click the **Privileged Session Recording Machine** data item. The Data Item Expression window is displayed with the Single Sign-On Privileged ID Audit Report in edit mode.
6. In **Expression Definition**, add the host name or the IP address of the virtual appliance. For example: 'abc.example.com' or '127.0.0.1'
7. Double-click the **Privileged Session Recording Server Port** data item. The Data Item Expression window is displayed with the Single Sign-On Privileged ID Audit Report in edit mode.
8. In **Expression Definition**, add the port number of the Privileged Session Recording server where the session recordings are located. For example: '9080'
9. Save the changes to the Single Sign-On Privileged ID Audit Report.

Chapter 6. AccessProfiles

An AccessProfile contains instructions on handling automation for an application. It enables session recording support to your client application logon workflows and enables single sign-on automation to privileged identity management workflows.

Creating your own privileged identity management AccessProfiles

Use the IBM Security Privileged Identity Manager AccessProfile to develop or enhance your own privileged identity management scenarios.

Before you begin

- Install AccessStudio.
- Ensure that you have the Privileged Identity Management AccessProfiles. You can download the AccessProfiles from the AccessProfiles Library.

Procedure

1. In AccessStudio, open the sample AccessProfile.
2. Build or enhance the Privileged Identity Management AccessProfiles. For more information, see “Modifying AccessProfiles” on page 71.
3. Debug and start your AccessProfile.
4. Upload your AccessProfile to the IMS Server.

Privileged Session Recorder widgets

Use the Privileged Session Recorder widgets in the bundled AccessProfiles to add session recording support to your client application logon workflows.

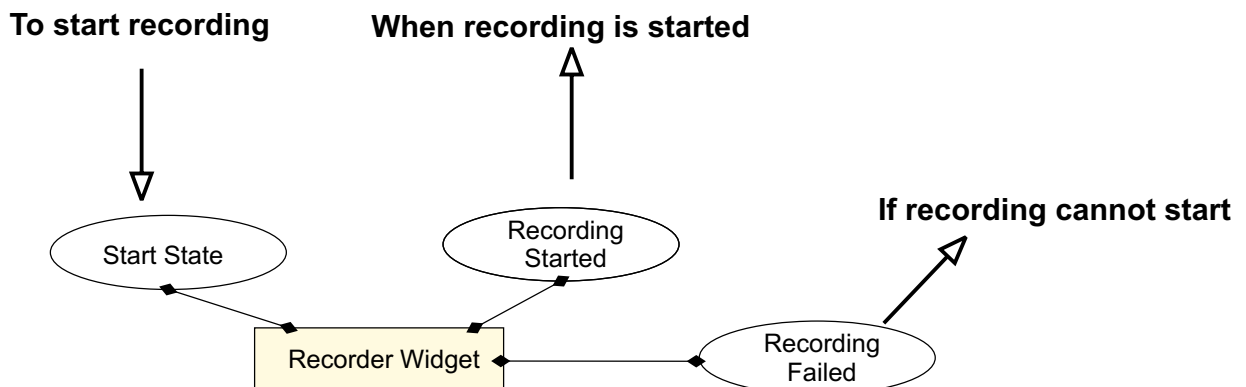


Figure 2. How the Privileged Session Recorder widgets work

Each recorder widget has an entry state, a success exit state, and a failed exit state. Some of the recorder widgets might have more than two pinnable states. For more information about pinnable states and widgets, see the *IBM Security Access Manager for Enterprise Single Sign-On AccessProfile Widgets Guide*.

IBM Security Privileged Identity Manager bundled AccessProfiles for RDP, PuTTY, IBM Personal Communications and VMware vSphere are integrated with the session recording widgets. The widgets start session recording when shared access identities are checked out.

Session recording stops when the target application is closed.

When you develop or customize an AccessProfile, add the appropriate recorder widget to the state.

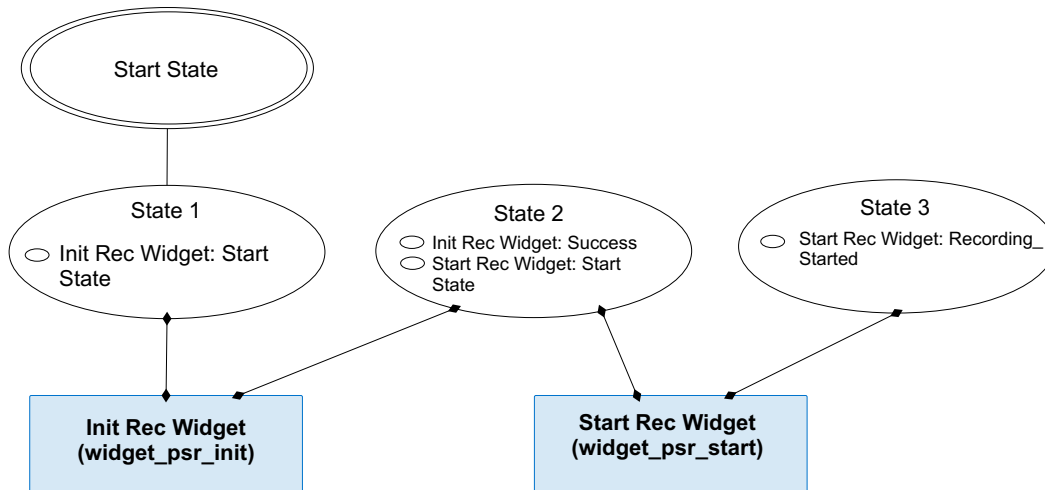


Figure 3. Example of a basic recording AccessProfile without check-in and check-out.

The following Privileged Session Recorder widgets are included:

Widget_PSR_Init

Generates the recording ID which will be used when the recording starts. Displays the message of consent dialog box.

Widget_PSR_Start

Starts a session recording. For example:

- Starts recording when a privileged identity is checked out.
- Starts recording when a secured application is started.

Widget_PSR_Pause

Pauses a session recording. For example, you can pause recording when confidential information from a personal application is being displayed in the application. Pausing a recording avoids including the confidential details in the session recording.

Widget_PSR_Resume

Resumes a session recording that is paused. For example, you can resume recording after the confidential information is no longer shown.

Widget_PSR_Stop

Stops a session recording. For example, you can stop recording when a privileged identity is checked in.

Privileged Session Recorder with the bundled AccessProfiles work in the following ways:

- Recording starts when the shared access user ID is checked out, and the user agrees to give consent for recording.
If the IBM Privileged Session Recorder Server connection is interrupted or the Privileged Session Recorder service is stopped on the client workstation, any mouse or key input for the client application might be blocked depending on the policies you configure in AccessAdmin.
For more information, see the IBM Security Access Manager for Enterprise Single Sign-On product documentation and search for privileged identity management policies.
- Recording automatically stops when the application is closed. For PuTTY, the bundled AccessProfile is designed to stop the recording when the session is inactive.

Note: If necessary, you can configure what action to take. For example, you can block user input, or close the application. Search for “Policies for Privileged Identity Management” in the IBM Security Access Manager for Enterprise Single Sign-On product documentation.

Initializing a session recording

Initialize a session recording with the **Widget_PSR_Init** widget. The widget generates a Recording ID for the recording.

Procedure

- Add the **Widget_PSR_Init** to the AccessProfile.
- Pin the **Init_Recording** state from the **Widget_PSR_Init** widget.
- Specify the necessary parameters to pass to the widget.

Recorded Application Window's XPath

Specifies the window signature.

User Consent Dialog Message

Specifies the user consent dialog box message.

Recorder Bag (Type: Account Data Bag)

Specifies the account data bag for internal use by the recording widgets.

Recording ID [Type: Property Store Item]

The ID to be associated with the recording.

Starting a session recording

Start an initialized session recording with the **Widget_PSR_Start** widget.

About this task

When a recording is started on the client workstation, a recorder tray notification is displayed in the Windows notification area.

*Table 11. Different application types use different parameter values for successful recordings with the **Widget_PSR_Start** widget.*

Parameters	VMware vSphere	Microsoft Remote Desktop Services	PuTTY (Terminal)	IBM Personal Communications (Terminal)
Listen to child process?	1	0	0	0
Terminal Window Signature	Not applicable.	Not applicable.	Passed by reference.	Passed by reference.

Table 11. Different application types use different parameter values for successful recordings with the `Widget_PSR_Start` widget. (continued)

Parameters	VMware vSphere	Microsoft Remote Desktop Services	PuTTY (Terminal)	IBM Personal Communications (Terminal)
Recording Mode	1	1	0	0

Procedure

1. Add the `Widget_PSR_Start` to the AccessProfile.
2. Pin the `Start_Recording` state from the `Widget_PSR_Start`.
3. Specify the necessary parameters to pass to the widget.

PIM Bag (Type: Account Data Bag)

Specifies the temporary data holder or cache that stores user credentials that must be checked in or checked out after AccessAgent captures credentials from the application.

Application Name (Type: Account Data Bag)

Specifies the application name that is recorded.

Recorder Bag (Type: Account Data Bag)

Specifies the account data bag for internal use by the recording widgets.

ISIM Authentication Service (Type: Account Data Bag)

Specifies the configured IBM Security Identity Manager authentication service ID as an account data bag.

Custom Metadata Name (Type: Property Store Item)

Specifies a custom metadata attribute as a property store item.

Custom Metadata Value (Type: Property Store Item)

Specifies a custom metadata value as a property store item.

Recording ID [Type: Property Store Item]

The ID to be associated with the recording.

Listen to events from child process?

Set to `1` to include child processes in the parent process session recording for certain screen-based recordings. For example, the `Listen to events from child process?` parameter is enabled in the VMware vSphere bundled AccessProfile to address the scenario in which a virtual machine is opened in a separate window. The parameter is set to `0` in the bundled AccessProfile for terminal applications.

Terminal Window Signature [Type: Property Store Item]

Specifies the unique identifier of the terminal application window element. For example, for PuTTY, the terminal window signature is `/child:wnd[@title~".*- PuTTY" and @class_name="PuTTY"]`. The property name is `Parent_Wnd_Signature`.

Recording Mode [Type: Property Store Item]

Set to `1` to start screen capture based recordings for Windows-based applications such as Microsoft Remote Desktop and VMware vSphere. Set `Recording Mode` to `0` to enable text-based recording for terminal applications such as PuTTY or IBM Personal Communications.

4. In the next state, pin the `Recording_Started` state from the `Widget_PSR_Start`.

Stopping a session recording

A recording stops when the monitored client application is closed. You can also stop a session recording with the **Widget_PSR_Stop** widget.

Procedure

1. Add the **Widget_PSR_Stop** to the AccessProfile.
2. Pin the **Stop_Recording** state from the **Widget_PSR_Stop** widget.
3. Specify the necessary parameters to pass to the widget.

PIM Bag (Type: Account Data Bag)

Specifies the temporary data holder or cache that stores user credentials that must be checked in or checked out after AccessAgent captures credentials from the application.

Capture Mode (Type: Account Data Bag)

Specifies whether screen capture already started for the account data bag.

Recorder Bag (Type: Account Data Bag)

Specifies the account data bag for internal use by the recording widgets.

Recording Mode [Type: Property Store Item]

Pass the same value as in **Widget_PSR_Start**.

Pausing a session recording

You can pause a recording that is in progress by adding an instance of the **Widget_PSR_Pause** widget to your AccessProfile. For example, you can pause recording when confidential information is being displayed in an application. Pausing avoids including the confidential information in the session recording.

Procedure

1. In AccessStudio, open your AccessProfile.
2. Add an instance of the **Widget_PSR_Pause** widget to the AccessProfile.
3. With a state in the AccessProfile selected, pin the **Pause_Recording** pinnable state.
4. With the pinned state selected, specify the necessary account data bag parameters in the **Form Editor**.

An *account data bag* is a temporary data holder or cache that stores user credentials.

PIM Bag (Type: Account Data Bag)

Specifies the temporary data holder or cache that stores user credentials that must be checked in or checked out after AccessAgent captures credentials from the application.

Capture Mode (Type: Account Data Bag)

Specifies whether screen capture already started for the account data bag.

Recorder Bag (Type: Account Data Bag)

Specifies the account data bag for internal use by the recording widgets.

Recording Mode [Type: Property Store Item]

Pass the same value as in **Widget_PSR_Start**.

5. In the next AccessProfile state, pin the **Recording_Paused** pinnable state.

Resuming a recording session

You can resume a recording session in an AccessProfile with the bundled **Widget_PSR_Resume** widget.

Procedure

1. In AccessStudio, open your AccessProfile.
2. Add an instance of the **Widget_PSR_Resume** widget to the AccessProfile.
3. With a state in the AccessProfile selected, pin the Resume_Recording pinnable state from the widget.
4. Specify the necessary parameters to pass to the widget.

Recording Mode [Type: Property Store Item]

Pass the same value as in **Widget_PSR_Start**.

5. Add another state.
6. Pin the Recording_Resumed state to the new state you added.

Shared access widgets

Use the bundled shared access widgets to add single sign-on automation to privileged identity management workflows.

Each shared access widget has an entry state, a success exit state, and sometimes, an alternate exit state.

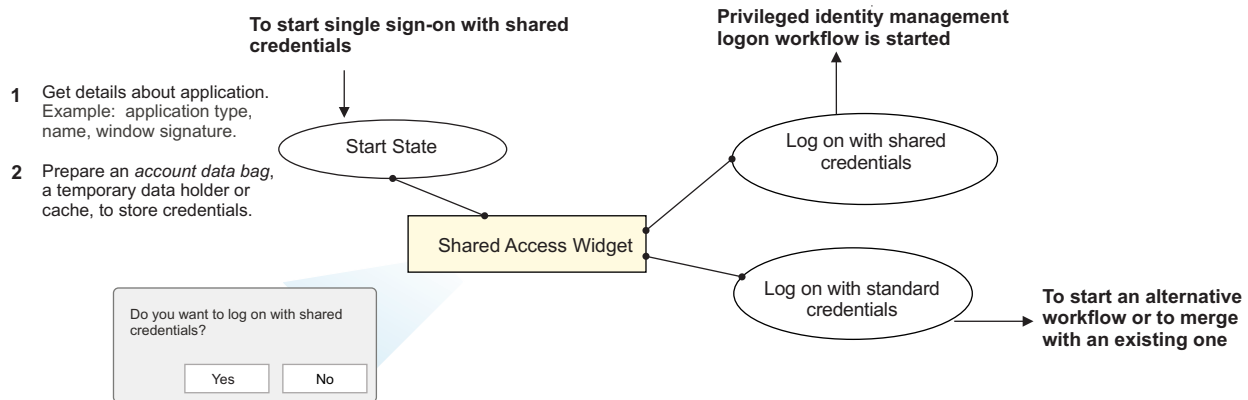


Figure 4. How a shared access widget is used in an AccessProfile

When you develop or customize an AccessProfile, pin the appropriate shared access widget to the state.

The bundled AccessProfiles for RDP, PuTTY, IBM Personal Communications, and VMware vSphere for IBM Security Privileged Identity Manager demonstrate how you can use the widgets to log on with shared credentials. The AccessProfiles are labeled in the following way `profile_appname_main`.

The widgets trigger the privileged identity management credential check-out workflows automatically when a supported application is detected.

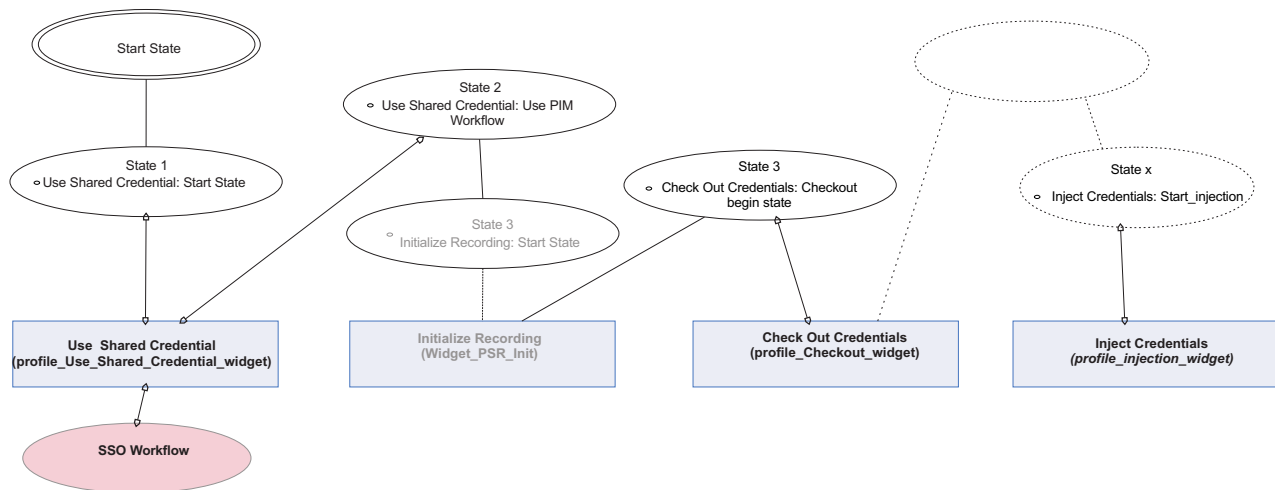


Figure 5. Example of a basic privileged identity AccessProfile that logs on with shared credentials. The check-in widget is not shown.

The following shared access widgets are included:

profile_use_shared_credential_widget

Specifies the type of credential logon workflow. Prompts the user to choose whether to log on with managed privileged credentials or not.

Table 12.

Log on with a shared credential	Action
Yes	The widget triggers the privileged identity management logon work flow with a shared credential
No	The process exits, or triggers a standard single sign-on credential workflow, if one is available.

You can use the single sign-on pinnable state to merge existing AccessProfiles that you might have for the same application. By merging AccessProfiles, an application can support both alternate and privileged identity management workflows.

profile_checkout_widget

Checks out a shared credential. This widget triggers the following actions:

- Prompts the user for IBM Security Privileged Identity Manager credentials. This process checks if the user has adequate privileges to check out credentials from a role.
- Prompts the user for the credential role to check out.

profile_<app>_injection_widgets

Injects shared access credentials into the user name and password fields for application logon. The bundled AccessProfiles use separate injection widgets for screen-based applications and terminal or mainframe applications.

- profile_RDP_and_vSphere_injection_widget: Used by RDP and VMware vSphere Client.
- profile_term_mf_injection_widget: Used by IBM Personal Communications and PuTTY.

profile_<app>_chkin_widget

Checks in the credential. There are separate check-in widgets for screen-based applications and terminal or mainframe applications.

- The check-in widget is not required in the following scenarios:
 - The application is closed by the user
 - The application closes unexpectedly due to a system issue.

The credential is still checked in automatically by the AccessAgent client.

- The check-in widget is required in some terminal scenarios. For example, in a PuTTY session with a checked out credential, you type `exit` and the session becomes inactive. The widget is required to check in the credential.

The bundled AccessProfiles work in the following ways:

- The shared credential is checked out when the user agrees to use a shared credential from a selected role.

The user is authenticated against the configured shared access authentication service. An authentication service for IBM Security Privileged Identity Manager is in the user wallet. A credential from the role is retrieved from the credential vault. The credential is added to the user wallet. The credential is then injected into the user name and password fields for the configured application.

Note: To hide the shared credential message of consent prompt for non-privileged identity users, you can create a user policy template for privileged users. See the IBM Security Privileged Identity Manager AccessAdmin policy configuration page for IBM Security Privileged Identity Manager.

- Shared credential is checked in when the application is closed.

If the IBM Security Privileged Identity Manager Server is not available, `bgmonitor` tries again until a threshold is reached. The threshold is configurable in the AccessAdmin policy configuration page for IBM Security Privileged Identity Manager.

The `bgmonitor` component is a service that ensures credentials are always checked-in on the client when an application closes unexpectedly or the system fails. The `bgmonitor` service provides the following features:

- Monitors for lease expiry of credentials.
- Starts when credential checkout is started by the AccessProfile.
- Only one instance of this process runs at a time.

A corresponding `bgmonitor` AccessProfile exists on the server. The `bgmonitor` AccessProfile triggers the `bgmonitor` process on the client when an application fails to check in any credentials.

Choosing a shared credentials logon workflow

Use a shared access credential logon workflow to prompt users for the logon workflow. Use a shared credentials logon workflow for privileged identity management. Use the alternate single sign-on workflow to merge with other existing workflows or to trigger alternative actions.

Procedure

1. Add the `profile_use_shared_credential_widget` to the AccessProfile.
2. Pin the **Start state** from the `profile_use_shared_credential_widget` widget.
3. Specify the parameters to pass to the widget.

Parent_Wnd_Signature [Property Store Item]

Specifies the unique identifier of the application window element. For example, for PuTTY, the window signature is /child::wnd[@title~"*. *- PuTTY" and @class_name="PuTTY"]. The property name is Parent_Wnd_Signature.

CICO_injection_bag [Type: Account Data Bag]

Specifies the temporary data holder or cache that stores credentials that must be checked in or checked out after AccessAgent captures credentials from the application.

Checking out credentials

Check out shared credentials from a repository and store the credentials in an account data bag.

Procedure

1. Add the **profile_checkout_widget** widget to the AccessProfile.
2. Pin the **Check out begin state** from the **profile_checkout_widget** widget.
3. Specify the parameters to pass to the widget.

CICO_injection_bag [Type: Account Data Bag]

Specifies the temporary data holder or cache that stores credentials that must be checked in or checked out after AccessAgent captures credentials from the application.

ItimSvcURL [Type: Property Store Item]

URL of the IBM Security Privileged Identity Manager check-in and check-out service. For example: https://pimhost:9081/WAR_CICO/services/CICOManager

Username window [Type: Property Store Item]

Windows signature for username window. Optional.

Password window [Type: Property Store Item]

Window signature for a password window. Optional.

ISIM Authentication Service (Type: Account Data Bag)

Specifies the configured IBM Security Identity Manager authentication service ID as an account data bag.

Check out done boolean [Type: Property Store Item]

Specify whether check-out operation is successful. 1 for a successful check-out.

RoleSelectionDlgParentHwndSignature [Type:Property Store Item]

Signature of the role selection dialog box parent window. If the parameter is an empty string, the role selection dialog box parent window is NULL.

Application Name (Type: Account Data Bag)

Specifies the application name that is recorded.

Recording ID [Type: Property Store Item]

The ID to be associated with the recording.

Injecting credentials

Inject the credentials that you checked out from the credential vault into a logon dialog prompt or username or password field with the widgets. There are different injection widgets for terminal applications and screen-based applications.

Before you begin

If necessary, check out credentials from the credential vault.

About this task

The bundled injection widgets are dependent on the type of application.

To get started with advanced profiling requirements for custom applications, start with the following injection widgets as an example.

1. Identify the type of application workflow that you want to develop.
For example, for a screen-based application, use the Remote Desktop Connection and vSphere Client examples. For a text-based or terminal application, use the PuTTY and IBM Personal Communications.
2. Open the injection widgets and the main application AccessProfile in AccessStudio.
3. Trace and observe the logon workflows that lead to a successful state in the main AccessProfiles. For example: `profile_RDP_main`, `profile_putty_main`
4. Copy the types of states, actions, scripts, and triggers that you can use.
5. Copy and modify the example VBScript actions that are used to pass parameters to each action.
6. Retrace the workflows that lead to alternate or failed exit states.

Procedure

1. Add the `profile_<appname>_inject_widget` widget to the AccessProfile.
2. Pin the **Injection begin state** from the `profile_<appname>_inject_widget` widget.
3. Specify the parameters to pass to the widget.

Table 13. Injection widget parameters for different application types.

Application	Parameters
Screen-based application	
profile_RDP_and_vSphere_injection_widget	
<ul style="list-style-type: none">• VMware vSphere Client• Microsoft Remote Desktop Connection	CICO_injection_bag [Type: Account Data Bag] Specifies the temporary data holder or cache that stores credentials that must be checked in or checked out after AccessAgent captures credentials from the application. Username window [Type: Property Store Item] Windows signature for username window. Optional. Password window [Type: Property Store Item] Window signature for a password window. Optional.
Terminal or mainframe application	
profile_term_mf_injection_widget	

Table 13. Injection widget parameters for different application types. (continued)

Application	Parameters
IBM Personal Communications	<p>CICO_injection_bag [Type: Account Data Bag] Specifies the temporary data holder or cache that stores credentials that must be checked in or checked out after AccessAgent captures credentials from the application.</p> <p>Username window [Type: Property Store Item] Windows signature for username window. Optional.</p> <p>Password window [Type: Property Store Item] Window signature for a password window. Optional.</p> <p>wnd_for_text_identification_on_mainframe_screen [Type: Property Store Item] Window for identifying text on the mainframe screen.</p> <p>Text is found for injecting username [Type: Property Store Item] Text that is identified as a field to trigger for injecting username.</p> <p>Text is found for injecting password [Type: Property Store Item] Text that is identified as a field to trigger for injecting the password.</p> <p>Text is first displayed for access denied or failure [Type: Property Store Item] Text that is first displayed when access is denied or access has failed.</p> <p>Text is found for successful logon [Type: Property Store Item] Text that is first displayed when logon is successful.</p> <p>Text is found for not injecting password [Type: Property Store Item] Text that is displayed if the password is not injected successfully.</p>
PuTTY	<p>CICO_injection_bag [Type: Account Data Bag] Specifies the temporary data holder or cache that stores credentials that must be checked in or checked out after AccessAgent captures credentials from the application.</p> <p>Username window [Type: Property Store Item] Windows signature for username window. Optional.</p> <p>Password window [Type: Property Store Item] Window signature for a password window. Optional.</p> <p>Text is first displayed for access denied or failure [Type: Property Store Item] Text that is first displayed when access is denied or access has failed.</p> <p>Text is found for successful logon [Type: Property Store Item] Text that is first displayed when logon is successful.</p> <p>Text is found for not injecting password [Type: Property Store Item] Text that is displayed if the password is not injected successfully.</p>

Checking in credentials

Use the check-in widget to check in shared credentials.

Procedure

1. Add the **profile_<appname>_chkin_widget** widget to the AccessProfile.
2. Pin the **Check in begin state** for one of the following check-in widgets.
 - **profile_RDP_and_vSphere_chkin_widget**
 - **profile_term_mf_chkin_widget**
3. Specify the parameters to pass to the widget.

Table 14. Check-in widget parameters for different application types.

Application	Parameters
Screen-based application	
profile_RDP_and_vSphere_injection_widget	
<ul style="list-style-type: none"> • VMware vSphere Client • Microsoft Remote Desktop Connection 	<p>CICO_injection_bag [Type: Account Data Bag] Specifies the temporary data holder or cache that stores credentials that must be checked in or checked out after AccessAgent captures credentials from the application.</p> <p>Username window [Type: Property Store Item] Windows signature for username window. Optional.</p> <p>Password window [Type: Property Store Item] Window signature for a password window. Optional.</p>
Terminal or mainframe application	
profile_term_mf_injection_widget	
IBM Personal Communications	<p>CICO_injection_bag [Type: Account Data Bag] Specifies the temporary data holder or cache that stores credentials that must be checked in or checked out after AccessAgent captures credentials from the application.</p> <p>Username window [Type: Property Store Item] Windows signature for username window. Optional.</p> <p>Password window [Type: Property Store Item] Window signature for a password window. Optional.</p> <p>wnd_for_text_identification_on_mainframe_screen [Type: Property Store Item] Window for identifying text on the mainframe screen.</p> <p>Text is found for injecting username [Type: Property Store Item] Text that is identified as a field to trigger for injecting user name.</p> <p>Text is found for injecting password [Type: Property Store Item] Text that is identified as a field to trigger for injecting the password.</p> <p>Text is first displayed for access denied or failure [Type: Property Store Item] Text that is first displayed when access is denied or access has failed.</p> <p>Text is found for successful logon [Type: Property Store Item] Text that is first displayed when logon is successful.</p> <p>Text is found for not injecting password [Type: Property Store Item] Text that is displayed if the password is not injected successfully.</p>

Table 14. Check-in widget parameters for different application types. (continued)

Application	Parameters
PuTTY	<p>CICO_injection_bag [Type: Account Data Bag] Specifies the temporary data holder or cache that stores credentials that must be checked in or checked out after AccessAgent captures credentials from the application.</p> <p>Username window [Type: Property Store Item] Windows signature for username window. Optional.</p> <p>Password window [Type: Property Store Item] Window signature for a password window. Optional.</p> <p>Text is first displayed for access denied or failure [Type: Property Store Item] Text that is first displayed when access is denied or access has failed.</p> <p>Text is found for successful logon [Type: Property Store Item] Text that is first displayed when logon is successful.</p> <p>Text is found for not injecting password [Type: Property Store Item] Text that is displayed if the password is not injected successfully.</p>

Modifying AccessProfiles

Modify the bundled AccessProfiles, learn how to use the widgets, or create your own AccessProfiles, to adapt to changes in applications and endpoint logon requirements.

To use session recording for customized AccessProfiles, see the bundled privileged identity management AccessProfiles that use the Recorder widgets.

Table 15. Capabilities of the different AccessProfiles

Bundled AccessProfiles	IBM Security Access Manager for Enterprise Single Sign-On	IBM Security Privileged Identity Manager
Standard single sign-on	Yes	Yes
Privileged identity management	-	Yes
Privileged identity management with session recording	-	Yes

To customize advanced AccessProfiles that are not covered, see the *IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide*. Alternatively, search the IBM website for “Advanced AccessProfile Redbooks®” for guidance.

Custom mainframe applications

Some custom mainframe applications have more logon requirements.

For example:

- Specifying more logon credential fields for credential injection.
- Simulating different keyboard keys to shift the terminal entry focus.

Use the privileged identity management AccessProfiles for IBM Personal Communications as a template.

Modifying the bundled AccessProfile for the IBM Personal Communications application

Modify the bundled IBM Personal Communications AccessProfile to customize its behavior.

Before you begin

- Install AccessStudio.
- Install the IBM Personal Communications client.
- Open the Personal Communications application.
- Upload the AccessProfiles to the IMS Server. See “Uploading AccessProfiles to the IMS Server” on page 76.

Tip: Before you apply any modifications, you can take a local backup of the AccessProfile. To back up the AccessProfile to file, you can save the AccessProfile to a location on your computer.

Procedure

1. Start AccessStudio.
2. Import the Privileged Identity Management AccessProfile package into the AccessStudio workspace by clicking **File > Import data from IMS**.
3. In the **AccessProfile** pane, open profile_PCOMM_main.
4. Select the **States** tab.
5. In the **AccessProfile** state diagram canvas, select the **Run a VBScript or JScript** action under the second state.
6. In the **Properties** pane, select the **Form Editor** tab.
7. Click **Open Script Editor**.
8. Edit the script.

- a. Select a unique text from the mainframe application screen.
- b. Remove the variable portion of the text.
- c. Retain the non-variable portion of the text in the form of a regular expression. For example:

- **Unique text:** WELCOME UserA
- **Variable:** UserA
- **Non-variable:** WELCOME
- **Regular expression of the non-variable text:** WELCOME.*

This regular expression matches any instances of text that might be displayed as:

```
WELCOME
-WELCOME-
EXAMPLE APPLICATION WELCOME
```

This regular expression does not match the following instances:

```
welcome
Welcome
Example Welcome
W.E.L.C.O.M.E
```

- d. Modify the second argument for each pc.SetPropValue entry. You can add the regular expression or replace the existing regular expression.

```
pc.SetPropValue "text_to_identify_the_welcome_screen",
  "^.*WELCOME.*$|.*User\sID\s:.*"
```

```
pc.SetPropValue "text_to_identify_and_initiate_PIM_workflow",
```

```

        .*WELCOME\STO\SCICS.*|. *User\sID\s:.*"
pc.SetPropValue "text_is_found_for_injecting_username",
    ".*[Ll]ogin.*:.*|. *LOGIN.*:.*|. *WELCOME\STO\SCICS.*|. *Userid.*|
    .*User\sID.*"
pc.SetPropValue "text_is_found_for_injecting_password",
    ".*(?i)(please type your password|missing password).*"
pc.SetPropValue "text_is_found_for_not_injecting_password",
    ".*(?i)(your userid is invalid).*"
pc.SetPropValue "text_is_first_displayed_for_access_denied_or_failure",
    ".*[Dd]enied.*|. *DENIED.*|. *[Ii]nvalid.*|. *not\sdefined\.*"
pc.SetPropValue "text_is_found_for_successful_logon",
    ".*[Ll]ast login.*:.*|. *LAST LOGIN.*:.*|. *Microsoft\sWindows.*|
    .*Sign-on\s\scomplete.*|. *Enterprise\sSummary.*"
pc.SetPropValue "Wnd_sig_Username",
    "/child::wnd[@class_name="\"PCSWS:Main:00400000\"]"
pc.SetPropValue "wnd_for_text_identification_on_mainframe_screen",
    "/child::wnd[@class_name="\"PCSWS:Main:00400000\""]/
    child::wnd[@class_name="\"PCSWS:Pres:00400000\" and @ctrl_id=2]"
pc.SetPropValue "Parent_Wnd_Signature",
    "/child::wnd[@class_name="\"PCSWS:Main:00400000\""]/
    child::wnd[@class_name="\"PCSWS:Pres:00400000\" and @ctrl_id=2]"
'Displays a consent dialog box with a custom message before starting
session recording.
pc.SetPropValue "recording_consent_dialog_custom_message", ""

'Specifies the parent window signature for the consent dialog message
pc.SetPropValue "recording_consent_dialog_parent_xpath",
    "/child::wnd[@class_name="\"PCSWS:Main:00400000\""]/
    child::wnd[@class_name="\"PCSWS:Pres:00400000\" and @ctrl_id=2]"

'Specifies the additional custom metadata that will be passed to the
Privileged Session Recorder Server during session recording
'For example, pc.SetPropValue "param_custom_metadata", "Department_Name"
pc.SetPropValue "param_custom_metadata", ""

'Specifies the value for the above specified
custom metadata that will be passed to the Privileged Session Recorder
Server during session recording
'For example, pc.SetPropValue "param_value", "IT"
pc.SetPropValue "param_value", ""

'Specifies whether to enable either text based or screen based recordings
for terminal or Windows applications respectively
'For example, for Terminal applications such as PuTTY and PCOMM, to have
text based capture, set the value to 0. For screen based capture with
Windows based applications such as RDP and vSphere set the value to 1.
pc.SetPropValue "RecordingMode", "0"

'Specifies the algorithm to be used for command recognition
in text-based recordings. This value is ignored in screen-based recordings.
'Set this value to 1 for text recording of UNIX sessions. Otherwise, set it
to 0.
pc.SetPropValue "psr_command_recognition_algo", "1"

```

9. Test the AccessProfile.

a. Start **Test Mode**.

b. Start IBM Personal Communications.

10. After the test is completed, save the AccessProfile. The AccessProfile on the IMS Server is updated.

Note: If you are working from a local copy of the AccessProfile, remember to publish the completed AccessProfile to the IMS Server.

Modifying the bundled AccessProfile for the PuTTY application

You can modify the bundled PuTTY application AccessProfile to customize its behavior.

Before you begin

- Install AccessStudio.
- Install the PuTTY client.
- Open the PuTTY application.
- Upload the AccessProfiles to the IMS Server. See “Uploading AccessProfiles to the IMS Server” on page 76.

Tip: Before you apply any modifications, you can take a local backup of the AccessProfile. To back up the AccessProfile to file, you can save the AccessProfile to a location on your computer.

Procedure

1. Start AccessStudio.
2. Import the Privileged Identity Management AccessProfile package into the AccessStudio workspace by clicking **File > Import data from IMS**.
3. In the **AccessProfile** pane, open profile_putty_main.
4. Select the **States** tab.
5. In the **AccessProfile** state diagram canvas, select the **Run a VBScript or JScript** action under the second state.
6. In the **Properties** pane, select the **Form Editor** tab.
7. Click **Open Script Editor**.
8. Edit the script.
 - a. Select a unique text from the mainframe application screen.
 - b. Remove the variable portion of the text.
 - c. Retain the non-variable portion of the text in the form of a regular expression. For example:
 - **Unique text:** WELCOME UserA
 - **Variable:** UserA
 - **Non-variable:** WELCOME
 - **Regular expression of the non-variable text:** WELCOME.*This regular expression matches any instances of text that might be displayed as:

```
WELCOME
-WELCOME-
EXAMPLE APPLICATION WELCOME
```

This regular expression does not match the following instances:

```
welcome
Welcome
Example Welcome
W.E.L.C.O.M.E
```
 - d. Modify the second argument for each pc.SetPropValue entry. You can add the regular expression or replace the existing regular expression.

```
pc.SetpropValue "text_is_found_for_injecting_password",
  ".*[Pp]assword.*|. *PASSWORD.*"

pc.SetpropValue "text_is_found_for_not_injecting_password",
```

```

    ".*[Dd]enied.*|.DENIED.*"

pc.SetPropValue "text_is_first_displayed_for_access_denied_or_failure",
    ".*[Dd]enied.*|.DENIED.*|[Ii]nvalid.*|.not\sdefined\.*"

pc.SetPropValue "text_is_found_for_successful_logon",
    ".*[Ll]ast login.*|.LAST LOGIN.*|.$.*.>.*|.##.*|
    .*Microsoft\Windows.*|.Sign-on\sis\scomplete.*|
    .*Enterprise\Ssummary.*"

pc.SetPropValue "Parent_Wnd_Signature",
    "/child::wnd[@title~\".*- PuTTY\" and @class_name=\"PuTTY\"]"

pc.SetPropValue "wnd_for_text_identification_on_mainframe_screen",
    "/child::wnd[@title~\".*- PuTTY\" and @class_name=\"PuTTY\"]"

'Displays a consent dialog box with a custom message before starting
session recording.

'Specifies the text that would appear on the consent
message (custom consent message) for session recording
pc.SetPropValue "recording_consent_dialog_custom_message", ""

'Specifies the parent window signature for the consent dialog message
pc.SetPropValue "recording_consent_dialog_parent_xpath",
    "/child::wnd[@title~\".*- PuTTY\" and @class_name=\"PuTTY\"]"

'Specifies the additional custom metadata that will be passed to the
Privileged Session Recorder Server during session recording
'For example, pc.SetPropValue "param_custom_metadata", "Department_Name"
pc.SetPropValue "param_custom_metadata", ""

'Specifies the value for the above specified custom metadata
that will be passed to the Privileged Session Recorder Server during
session recording
'For example, pc.SetPropValue "param_value", "IT"
pc.SetPropValue "param_value", ""

'Specifies whether to enable either text based recordings for terminals
or screen based recordings for Windows based applications.
'For example, for Terminal applications such as PuTTY and PCOMM, to enable
text-based recordings, set the value to 0. For Windows based applications
such as RDP and vSphere, to have screen based capture, set the value to 1.
pc.SetPropValue "RecordingMode", "0"

'Specifies the algorithm to be used for command recognition
in text-based recordings. This value is ignored in screen-based recordings.
'Set this value to 1 for text recording of UNIX sessions. Otherwise, set it
to 0.
pc.SetPropValue "psr_command_recognition_algo", "1"

```

9. Test the AccessProfile.

- a. Start **Test Mode**.
- b. Start PuTTY.

10. After the test is completed, save the AccessProfile. The AccessProfile on the IMS Server is updated.

Note: If you are working from a local copy of the AccessProfile, remember to publish the completed AccessProfile to the IMS Server.

Multiple AccessProfiles for the same client application

Each application signature for an AccessProfile must be unique. Single sign-on cannot occur if there are multiple AccessProfiles with the same application signature on the IMS Server.

If you have more than one AccessProfile for the same application, consider deleting or modifying copies of the AccessProfile.

Note: Duplicate AccessProfiles with signature conflicts are also logged in the AccessAgent logs as errors.

For example, a Remote Desktop Connection (RDP) AccessProfile is already on the IMS Server.

- You might already have a custom Remote Desktop Connection (RDP) AccessProfile for logging on to remote desktops.
- If you upload a new privileged identity management AccessProfile with the same application signature, single sign-on does not trigger.
- Consider the actions that you can take to resolve the issue.
 - Delete the existing AccessProfile for the RDP application from the IMS Server if the AccessProfile is not in use.
 - Merge the AccessProfiles.

Important: Privileged identity management AccessProfiles work only with AccessAgent, Version 8.2.1

Identifying AccessProfile collision

You can use the AccessStudio message pane logs to determine whether there are multiple AccessProfiles for the same client application on the IMS Server.

Before deployment, complete these steps on a test computer with the AccessAgent installed:

1. Ensure that you are logged on to AccessProfiles.
2. Import data from the IMS Server with AccessStudio.
3. Start the client application that you are testing for AccessProfile collision.
4. From the AccessStudio real-time logs, look for the phrase:
...multiple AccessProfiles were found.

Merging AccessProfiles

If you want both the privileged identity management AccessProfiles and the AccessProfiles you already have, then you must consider advanced AccessProfile merging.

For help with advanced AccessProfile merging, contact IBM Services.

Uploading AccessProfiles to the IMS Server

To activate and use the AccessProfile, upload the AccessProfile to the IMS Server.

Before you begin

If you have multiple AccessProfiles, see “Multiple AccessProfiles for the same client application” on page 75 for a better understanding before you upload AccessProfiles to the IMS Server.

About this task

There are four AccessProfiles available for upload to the IMS Server.

You must upload the following AccessProfiles:

- Use_Shared_Credentials_Authentication_Service.eas

- Concurrent_profiles_bgMonitor_Wnd_Explorer.eas

Then, upload either of these AccessProfiles:

- PIM_Profiles_With_General_RDP_Flow.eas

This AccessProfile contains both privileged identity management workflows and non-privileged identity management workflows.

Use this AccessProfile if single sign-on to RDP is also required for non-privileged users.

Note:

- This AccessProfile is just an example of a merged AccessProfile.
- If the non-privileged identity management workflows included in this AccessProfile is outdated, download the latest version of the AccessProfile from the AccessProfiles Library. After you download the latest version, merge it with the RDP AccessProfile for the privileged identity management workflow. The RDP Profile ID is profile_RDP_main.
- PIM_Profiles.eas
This AccessProfile contains the privileged identity management workflows only.

If you cannot find or download these AccessProfiles from the AccessProfiles Library, you can get the files from this location:

<IMS Server installation folder>\com.ibm.tamesso.ims-delhi.build.boot\src\config\data\config\pim\Profiles.

For example: C:\Program Files\IBM\ISAM ESSO\IMS Server\com.ibm.tamesso.ims-delhi.build.boot\src\config\data\config\pim\Profiles.

Procedure

1. Open the command prompt.
2. Browse to <IMS Server installation folder>\bin.
3. Run the following command:

```
uploadSync.bat <was_admin> <was_admin_password>
--dataFile "<accessprofile_absolute_path>".
```

For example:

```
C:\Program Files\IBM\ISAM ESSO\IMS Server\bin>uploadSync.bat wasadmin
p@ssw0rd --dataFile "C:\Program Files\IBM\ISAM ESSO\IMS
Server\com.ibm.tamesso.ims-delhi.build.boot\src\config\data\config\pim\
Profiles\Concurrent_profiles_bgMonitor_Wnd_Explorer.eas"
```

Related information:

 AccessProfiles Library

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web

sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at <http://www.ibm.com/legal/copytrade.shtml>.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.



Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Privacy Policy Considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering uses other technologies that collect each user's user name, password or other personally identifiable information for purposes of session management, authentication, single sign-on configuration, usage tracking, or functional purposes. These technologies can be disabled, but disabling them will also eliminate the functionality they enable.

This Software Offering does not use cookies to collect personally identifiable information. The only information that is transmitted between the server and the browser through a cookie is the session ID, which has a limited lifetime. A session ID associates the session request with information stored on the server.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at <http://www.ibm.com/privacy> and IBM’s Online Privacy Statement at <http://www.ibm.com/privacy/details/us/en> sections entitled “Cookies, Web Beacons and Other Technologies” and “Software Products and Software-as-a Service”.



Printed in USA