IBM Security Directory Suite
8.0.1

Installation and Configuration Guide

Note

Before using this information and the product it supports, read the general information under "Notices" on page 73.

Edition notice

Note: This edition applies to version 8.0.1.x of *IBM Security Directory Suite* (product number 5725-Y17) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this publication

IBM® Security Directory Suite, previously known as IBM Security Directory Server or IBM Tivoli® Directory Server, is an IBM implementation of the Lightweight Directory Access Protocol.

IBM Security Directory Suite Installation and Configuration Guide contains information for installing, configuring, and uninstalling IBM Security Directory Suite. It also includes information about upgrading from a previous version.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

For more information, see "Accessibility features for IBM Security Directory Suite" in the IBM Knowledge Center.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection, and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated, or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Chapter 1. Hardware and software requirements

The IBM Security Directory Suite virtual appliance has specific hardware and software requirements.

Virtual hypervisors

- VMware ESXi, Version 5.5 or later
- Kernel-based Virtual Machine (KVM), Version 0.10.0 or higher on RHEL 6 or RHEL 7, and Version 16.04.5 TLS on Ubuntu
- XenServer, Version 6.5

Hardware requirements

- CPU: 2.2 GHz, 4 cores (64-bit)
- Minimum 4 GB system memory
- Disk space: Minimum 40GB free hard disk space (20GB is used for active partition and 20GB for backup partition)
- Network interface cards: 3

Note: Adjust the CPU, memory, and disk space according to your data load requirements.

Software Requirements

IBM Security Directory Suite comes with all the required software in its ISO image.

The following browsers are supported for the graphical user interface of the virtual appliance console:

- Microsoft Internet Explorer, Version 9 or later
- Mozilla FireFox, Version 17.0 or later

Detailed System Requirements

You can use the Software Product Compatibility Reports to view the following detailed information about IBM Security Directory Suite:

- Operating systems
- Prerequisites
- Hypervisors
- Translations
- Detailed system requirements
- Hardware requirements
- End of service

For more information, see “Customizing system requirements search” on page 1.

Customizing system requirements search

You can customize your system requirements search for IBM Security Directory Suite, that match your filter criteria.

Procedure

1. Open the Software Product Compatibility Reports website.
2. Select the required report option for which you want to view the report.

   You can choose one of the following options:

   - Operating systems

- Prerequisites
- Hypervisors
- Translations
- Detailed system requirements
- Hardware requirements
- End of service

3. To generate a report for detailed system requirements, select the **Create a report** link for the search criteria, `Detailed system requirements`.
4. On the **Detailed system requirements for a specific product** page, provide the following values:
   a) In the **Full or partial product name** field, enter the product name, `IBM Security Directory Suite`.
   b) From the **Search results** list, select the appropriate product name.
   c) From the **Version** list, select the appropriate version number.
   d) For **Scope of report**, select the appropriate option.
   e) From the **Operating system family** list, select an appropriate operating system.
   f) Click **Submit**.

Results

The Software Product Compatibility Reports website generates a report that match your search criteria.

Chapter 2. Virtual appliance installation

The IBM Security Directory Suite comes in a virtual appliance format.

The virtual appliance can be hosted on one of the following supported virtual hypervisors:

- VMware ESXi, Version 5.5 or later
- Kernel-based Virtual Machine (KVM), Version 0.10.0 or higher on RHEL 6 or RHEL 7, and Version 16.04.5 TLS on Ubuntu
- XenServer, Version 6.5

VMware support

The IBM Security Directory Suite virtual appliance can be installed on a VMware ESXi, Version 5.5 or later hypervisor.

The IBM Security Identity Manager virtual appliance for VMware is distributed as a pre-installed disk image of the virtual appliance in `.iso` format.

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

Setting up the virtual machine

Set up the virtual machine that you must use to host the virtual appliance.

Procedure

1. Download the `8.0.1.`*`x`*`-ISS-ISDS_`*`build number`*`.iso` build.
2. Create a virtual machine on ESXi 5.5 or later with the following configuration.
   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) For the virtual appliance, the expected guest operating system is Linux® with version 2.6.x 64 bit.
   f) Enter the number of virtual sockets and cores per virtual sockets for the virtual machine.
   For example, enter the value as 2 for the following options to sum up the total number of cores to 4.
      - **Number of virtual sockets**
      - **Number of cores per virtual socket**

   g) Enter the memory size.
   See Chapter 1, “Hardware and software requirements,” on page 1.
   h) Set the number of network connections.

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

   i) Set **E1000** as the network adapter.
   j) Set the SCSI controller type to **LSI Logic Parallel**.
   k) Select the **Create a new virtual disk** option as the type of disk to use.
   l) Enter the disk size for the virtual machine.
   See Chapter 1, “Hardware and software requirements,” on page 1.
   m) Accept the default settings in the **Advanced Options** page.
3. Check summary for the configuration accuracy.

4. Select the **Edit the virtual machine settings before completion** check box to proceed.
5. Click **Add** in the **Hardware** tab of the **Virtual Machine Properties** window.
6. Choose **CD/DVD drive**.
7. Select the type of media that you want the virtual drive to access.
   For example, select **Use ISO image**.
8. Browse to the location of the `.iso` file that is uploaded in the data store.
9. Click **Finish** on the **Add Hardware** window.
10. Select the **Connect at power on** check box on the **Virtual Machine Properties** window.
11. Click **Finish** on the **Virtual Machine Properties** window.
12. Click **Power on the virtual machine** to proceed with the virtual appliance installation.
13. Optional: To mount or change the IBM Security Directory Suite media for an existing virtual machine, do these steps.
    a) List the options. Right-click on virtual machine that you created, and then select **Edit Settings**.
    b) Click **Add** in the **Hardware** tab of the **Virtual Machine Properties** window.
    c) Choose **CD/DVD drive 1**.
    d) Browse to the location of the `.iso` file that is uploaded in the data store.
    e) Select the type of media that you want the virtual drive to access.
    For example, select **Use ISO image**.
    f) Select the **Connect at power on** check box on the **Virtual Machine Properties** window.
    g) Click **Power on the virtual machine** to proceed with the virtual appliance installation.

What to do next

Proceed with the virtual appliance installation.

Installing the virtual appliance on VMware

Install IBM Security Directory Suite virtual appliance on a VMware ESXi, Version 5.5 or later hypervisor.

Before you begin

You must complete the steps for setting up the virtual machine. See “Setting up the virtual machine” on page 3,

Procedure

1. When you start the virtual machine for the first time, press enter to continue with the virtual appliance installation.
2. Select the language that you want to use during the installation.
   For example, specify 1 for **English**.
3. Enter as `yes` to proceed with the firmware image installation process.
4. When the installation process is complete, do these steps to unmount the installation media.
   a) Right-click on the virtual machine, and then select **Edit Settings**.
   b) On the **Hardware** tab of the **Virtual Machine Properties** window, select **CD/DVD drive 1**.
   c) Clear these device status option check boxes.
   - **Connected**
   - **Connect at power on**
5. Click **OK** to close the **Virtual Machine Properties** window.
6. Select **Yes** and click **OK** to confirm the installation media disconnection.
7. Press the Enter key and then press any key to continue with the installation process.

Results

Proceed with setting up the initial virtual appliance. See “Setting up the virtual appliance” on page 8.

KVM support

You can install the IBM Security Directory Suite virtual appliance on a Kernel-based Virtual Machine (KVM), Version 0.10.0 or higher on RHEL 6 or RHEL 7, and Version 16.04.5 TLS on Ubuntu.

The IBM Security Directory Suite virtual appliance for KVM is distributed as a pre-installed disk image of the virtual appliance in `.iso`.

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

A network bridge is required to setup network interface for the KVMs.

Important:

Some library versions that are installed with RHEL 7 do not support installation of the IBM Security Directory Suite virtual appliance `.iso` image.

Ensure that the following compatible versions of the libraries are installed on the RHEL 7 system. IBM Security Directory Suite supports only the following versions:

```
libgovirt-0.1.0-3.el7.x86_64.rpm
virt-install-0.10.0-20.el7.noarch.rpm
virt-manager-0.10.0-20.el7.noarch.rpm
virt-manager-common-0.10.0-20.el7.noarch.rpm
virt-viewer-0.5.7-7.el7.x86_64.rpm
```

Installing the virtual appliance on RHEL and Ubuntu KVM

Install IBM Security Directory Suite virtual appliance on a Kernel-based Virtual Machine (KVM), Version 0.10.0 or higher on RHEL 6 or RHEL 7, and Version 16.04.5 TLS on Ubuntu.

Procedure

1. Run the **`virt-manager`** command to open the **Virtual Machine Manager**.
2. Click **Create a New Virtual Machine**.
3. On the wizard, enter a name for the virtual machine.
4. Select **Local install media (ISO image or CDROM)**.
5. Click **Forward**.
6. Select **Use ISO image** and click **Browse** to select the product ISO file.
7. Select the operating system as **GENERIC** with Version **GENERIC**.
8. Click **Forward**.
9. Enter the memory size.
   For example, 1024 GB.
10. Set the number of CPUs.
    For example, 8.
11. Click **Forward**.
12. Enter the disk size of the virtual machine.
    For example, 50 GB.
13. Click **Forward**.
14. Select the network bridge.
15. Select **Customize configuration before install**.
16. Click **Finish**.
17. Click **Add Hardware**.
18. Select **Network**.

19. Select the network bridge and click **Finish**.
20. Click **Add Hardware** again.
21. Select **Network**.
22. Select the network bridge and click **Finish**.
23. Click **Processor** and select **Configuration**.
24. For model selection, select **Clear CPU configuration**, and click **Apply**.
25. Click **Begin Installation**.
26. On the KVM console, follow the steps to complete the installation.
27. Press **Enter** key after the disk partitioning and installation is complete.
    Wait for the appliance login prompt (`unconfigured.appliance login:`) to be displayed.
28. Provide the following user credentials when the system restarts after the virtual appliance installation.
    - **Unconfigured login**: `admin`
    - **Password**: `admin`

What to do next

Proceed with setting up the initial virtual appliance. See "Setting up the virtual appliance" on page 8.

XenServer support

The IBM Security Directory Suite virtual appliance can be installed on a XenServer, Version 6.5 hypervisor.

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

The IBM Security Directory Suite virtual appliance for XenServer is distributed as a pre-installed disk image of the appliance in Virtual Hard Disk (VHD) format. Standard installation ISO images cannot be used due to some restrictions with XenServer. The disk has a fixed size of 100 GB. It is recommended to enable off-the-box logging and auditing to ensure that the disk is not consumed with log files.

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

Installing the virtual appliance on XenServer

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

Before you begin

Ensure that you have the following prerequisites:

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

Procedure

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

Note: In most scenarios, assign the virtual machine at least one processor and 2 GB of memory. These settings can be adjusted after the virtual machine starts running.

b) Click **Next**.

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

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

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

    Note: The import operation might take a considerable amount of time to complete. You can click the **Logs** tab to check the progress of the import.
11. When the import is complete, run the following commands on the XenServer console to set the image to paravirtualized mode.

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

    For example:

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

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

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

12. Start the imported virtual machine.

Note: At least 3 network interfaces must be configured in order for the virtual appliance to start. Sometimes the XenCenter must be restarted before the new virtual appliance can be started correctly.

What to do next

Proceed with setting up the initial virtual appliance. See “Setting up the virtual appliance” on page 8.

Setting up the virtual appliance

For the virtual appliance, the appliance setup wizard runs the first time when you connect to the virtual console of an unconfigured virtual appliance.

Procedure

1. Provide the following user credentials when the system restarts after the virtual appliance installation:
   - **Unconfigured login**: `admin`
   - **Password**: `admin`
2. On the virtual appliance setup wizard screen, press Enter to continue.
3. Choose one of these options to proceed.
   - Press 1 to choose the language.
   - Press 2 to read the IBM terms.
   - Press 3 to read 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: Proceeed to acceptance

Select option: 4


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

Select option: 1
```

4. Select option 1 to accept the terms.
5. Optional: Select option 1 to enable FIPS.

   Important: Enable FIPS only if you need it because it cannot be disabled after it is enabled. For more information, see Chapter 10, “FIPS compliance,” on page 67.

```
FIP 140-2 Mode Configuration

You must enable FIPS mode in order to comply with FIPS 140-2 and NIST 800-131a.

If you select the enable FIPS mode, appliance will be rebooted immediately to
perform FIPS power-up integrity checks.
Do not choose to enable FIPS mode without reading the FIPS section in the user
guide.

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

FIPS 140-2 Mode is not enabled.
1: Enable FIPS 140-2 Mode
x: Exit
p: Previous screen
n: Next screen

Select option: 1


FIPS 140-2 Configuration
Enable FIPS 140-2 mode?
1: yes
2: no
Enter index: 1
You have selected to enable FIPS mode. The appliance will now reboot to perform
the FIPS integrity checks.
When appliance comes back up, you will need to login as admin useer to complete
the setup.
Enter 'YES' to confirm: YES
```

6. If you enabled FIPS, then restart the system.
7. 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
```

8. Change the host name.

   Use a registered host name or static IP address to manage the virtual appliance for networking and recording important information for configuring the virtual appliance network.

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

Host Name Configuration
Host name: sdsva.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.

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

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

Select option: 3

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

10. Configure the DNS for the virtual appliance.

    Use only a DNS registered IP address to manage the virtual appliance for configuring the virtual appliance network.

```
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
```

11. Configure the time settings for the virtual appliance.

    Note: If you want to use this virtual appliance as a member node in the cluster, use the same date and time settings that you used to set up the virtual appliance for the primary node.

```
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
```

12. Review the summary of configuration details.

    Note: After you configure the FIPS mode, you cannot change the configuration. On the summary screen, if you select the option to modify the configuration, and then try to select the option to change FIPS mode, the selection moves to the next available option on the screen. If you enabled FIPS mode and now want to disable it, or vice versa, you must reinstall virtual appliance.
13. Press 1 to accept the configuration.

Results

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

What to do next

Restart the virtual appliance. At the *hostname* command prompt, enter `reboot`. After the virtual appliance is restarted, log on to the virtual appliance console.

Logging on to the virtual appliance console

To get started after you install the virtual appliance, you need to know the login URL and the user name and password.

About this task

The following browsers are supported for the graphical user interface of the virtual appliance console:

- Microsoft Internet Explorer, Version 9 or later
- Mozilla FireFox, Version 17.0 or later

Procedure

1. In a supported web browser, type the URL as `https://`*`sdsva_hostname`* to open the **Appliance Dashboard** of the virtual appliance.

   For example, `https://sdsva.example.com`.
2. Enter the user name as `admin`.
3. Enter the admin user's password.
4. Click **Login**.

Results

When you log in for the first time, IBM Security Directory Suite - Limited Edition is displayed by default.

What to do next

If you purchased the IBM Security Directory Suite,Standard or Enterprise Edition, you can activate your license by using virtual appliance console. See Activating IBM Security Directory Suite license.

Unlocking a locked admin user

The virtual appliance admin user account is locked out after 10 failed login attempts. The account is unlocked after 60 minutes.

About this task

The IBM Security Directory Suite virtual appliance admin user is locked out after 10 failed attempts to log in to the virtual appliance console or the command-line interface. The locked admin user account can be unlocked with the following methods.

Procedure

1. If the admin user is locked after 10 failed attempts to log in to the virtual appliance console, take one of the following actions:
   - Wait for 60 minutes after which the admin user is automatically unlocked.
   - Use the **unlockadmin** command to unlock the admin user account immediately. From the virtual appliance command-line interface, run the following command:

     ```
     sds server_tools unlockadmin
     ```

     This command deletes the failed login attempt lock file and allows the admin user to log in to the virtual appliance console. For more information, see **unlockadmin**.
2. If the admin user is locked after 10 failed attempts to log in to the virtual appliance command-line interface, you must wait for 60 minutes until the admin user is automatically unlocked.

Default settings for IBM Security Directory Suite virtual appliance

The default ports, passwords, locations, and other default values that are used by IBM Security Directory Suite virtual appliance are listed here.

Default settings for virtual appliance console

If you want to upload your certificate file, use the Custom File Management option of IBM Security Directory Suite virtual appliance. Follow the steps in the topic, Managing custom files.

Table 1. Default settings for virtual appliance console

Description	Default settings
Login URL	https://[host_name]/login
Login user name	admin
Login password	admin
Key database certificate file	/userdata/directory/Certificates/filename.kdb
Java keystore file	/userdata/directory/Certificates/jksfile.jks

Default settings for Web Administration Tool

Table 2. Default settings for Web Administration Tool	
Description	**Default settings**
Login URL	`https://[host_name]:12101/IDSWebApp/IDSjsp/Login.jsp`
Login user name	superadmin
Login password	secret
HTTPS port	12101
Truststore and keystore	`/userdata/directory/Certificates/defaultwebadmin.jks`
Password for `defaultwebadmin.jks`	secret

Default settings for Directory Server

Note:

- To change the administrator DN credentials, follow the steps in the topic, Changing the administrator DN credentials.
- To regenerate and upload a key stash file for Directory Server, see the topic, Managing custom files and follow the steps in the section, **Step 2** > **To upload a file** > **etc**.

Table 3. Default settings for Directory Server	
Description	**Default setting**
Administrator DN	cn=root
Administrator DN password	root
Keystore password	server
Path to key database files	/userdata/directory/Certificates/
Non-SSL port	389
SSL port	636
Key stash file	

Default settings for Directory Administration Server

Table 4. Default settings for Directory Administration Server	
Description	**Default setting**
Non-SSL port	3538
SSL port	3539

Default settings for Federated Directory Server with Directory Server as target

Table 5. Default settings for Federated Directory Server with Directory Server as target	
Description	**Default settings**
Login URL	https://[host_name]:1098/fds

Table 5. Default settings for Federated Directory Server with Directory Server as target (continued)	
Description	**Default settings**
Login user name	admin
Login password	admin
Path to key database file	/userdata/directory/Certificates/ FDS_Default_SSLCerts
Keystore password	administrator
Server port	1099
Web server port	1098
Derby port	4527
Active MQ port	61619

Default settings for Federated Directory Server with SCIM as target

Table 6. Default settings for Federated Directory Server with SCIM as target	
Description	**Default setting**
Login URL	https://[host_name]:2098/fds
Login user name	admin
Login password	admin
Path to key database file	/userdata/directory/Certificates/ FDS_SCIMTarget_Default_SSLCerts
Keystore password	administrator
Server port	2099
Web server port	2098
Derby port	2527
Active MQ port	61617

Default settings for SCIM service

Table 7. Default settings for SCIM service	
Description	**Default setting**
Path to key database file	/userdata/directory/Certificates/ SCIMService_Default_SSLCerts
Keystore password	administrator
Server port	3099
Derby port	3527
Active MQ port	61618

Supported locales

The locales supported by IBM Security Directory Suite, Version 8.0.1.x components are listed here.

Table 8. Supported locales			
Language	**Web Administration Tool**	**Virtual appliance**	**Command-line interface**
Brazilian Portuguese	Yes	Yes	Yes
Czech	Yes	Yes	No
Dutch	Yes	No	No
French	Yes	Yes	Yes
German	Yes	Yes	Yes
Hungarian	Yes	Yes	No
Italian	Yes	Yes	Yes
Japanese	Yes	Yes	Yes
Korean	Yes	Yes	Yes
Polish	Yes	Yes	No
Russian	Yes	Yes	Yes
Simplified Chinese	Yes	Yes	Yes
Slovakian	Yes	No	No
Spanish	Yes	Yes	Yes
Traditional Chinese	Yes	Yes	Yes

To change the locale for virtual appliance console, take one of the following actions:

- Before you log into the virtual appliance console, click **Language** on the top right side of the page and select the required language.
- After you log into the virtual appliance console, click **Language** on the banner area and select the required language.

To change the locale for the virtual appliance command-line interface, take one of the following actions:

- If you are changing the language for the first time, you must create an environment variable for language and specify its value. By default, after installation, there is no environment variable available for language. Run the following command from the virtual appliance command-line interface:

```
idsenvvars -a LANG -v lang_code
```

- If you want to change the language again, you can update the value of the environment variable LANG. Run the following command:

```
idsenvvars -m LANG -v lang_code
```

Substitute *lang_code* with the appropriate code for your language from the following list:

fr_FR.utf8
de_DE.utf8
es_ES.utf8
ru_RU.utf8
it_IT.utf8
pt_BR.utf8
ja_JP.utf8
ko_KR.utf8

zh_CN.utf8
zh_TW.utf8

Chapter 3. DB2 installation and configuration

The IBM Security Directory Suite ISO installation package provides a virtual appliance with a ready-to-use Directory Server instance and a default DB2® database that is already created. However, if you want to configure the Directory Server instance in virtual appliance with a remote DB2 database, you can install DB2.

Related information

Remote DB2 with virtual appliance limitations and issues

Installing a new remote DB2 database with Directory Server for virtual appliance

You can install a DB2 database on a system other than the virtual appliance machine and configure the Directory Server instance in virtual appliance to use this remote DB2 database.

About this task

For more information about DB2 prerequisites and DB2 installation, see the DB2 product documentation at the IBM Knowledge Center for DB2.

Procedure

1. Use the part number that is provided in the IBM Security Directory Suite, Version 8.0.1.x - Download Document to download the DB2 installation package from IBM Passport Advantage website.
2. Install DB2 on a remote system.
   - For IBM DB2 10.5, go to https://www.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.qb.server.doc/doc/c0008711.html
   - For IBM DB2 11.1, go to https://www.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.qb.server.doc/doc/c0008711.html

   Note: For DB2 installations, consider the following notes:

   - When you install the full DB2 product by using the latest fix packs that you download from IBM Fix Central, either use **db2_install** or **db2setup** to install the SERVER component of the DB2 product.
   - After you install DB2 Enterprise Edition, you must apply the DB2 licenses manually to start using the product features.
3. Download the part number for IBM DB2 Enterprise Server Edition - Restricted Use - Quick Start and Activation 10.5.0.3 for Linux, UNIX and Windows from Passport Advantage for license activation.

   Note: Starting fromIBM Security Directory Suite 8.0.1, Fix Pack 12, IBM DB2 11.1.4.4 or later is supported. For license activation, download the following activation parts from Passport Advantage:

   - ESE: DB25ML - `DB2_ESE_Restricated_Activation_11.1.zip`
   - HC: CNB26ML - `DB_OHC_Restricted_Activation_11.1.zip`
4. Extract the contents of the package.
5. Apply the DB2 ESE Activation license (Key). Run the following command:

   Windows system:

   ```
   db2install_path\bin\db2licm -a extracted_dir\ese_o\db2\license\db2ese_o.lic
   ```

   Linux or UNIX systems:

   ```
   INSTHOME/sqllib/adm/db2licm -a extracted_dir/ese_o/db2/license/db2ese_o.lic
   ```

Note: For IBM DB2 11.1, you must extract and apply the **DB2 11.1 ESE Activation Key** followed by the **DB 11.1 HC Activation Key** that is provided with IBM Security Directory Suite, Version 8.0.1.x. Run the following commands to apply the HC activation key:

Windows system

```
db2install_path\bin\db2licm -a extracted_dir\hc\db2\license\db2hc.lic
```

Linux or UNIX systems

```
INSTHOME/sqllib/adm/db2licm -a extracted_dir/hc/db2/license/db2hc.lic
```

What to do next

To configure the remote DB2 with Directory Server in virtual appliance, follow the steps in the topic, "Configuration of a remote DB2 database for the virtual appliance" on page 18.

Related information

Remote DB2 with virtual appliance limitations and issues

Configuration of a remote DB2 database for the virtual appliance

The IBM Security Directory Suite, Version 8.0.1.x virtual appliance comes with a pre-configured DB2 instance with an embedded DB2 database. You can also configure the existing directory server instance to use an external or remote DB2 database instance on another system.

This feature is primarily intended for following users:

- Users who have an existing server.
- Users who require fine grained control over their DB2 instance for performance tuning and compliance.
- Users who require High Availability or monitoring.
- Users who are anticipating a high volume of transactions or data with highly scalable disk space requirements.

A remote database can be configured on top of an existing embedded database in which case the information in the embedded database is retained. However, the remote database cannot be configured for the following scenarios:

- The remote database cannot be configured in combination with any of these options: **`-c -collate -k -m -s -x -z`**.
- A remote database cannot be configured on top of an existing embedded database if an existing change log is configured. As the Directory Server is configured to a remote database, the change log must also be remote.
- A remote database cannot be configured on top of an existing remote database configuration. If the remote database is configured to communicate over SSL, the change log (if configured) will also automatically communicate over SSL.
- Multiple virtual appliance Directory Servers cannot be configured to the same remote DB2 instance at the same time. The configuration is only allowed if the virtual appliance UUID matches the one in the remote DB2 or UUID does not exist in the remote DB2. To configure another virtual appliance Directory Server with any preconfigured remote DB2, you must first use idsucfgdb command to unconfigure the remote DB2 from that Directory Server. Alternatively, you can use the `-F` flag to override the UUID check and force its rewrite. Then, reconfigure the remote DB2 with another virtual appliance Directory Server by completing the steps in the following procedure.

Follow the sequence in this roadmap. If you want to update the IBM Security Directory Suite, Version 8.0.1.x to use SSL communications with a previously configured remote DB2 database, see "Updating the IBM Security Directory Suite, Version 8.0.1.x virtual appliance configuration to use SSL communications with a previously configured remote DB2 database" on page 30.

Table 9. Roadmap for configuration of a remote DB2 database	
Task	**Instructions**
Configure the remote DB2 database.	See "Configuring the remote DB2 database for the virtual appliance" on page 19.
Update the DB@ server-side configuration for SSL communication.	See "Updating DB2 server-side configuration for SSL on a remote system" on page 24.
Update the remote database management configuration.	See "Updating the remote database management configuration (DBM CFG)" on page 28.
Load the certificates into the virtual appliance.	"Loading the certificates into the virtual appliance" on page 29
Configure the virtual appliance to use SSL communications with the remote DB2 database.	"Configuring the IBM Security Directory Suite, Version 8.0.1.x virtual appliance to use SSL communications with the remote DB2 database" on page 30

Configuring the remote DB2 database for the virtual appliance

Use these instructions to configure the existing server instance to use an external or remote DB2 database instance on another system.

Before you begin

- Ensure that the service port that is to be used by DB2 is not in use by another service before you use the **idscfgremotedb** script.
- The network connectivity between the Directory Server and the remote server can impact performance. It is suggested that the remote server must be in the same geographical area and subnet as the Directory appliance.

Procedure

1. Log on to the IBM Security Directory Suite virtual appliance local management interface (LMI) web interface as an admin user. See Logging on to the virtual appliance console.
2. From the top-level menu of the virtual appliance console, select **Configure Directory Suite** > **Advanced Configuration** > **Custom File Management**.
3. In the **All Files** tab, click the `idstools` folder.
4. Select the `idscfgremotedb.zip` file that is displayed in the right pane of the table.
5. Click **Download** to save the file.
6. Do one of these actions.
   - Transfer the file to a remote DB2 server system on AIX, Linux, Solaris, or Windows operating systems.
   - Download the compressed file from the IBM Security Directory Suite, Version 8.0.1.x virtual appliance directly to a remote DB2 server system by running the command on the remote DB2 server system:

     ```
     curl -u admin:password -k -O
     https://sds801va1_hostname_or_IPaddress/custfile_mgmt/download?idstools/
     idscfgremotedb.zip
     ```
7. Log on to the remote DB2 server system as a root user or as an administrator.
8. Extract the contents of the `idscfgremotedb.zip` file.

On Window systems use Windows Explorer to extract the files. If the **zip** command is available on UNIX systems, run the command:

```
unzip idscfgremotedb.zip
```

If the **zip** command is not available, on UNIX systems run the command:

```
jar -xvf idscfgremotedb.zip
```

Two files are extracted, `idscfgremotedb` for AIX, Linux and Solaris systems, and `idscfgremotedb.cmd` for Windows systems.

9. Create a group and a user on the remote DB2 server system.

   Note: In this step `dbsysadmin` is the group and `db2inst1` is the user name. You can substitute different group and user names.

   For UNIX systems, perform these steps based on your system.

   a) Create a group called `dbsysadm` and make the root user a member of the group.

      For UNIX systems, perform these steps.

      AIX systems

      ```
      mkgroup "users=root" dbsysadm
      ```

      Linux and Solaris systems

      ```
      groupadd dbsysadm
      usermod -G root,dbsysadm root
      ```

   b) Create an instance user `db2inst1`.

      Run this command.

      ```
      useradd -d /home/db2inst1 -g dbsysadm -G dbsysadm -m
            -s /usr/bin/ksh db2inst1
      ```

   c) Verify the user.

      AIX systems

      ```
      lsuser db2inst1
      ```

      ```
      Output:
      db2inst1 id=1782 pgrp=dbsysadm groups=dbsysadm home=/home/db2inst1
      shell=/usr/bin/ksh login=true...
      ```

      Linux and Solaris systems

      ```
      id db2inst1
      ```

      ```
      Output:
      uid=1001(db2inst1) gid=1001(dbsysadm) groups=1001(dbsysadm)
      ```

   d) Set the password for `db2inst1`.

      AIX systems

      ```
      passwd db2inst1
      pwdadm -c db2inst1
      ```

      Linux and Solaris systems

      ```
      passwd db2inst1
      ```

   For Windows systems, perform these steps.

   a) Click **Computer Management** > **Local Users and Groups** > **Users** > **More Actions** > **New User**.

b) Type db2inst1 as the user name.

c) Type and confirm the user password.

d) Clear the **User must change password at next logon** check box.

e) Click **Create**.

f) Right-click the user db2inst1 and select **properties**.

g) Click **Member Of**.

h) Click **Add**.

Add the user to the two groups Administrators and DB2ADMNS.

i) Type Administrators and click **OK**.

ii) Type DB2ADMNS and click **OK**.

i) Click **OK**.

10. Create the instance and database in the instance's home directory with the **idscfgremotedb** utility.

AIX and Solaris systems

```
./idscfgremotedb -c -u db2inst1 -w passwd -p /opt/IBM/db2/V10.5
    -s 6512 -t ldapdb -l /home/db2inst1
```

Linux systems

```
./idscfgremotedb -c -u db2inst1 -w passwd -p /opt/ibm/db2/V10.5
    -s 6512 -t ldapdb -l /home/db2inst1
```

Windows systems

```
C:\temp\idscfgremotedb> idscfgremotedb.cmd -c -u db2inst1 -w passwd
-l c: -p C:\PROGRA~1\IBM\SQLLIB -s 6512 -t sdsdb
```

For information about the command options, see idscfgremotedb.

Note:

- You can also use an existing instance that is used by any existing Directory Server.
- The **idscfgremotedb** script requires an existing user on the remote server with a valid password and proper authority. The path that is specified by the -p db2_path must exist and contain a preinstalled DB2.

11. Update the default encryption keys to create seed and salt values.

If you are going to import data from another IBM Security Directory Suite version 8.0.* or Tivoli Directory Server 6.* instance, you must keep the same seed and salt values on the new IBM Security Directory Suite, Version 8.0.1.x virtual appliance directory server instance.

a) Log in to the IBM Security Directory Suite, Version 8.0.1.x command line interface by using **ssh** or **putty**.

b) Run the **idsgendirksf** command to update the ibmslapddir.ksf file in the instance's etc folder, /*home*/sdsinst1/idsslapd-sdsinst1/etc/, and in the CustomOut folder.

Replace *encrypt_seed* and *encrypt_salt* with the values of your source directory server system.

```
sds801va1> sds server_tools idsgendirksf -e encrypt_seed -s encrypt_salt
-l ibmslapddir.ksf -n
```

12. Configure the Directory Server instance in the appliance to use the remote instead of the pre-configured embedded by using the **idscfgdb** command.

Run the **idscfgdb** command to configure the IBM Security Directory Suite, Version 8.0.1.x virtual appliance instance to connect with the remote DB2 database. For more information about the command options, see idschfdb.

```
idscfgdb –I instance_name –a instance_user_id –t db_alias –w instance_user_pwd
–Y -S port –l location –P remote_DB2_hostname_or_IPaddress
–u remote_username –p remote_pwd
```

For example,

```
sds801va1> sds server_tools idscfgdb -I sdsinst1 -a sdsinst1 -t ldapdb -w sdsinst1
      -Y -S 6512 -l /home/db2inst1 -P remote_DB2_hostname_or_IPaddress -u db2inst1
      -p passwd -n
```

Note:

- The **idscfgdb** command does not unconfigure or drop the existing embedded database instance. Existing data is not lost.
- Ensure that only a single Directory appliance is configured with any specified instance, which is not ensured by the **idscfgdb** command. Multiple applications or Directory appliances that are using the same remote DB2 instance can result in an application failure or data loss and is not a supported configuration.

13. Create and configure a change log database on the remote DB2.

Note:

- If you create the changelog database without creating the actual database on a remote DB2 server, the script creates a changelog database with a 'SERVER' authentication type.

  However, if you create the changelog database after you create the actual database on a remote DB2 server, the script derives the authentication type of the actual database (for example, either '**SERVER**' or '**SERVER_ENCRYPT**')
- The change log database must be created inside an existing instance, on a remote system. This instance is the same as the instance to which the appliance instance is configured for remote communication.
- The change log database is created on the remote by using the same script that is used to create the remote instance.

a) Run one of the following commands on the remote DB2 server system based on your system.

AIX and Solaris systems

```
./idscfgremotedb -c -u db2inst1 -w passwd -p /opt/IBM/db2/V10.5
    -s 6512 -t ldapclog
```

Linux systems

```
./idscfgremotedb -c -u db2inst1 -w passwd -p /opt/ibm/db2/V10.5
    -s 6512 -t ldapclog
```

Windows systems

You must run this command as an administrator.

```
C:\temp\idscfgremotedb> idscfgremotedb.cmd -c -u db2inst1 -w passwd
    -l c: -p C:\PROGRA~1\IBM\SQLLIB -s 6512 -t ldapclog
```

For information about the command options, see idscfgremotedb.

b) Verify that you successfully created a change log database in the remote instance.

```
su - db2inst1
    [db2inst1@islrppcxv44 ~]$ db2 connect to db2inst1 user db2inst1 using inst123
    [db2inst1@islrppcxv44 ~]$ db2 list db directory

 System Database Directory

 Number of entries in the directory = 2
```

```
Database 1 entry:

 Database alias = db2inst1
 Database name = db2inst1
 Local database directory = /home/db2inst1
 Database release level = 10.00
 Comment =
 Directory entry type = Indirect
 Catalog database partition number = 0
 Alternate server hostname =
 Alternate server port number =

Database 2 entry:

 Database alias = LDAPCLOG
 Database name = LDAPCLOG
 Local database directory = /home/db2inst1
 Database release level = 10.00
 Comment =
 Directory entry type = Indirect
 Catalog database partition number = 0
 Alternate server hostname =
 Alternate server port number =
```

14. Run the **idscfgchglg** command on the IBM Security Directory Suite, Version 8.0.1.x virtual appliance command line interface to configure the virtual appliance directory instance to connect with the remote change log database.

```
sds801va1> sds server_tools idscfgchglg -I sdsinst1 -Y -n
    [-m max_entries] [-y max_days] [-h max_hours]
```

Note: When a remote database is configured to the directory server instance, you can configure only a remote change log. The remote change log database must be created in the same instance that is configured to the directory server instance.

The **idscfgchglg** command gets the authentication type from the IBM Security Directory Suite virtual appliance instance configuration. For example, either 'SERVER' or 'SERVER_ENCRYPT'.

You must complete the following tasks to configure the appliance instance to remote over SSL and to configure the change log:

- Create both databases. That is, create a remote instance and the change log database inside an existing instance before you configure the remote instance for SSL.
- After you create both databases, you can proceed with the SSL configuration on the remote instance.

The sequence of the previous steps is important. If SSL is configured before you configure the change log database, then the script overrides the SSL settings of the remote DB2 instance.

Reconfiguring an IBM Security Directory Server instance on a virtual appliance with a configured remote Db2® database to update the authentication type

If you choose to change the authentication type of the remote db2 instance that is running on a remote DB2 server, you can change the authentication type of the IBM Security Directory Server instance. You change the authentication type of an instance that is already configured with a remote Db2 database.

Procedure

1. Log in as an administrator to the virtual appliance command line interface(CLI) by using ssh.
2. Stop the directory server.

```
sds801va1> sds server_tools ibmslapd -k
```

3. Use the **idscfgdb** command to update the authentication type of the virtual appliance instance.

```
sds801va1> sds server_tools idscfgdb -l sdsinst1 -Z authentication_type -P
remote_DB2_hostname_or_IPaddress -S port -Y
```

Note:

- If the remote change log is also configured on the virtual appliance, the authentication type of the change log is also updated.
- If IBM Security Directory Server instance is already configured with a remote DB2 database over SSL, then to update authentication type of VA instance, use **idscfgdb** command with the **-Z <auth_type>** and **-L options**. For example:

```
sds801va1> sds server_tools idscfgdb -l sdsinst1 -Z authentication_type -P
remote_DB2_hostname_or_IPaddress -S port -Y -L
```

- Other SSL options, such as **-B** and **-H** are not required to re-configure authentication type. If specified, the parameters are ignored.
- If you change the authentication type of DB2 instance on a remote DB2 server from **SERVER** to **SERVER_ENCRYPT**, but you reconfigure the instance by using **idscfgdb** with the wrong authentication type of **SERVER**, the command will succeed. However, the directory server will fail to start and display the following error:

  ```
  VAUUID check on the remote database failed.
  ```

4. Start the directory server.

```
sds801va1> sds server_tools ibmslapd -n
```

Updating DB2 server-side configuration for SSL on a remote system

Complete the following tasks to configure the appliance instance to use SSL communications with a remote DB2 database and to configure the change log.

About this task

Table 10. Db2 SSL configuration parameters

Parameter	Description	Comments
ssl_svr_keydb	The SSL key file path for DB2 server (for incoming SSL connections).	The fully qualified path and name of the kdb file. For example, /*home*/db2inst1/sqllib/security/cacert_server/mydbserver.kdb
ssl_svr_stash	The SSL key stash file path for DB2 server.	The fully qualified path and name of the stash file. For example, /*home*/db2inst1/sqllib/security/cacert_server/mydbserver.sth.
ssl_svr_label	The personal certificate label in key file.	The name of the personal certificate, or if the value is null, the default certificate is used.

Table 10. Db2 SSL configuration parameters (continued)		
Parameter	**Description**	**Comments**
ssl_svcename	The SSL service name.	The name or port that DB2 server uses to await communications from remote client nodes that use SSL protocol. The name is defined in the `/etc/services` directory with a dedicated unused port number.
ssl_versions	The supported SSL versions.	Specifies the secure sockets layer (SSL) and transport layer security (TLS) versions: TLSv12 and TLSv1. When both TLSv12 and TLSv1 are set, TLS v1.2 is enabled with an option to fall back on TLS v1.1 or TLS v1.0.
ssl_cipherspecs	The supported cipher specifications at the server.	None.
ssl_clnt_keydb	The SSL key file path for DB2 client (for outbound SSL connections).	The fully qualified path and name of the `.kdb` file. For example,`/userdata/directory/Certificates/`*`mydbclient`*`.kdb`.
ssl_clnt_stash	The SSL stash file path for the DB2 client.	The fully qualified path and name of the stash file. For example, `/userdata/directory/Certificates/`*`mydbclient`*`.sth`.

Procedure

1. Log on to the remote DB2 system to find the current DB@ instance's SSL server port.

   UNIX systems

   ```
   grep db2inst1svc /etc/services
   ```

   Sample return.

   ```
   db2inst1svc        6512/tcp
   ```

   Windows systems

   Open a DB2 command window as an administrator.

   ```
   C:\> C:\Progra~1\IBM\SQLLIB\BIN\db2cwadmin.bat
   C:\> findstr db2inst1svc C:\Windows\System32\drivers\etc\services
   ```

   Sample return.

   ```
   db2inst1svc        6512/tcp
   ```

2. Find and add or assign an unused port for as the DB2 instance SSL service port.

   UNIX systems

   ```
   ==> grep -i 6516 /etc/services  # No results expected.
   ==> echo "db2inst1svcssl    6516/tcp" >> /etc/services
   ==> grep db2inst1svc /etc/serviceses
   ```

Sample return.

```
db2inst1svc        6512/tcp
db2inst1svcssl     6516/tcp
```

Windows systems

```
C:\> findstr 6516 C:\Windows\System32\drivers\etc\services
C:\> echo db2inst1svcssl     6516/tcp >>
C:\Windows\System32\drivers\etc\services
C:\> findstr db2inst1svc C:\Windows\System32\drivers\etc\services
```

Sample return.

```
db2inst1svc        6512/tcp
db2inst1svcssl     6516/tcp
```

3. Create a key database (kdb) file with either self-signed or certificate authority (CA)-signed certificates.

- Self-signed certificates

  Create a folder to hold the key databases and the extracted certificate files.

  a. Create the folder based on your system.

  UNIX systems

  ```
  # su - db2inst1
  $ mkdir ~/sqllib/security/keystore; cd ~/sqllib/security/keystore
  ```

  Windows systems

  ```
  C:\PROGRA~1\IBM\SQLLIB\security> mkdir keystore
  C:\PROGRA~1\IBM\SQLLIB\security> cd keystore
  ```

  b. Create a key database with a self-signed certificate for the DB2 server.

  ```
  $ gsk8capicmd_64 -keydb -create -db mydbserver.kdb -pw passwd -stash
  ```

  c. Create a self-signed certificate.

  ```
  $ gsk8capicmd_64 -cert -create -db mydbserver.kdb -pw passwd
                   -label myselfsigned -dn "cn=dbserverhostname"
                   -size 2048 -default_cert yes -sig_alg SHA256WithRSA
  ```

  d. Extract the server certificate.

  ```
  $ gsk8capicmd_64 -cert -extract -db mydbserver.kdb -pw passwd
                   -label myselfsigned -target mydbserver.arm -format ascii
  ```

  e. Create key database for the DB2 client, the IBM Security Directory Suite, Version 8.0.1.x virtual appliance.

  ```
  $ gsk8capicmd_64 -keydb -create -db mydbclient.kdb -pw passwd -stash
  ```

  f. Add the extracted server certificate into the client key database.

  ```
  $ gsk8capicmd_64 -cert -add -db mydbclient.kdb -pw passwd
                   -label myselfsigned -file mydbserver.arm -format ascii
  ```

- CA-signed certificates

  Create a folder to hold the key databases and the extracted certificate files.

  a. Create the folder based on your system.

  UNIX systems

  ```
  # su - db2inst1
  $ mkdir ~/sqllib/security/cacert_server; cd ~/sqllib/security/cacert_server
  ```

Windows systems

```
C:\PROGRA~1\IBM\SQLLIB\security> mkdir cacert_server
C:\PROGRA~1\IBM\SQLLIB\security> cd cacert_server
```

b. Create key database for the DB2 server.

```
$ gsk8capicmd_64 -keydb -create -db mydbserver.kdb -pw passwd -stash
```

c. Create a certificate signing request (CSR) for the DB2 server.

```
$ gsk8capicmd_64 -certreq -create -db mydbserver.kdb -stashed
     -label "mydbservercert" -dn "cn=mydbserver,ou=divisiona,o=acompany"
     -file mydbservercertreq.arm -sigalg SHA256WithRSA
```

d. Transfer the certificate signing request (CSR) `mydbservercertreq.arm` file to the CA system and get it signed by a CA.

e. Download signed certificate, the root certificate, and any intermediate signer certificates.

f. Add the root signer certificate to the DB2 server key database.

```
$ gsk8capicmd_64 -cert -add -db mydbserver.kdb -stashed
      -label "Root CA cert" -file rootca.arm -format ascii -trust enable
```

g. Add any intermediate signer certificates to the DB2 server key database.

```
$ gsk8capicmd_64 -cert -add -db mydbserver.kdb -stashed
      -label "Intermediate CA cert" -file interca.arm -format ascii
      -trust enable
```

h. Receive the signed DB2 server certificate.

```
$ gsk8capicmd_64 -cert -receive -db mydbserver.kdb -stashed
                 -file mydbservercert.arm -default_cert yes
```

i. Create a folder to hold the key databases and extracted certificate files.

Create the folder based on your system.

– For UNIX systems

```
$ mkdir ~/sqllib/security/cacert_client; cd ~/sqllib/security/cacert_client
```

– For Windows systems

```
C:\PROGRA~1\IBM\SQLLIB\security> mkdir cacert_client
C:\PROGRA~1\IBM\SQLLIB\security> cd cacert_client
```

j. Create a key database for the DB2 client.

```
$ gsk8capicmd_64 -keydb -create -db mydbclient.kdb -pw passwd -stash
```

k. Create a certificate signing request (CSR) for the DB2 client.

```
$ gsk8capicmd_64 -certreq -create -db mydbclient.kdb -stashed
     -label "mydbclientcert" -dn "cn=mydbclient,ou=divisiona,o=acompany"
     -file mydbclientcertreq.arm -sigalg SHA256WithRSA
```

l. Transfer the CSR *mydbclientcertreq*`.arm` file to the CA system and get it signed by a CA.

m. Download signed certificate and also download the Root and any intermediate signer certificates.

n. Add the certificates to the DB2 client key database.

o. Add the root signer certificate to the DB2 client key database.

```
$ gsk8capicmd_64 -cert -add -db mydbclient.kdb -stashed
      -label "Root CA cert" -file rootca.arm -format ascii -trust enable
```

p. Add any intermediate signer certificates to the DB2 client key database.

```
$ gsk8capicmd_64 -cert -add -db mydbclient.kdb -stashed
      -label "Intermediate CA cert" -file interca.arm -format ascii
      -trust enable
```

q. Receive the signed DB2 client certificate.

```
$ gsk8capicmd_64 -cert -receive -db mydbclient.kdb -stashed
                 -file mydbclientcert.arm -default_cert yes
```

Updating the remote database management configuration (DBM CFG)

To use SSL with the remote database, you must configure several parameters on the remote DB2 server system.

About this task

Procedure

1. Access the DB2 instance.

   Based on your system, do one of the following actions:

   UNIX systems

   Log in to the DB2 instance or use the **su** command.

   ```
   su - db2inst1
   ```

   Windows systems

   On the remote DB2 server system at the administrator DB2 command line, run the following command.

   ```
   C:\> set db2instance=db2inst1
   ```

2. Update the DBM CFG configuration SSL key file path parameter for the DB2 server.

   Run the following command for the **ssl_svr_keydb** parameter.

   ```
   $ db2 update dbm cfg using ssl_svr_keydb
              /home/db2inst1/sqllib/security/keystore/mydbserver.kdb
   ```

   Note: For CA-signed certificates, use the corresponding `.kdb` file with the full path.

   On Windows systems, use the file with the full path such as the following path.
   `C:\PROGRA~1\IBM\SQLLIB\security\keystore\mydbserver.kdb`

3. Update the DBM CFG configuration SSL stash file path parameter for the DB2 server.

   Run the following command for the **ssl_svr_stash** parameter.

   ```
   $ db2 update dbm cfg using ssl_svr_stash
              /home/db2inst1/sqllib/security/keystore/mydbserver.sth
   ```

   Note: For CA-signed certificates, use the corresponding `.sth` file with the full path.

   –On Windows systems use the file with the full path such as:
   `C:\PROGRA~1\IBM\SQLLIB\security\keystore\mydbserver.sth`

4. Update the DBM CFG configuration service name parameter for the DB2 server.

   Run the following command for the **ssl_svcename** parameter.

   ```
   $ db2 update dbm cfg using ssl_svcename db2inst1svcssl
   ```

5. Update the DBM CFG configuration supported SSL versions parameter for the DB2 server.

Run the following command for the **ssl_versions** parameter.

```
$ db2 update dbm cfg using ssl_versions "TLSV12,TLSV1"
```

6. Update the DB2 registry variable **DB2COMM** to uses SSL or to include SSL with TCPIP.

```
$ db2set -i db2inst1 DB2COMM=SSL
$ db2set -all | grep DB2COMM
```

Output

```
[i] DB2COMM=SSL
```

7. Restart DB2.

```
$ db2stop
$ db2start
```

8. Verify that the SSL port is listening.

```
 netstat -an | egrep "(Local|6516)"
```

Output

```
Proto Recv-Q Send-Q  Local Address  Foreign Address  (state)
tcp4       0      0  *.6516         *.*              LISTEN
```

What to do next

Configure the IBM Security Directory Suite, Version 8.0.1.x virtual appliance to use the remote database with SSL. See "Configuring the IBM Security Directory Suite, Version 8.0.1.x virtual appliance to use SSL communications with the remote DB2 database" on page 30. To update a previously configured IBM Security Directory Suite, Version 8.0.1.x virtual appliance to use SSL to communicate with the remote database, see "Updating the IBM Security Directory Suite, Version 8.0.1.x virtual appliance configuration to use SSL communications with a previously configured remote DB2 database" on page 30.

Loading the certificates into the virtual appliance

Use the local management interface to load the DB2 client-related key database file (`.kdb`) and the stash file (`.sth`) into the IBM Security Directory Suite, Version 8.0.1.x virtual appliance.

About this task

Procedure

1. Access the IBM Security Directory Suite, Version 8.0.1.x LMI with a browser.
   Use either the virtual appliance host name or IP address.

```
https://SDS801xva_hostname
https://SDS801xva_IPaddress
```

2. Log in as an administrator and enter the administrator password.
3. Click **Configure Directory Suite** > **Custom File Management**.
4. Click **Certificates** on the **All Files** tab.
5. Click **Upload**.
6. Click **Browse** to locate and select the `.kdb` file.
7. Click **Save Configuration** to complete the upload process.
8. Repeat the process to upload the `.sth` file.

Configuring the IBM Security Directory Suite, Version 8.0.1.x virtual appliance to use SSL communications with the remote DB2 database

Use this task if you are using a newly configured IBM Security Directory Suite, Version 8.0.1.x virtual appliance that is configured to use the default local embedded database.

Before you begin

The DB2 client-side `.kdb` and `.sth` files must be created and uploaded to the IBM Security Directory Suite, Version 8.0.1.x virtual appliance.

Procedure

1. Log in to the virtual appliance command line interface (CLI) by using **ssh** or **putty**.
2. Use the idscfgdb utility to configure the IBM Security Directory Suite, Version 8.0.1.x to use the remote database with SSL.

```
sds801va1> sds server_tools idscfgdb -I sdsinst1 -a sdsinst1
           -t ldapdb -w sdsinst1 -Y -S 6516 -l /home/sdsinst1
           -P remote_db2_server_hostname_or_IPaddress -u db2inst1 -p passwd
           -L -B mydbclient.kdb -H mydbclient.sth -n
```

   The following parameters are the SSL parameters in the preceding command.

   -L
   Set up SSL communication with the remote database.

   -B
   The name of the `.kdb` file that you previously uploaded to the **Certificates** folder.

   -H
   The name of the `.sth` file that you previously uploaded to the **Certificates** folder.

   Note: Provide file names that are in **Certificates** folder without any path as shown in the command.
3. Start the Directory Server.

```
sds801va1> sds server_tools ibmslapd -n
```

   Note: If remote database configuration on the virtual appliance fails, reconfigure the local database and try configuring remote database again.

Updating the IBM Security Directory Suite, Version 8.0.1.x virtual appliance configuration to use SSL communications with a previously configured remote DB2 database

Use this task to change to SSL communications if you have an IBM Security Directory Suite, Version 8.0.1.x virtual appliance that is configured to use TCPIP to communicate to a remote database.

About this task

Procedure

1. Log in as an administrator to the virtual appliance command line interface (CLI) by using **ssh** or **putty**.
2. Stop the directory server.

```
sds801va1> sds server_tools ibmslapd -k
```

3. Use the **idsucfgdb** to unconfigure the remote database.

```
sds801va1> sds server_tools idsucfgdb -I sdsinst1 -Y -n
```

Note: These options leave the data in database intact. For more information about the option, see idsucfgdb.

4. Perform the following tasks on the remote DB2 server system.
   a. “Updating DB2 server-side configuration for SSL on a remote system” on page 24
   b. “Loading the certificates into the virtual appliance” on page 29
   c. “Updating the remote database management configuration (DBM CFG)” on page 28
5. Log in to the virtual appliance command line interface (CLI) by using **ssh** or **putty**.
6. Use the **idscfgdb** utility to configure the IBM Security Directory Suite, Version 8.0.1.x to use the remote database with SSL.

```
sds801va1> sds server_tools idscfgdb -I sdsinst1 -a sdsinst1
           -t ldapdb -w sdsinst1 -Y -S 6516 -l /home/sdsinst1
           -P remote_db2_server_hostname_or_IPaddress -u db2inst1 -p passwd
           -L -B mydbclient.kdb -H mydbclient.sth -n
```

   The following parameters are the SSL parameters in the preceding command.

   -L
   Set up SSL communication with the remote database.

   -B
   The name of the `.kdb` file that you previously uploaded to the **Certificates** folder.

   -H
   The name of the `.sth` file that you previously uploaded to the **Certificates** folder.

   Note: Provide file names that are in **Certificates** folder without any path as shown in the command.
7. Start the Directory Server.

```
sds801va1> sds server_tools ibmslapd -n
```

Note: If remote database configuration on the virtual appliance fails, reconfigure the local database and try configuring remote database again.

Unconfiguring and reconfiguring the remote database

If remote database configuration on the virtual appliance fails, reconfigure the local database and try configuring remote database again.

About this task

Procedure

1. Use **idsucfgdb** to unconfigure the IBM Security Directory Suite, Version 8.0.1.x virtual appliance directory instance remote database.

```
sds801va1> sds server_tools idsucfgdb -I sdsinst1 -Y -n
```

2. Use **idsucfgdb** to unconfigure and reconfigure the IBM Security Directory Suite, Version 8.0.1.x virtual appliance directory local or embedded DB2 database.

   This step cleans up and deletes the local or embedded database and creates a new blank database.

```
sds801va1> sds server_tools idsucfgdb -I sdsinst1 -r -n
sds801va1> sds server_tools idscfgdb -I sdsinst1 -a sdsinst1 -w sdsinst1 -t sdsinst1
    -l /home/sdsinst1 -n
```

3. Use **idsucfgchglg** to unconfigure the IBM Security Directory Suite, Version 8.0.1.x virtual appliance directory instance remote change log database.

```
sds801va1> sds server_tools idsucfgchglg -I sdsinst1 -Y -n
```

4. Use **idsucfgchglg** to unconfigure and reconfigure the IBM Security Directory Suite, Version 8.0.1.x virtual appliance directory local or embedded change log database.

```
sds801va1> sds server_tools idsucfgchglg -I sdsinst1 -n
sds801va1> sds server_tools idscfgchglg -I sdsinst1 -n
  [-m max_entries] [-y max_days] [-h max_hours]
```

Configuration of the virtual appliance to use an existing remote DB2 instance

You can configure virtual appliance to use an existing remote DB2 that is used by a Directory Server 6.4 instance on software stack.

This task replaces the need to export and import data when you move to the virtual appliance. You must migrate the Security Directory Server version 6.4 configuration and schema to the IBM Security Directory Suite, Version 8.0.1.x virtual appliance. Then, you must reconfigure IBM Security Directory Suite, Version 8.0.1.x to use a remote DB2 database.

Follow the sequence in this roadmap.

Table 11. Roadmap for configuration of an existing remote DB2 database

Task	Instructions
Back up your data.	See “Backing up your configuration and schema data” on page 32.
Migrate the Directory Server 6.4 information to the virtual appliance.	See “Migrating the Directory Server from version 6.4 to the IBM Security Directory Suite, Version 8.0.1.x virtual appliance” on page 33.
Unconfigure Directory Server 6.4.	See “Unconfiguring Directory Server version 6.4 and retain the DB2 instance and database. ” on page 34.
Configure the virtual appliance to use the remote DB2 database.	“Configuring the virtual appliance to connect to the remote DB2 database” on page 35

Backing up your configuration and schema data

You must back up your configuration and schema data before you can configure virtual appliance to use an existing remote DB2 that is used by a Directory Server instance on software stack.

Before you begin

Ensure that the Directory Server instance on software stack is stopped before proceeding.

Procedure

Back up your configuration, schema, and any custom schema files.

As a root user or administrator, do one of the following tasks based on your system.

AIX and Solaris systems

```
==> mkdir /home/ldapdb2/ldapsaveconf
==> chmod g+w /home/ldapdb2/ldapsaveconf
==> chown ldapdb2:idsldap /home/ldapdb2/ldapsaveconf
==> cd /opt/IBM/ldap/V6.4/sbin
==> ./migbkup /home/ldapdb2/idsslapd-ldapdb2 /home/ldapdb2/ldapsaveconf
==> cp /home/ldapdb2/idsslapd-ldapdb2/etc/<customschemafiles>
       /home/ldapdb2/ldapsaveconf/etc
==> cd /home/ldapdb2; tar -cvf ldapsaveconf.tar ldapsaveconf
```

Linux systems

```
==> mkdir /home/ldapdb2/ldapsaveconf
==> chmod g+w /home/ldapdb2/ldapsaveconf
==> chown ldapdb2:idsldap /home/ldapdb2/ldapsaveconf
==> cd /opt/ibm/ldap/V6.4/sbin
==> ./migbkup /home/ldapdb2/idsslapd-ldapdb2 /home/ldapdb2/ldapsaveconf
==> cp /home/ldapdb2/idsslapd-ldapdb2/etc/<customschemafiles>
       /home/ldapdb2/ldapsaveconf/etc
==> cd /home/ldapdb2; tar -cvf ldapsaveconf.tar ldapsaveconf
```

Windows systems

```
==> mkdir C:\ldapsaveconf
==> cd "\Program Files\IBM\ldap\V6.4\sbin"
==> .\migbkup.bat c:\idsslapd-sdstst1 c:\ldapsaveconf
==> cp C:\idsslapd-ldapdb2\etc\<customschemafiles> C:\ldapsaveconf\etc
```

Create a compressed file.

a. Go to Windows Explorer.

b. Click **C:** and locate the `ldapsaveconf` folder.

c. Right-click the `ldapsaveconf` folder.

d. Click **Send to** > **Compressed (zipped) folder**

Migrating the Directory Server from version 6.4 to the IBM Security Directory Suite, Version 8.0.1.x virtual appliance

After you back up your data, you must load the data into the virtual appliance.

About this task

When you log on to the virtual appliance and run the **`idsimigr`** utility, the system performs the following tasks automatically.

- Removes the existing directory server instance, DB2 instance, and the DB2 database.
- Creates a directory server instance and migrates the configuration, encryption seed, encryption salt, and schema from the version 6.4 compressed file.
- Creates a DB2 instance.

Procedure

1. Migrate Directory Server 6.4 data to the IBM Security Directory Suite, Version 8.0.1.x virtual appliance.

   Use one of the following methods.

   For Windows or UNIX systems, migrate by using the virtual appliance local management interface (LMI).

   a. Transfer the `ldapsaveconf.tar` or `ldapsaveconf.zip` file that you created in the `/home/ldapdb2` folder on the Directory Server 6.4 system to a system where you can connect the virtual appliance LMI.

   b. Log on to the LMI.

   c. Click **Configure Directory Suite** > **Advanced Configuration** > **Custome File Management**.

   d. Go to the **All Files** tab and click **CustomIn** > **Upload**.

   e. Select `ldapsaveconf.tar` and upload it to the virtual appliance.

   Alternatively for UNIX systems, upload by using the virtual appliance command line interface (CLI).

   a. Log in to the virtual appliance command line interface (CLI) as an administrator by using **`ssh`** or **`putty`**.

b. Use the **idsgetfile** command to download the `ldapsaveconf.tar` file directly onto virtual appliance from remote Directory Server 6.4 UNIX server.

```
sds801va1 > sds client_tools idsgetfile -h remote_6.4_server_hostname -u root
   -f /home/ldapdb2/ldapsaveconf.tar
```

2. Log in to the virtual appliance command line interface (CLI) as an administrator, if you are not already logged in, by using **ssh** or **putty** and run the **idsimigr** command.

```
sds801va1 > sds migration_tools idsimigr -u <ldapsaveconf.xxx>
```

Note: For the **-u** parameter, specify the `ldapsaveconf.tar` or `ldapsaveconf.zip` file that you uploaded without any path.

3. Run the **idscfgdb** utility to create a blank local database.

```
sds801va1 > sds server_tools idscfgdb -I sdsinst1 -a sdsinst1 -w sdsinst1 -t sdsinst1
              -l /home/sdsinst1 -n
```

Unconfiguring Directory Server version 6.4 and retain the DB2 instance and database.

About this task

Procedure

1. Log in to SDS 6.4 system as a root user.
2. Stop Directory Server and Admin Server processes.

```
==> ibmslapd -I ldapdb2 -k
==> ibmdiradm -I ldapdb2 -k
```

3. Use the **idsucfgb** utility to unconfigure the database from the directory server configuration without deleting the database.

```
==> idsucfgdb -I ldapdb2 -n
```

Note: Do not use the **-r** flag.

4. Use the **idsidrop** utility to delete the directory server instance without deleting the DB2 instance.

```
==> idsidrop -I ldapdb2 -n
```

5. Identify the DB2 instance name and the database name.
   a) Find the Db2 installation path.

```
==> /usr/local/bin/db2ls
```

   b) Find the DB2 instance name.

```
==> /opt/IBM/db2/V10.5/instance/db2ilist
```

   c) Find the database name.

```
==> su - ldapdb2 -c "db2 list db directory"
```

6. Find the service name from the `db2 dbm config` file.

```
==> su - ldapdb2
db2 get dbm cfg | grep -i svcename
```

Sample return.

```
TCP/IP Service name                          (SVCENAME) = ldapdb2svcids
 SSL service name                       (SSL_SVCENAME) =
```

7. Find the DB2 service port from the `/etc/services` file.

```
$ grep -w ldapdb2svcids /etc/services
```

Sample return.

```
ldapdb2svcids   3708/tcp
```

Configuring the virtual appliance to connect to the remote DB2 database

About this task

Procedure

1. Use the **idscfgdb** utility to configure the virtual appliance directory instance to connect with the remote DB2 database.

```
sds801va1> sds server_tools idscfgdb -I sdsinst1 -a sdsinst1 -t ldapdb -w sdsinst1
       -Y -S 3708 -l /home/sdsinst1 -P remote_6.4_server_hostname
       -u ldapdb2 -p passwd -n
```

2. Start **ibmslapd** in configuration only mode and reconfigure it with the default SSL settings.

   Use one of these methods.

   - Web administration tool method
     a. Log in to the Web Admin tool.
     b. Expand **Server administration**.
     c. Click **Manage security properties** > **Key database**.
     d. Type these values in the fields.

Table 12. Configuration values	
Field	**Value**
Key database path and file name	`/userdata/directory/Certificates/serverc.kdb`
Key password	`server`
Confirm password	`server`
Key label	`server_cert`

     e. Click **OK**.
   - Command line method
     a. Run the command.

```
sds801va1 > sds client_tools idsldapmodify -h sds801va1 -p 389 -D cn=root
-w passwd cn=SSL,cn=Configuration
ibm-slapdSslKeyDatabase=/userdata/directory/Certificates/serverc.kdb
ibm-slapdSSLKeyDatabasePW=server
ibm-slapdSslCertificate=server_cert
```

     b. Press Enter.
     c. Press Enter.
     d. Press CTRL+D

3. Restart the Directory Server and the Admin Server.

```
sds801va1 > sds server_tools ibmslapd -k
sds801va1 > sds server_tools ibmdiradm
sds801va1 > sds server_tools ibmslapd -n
```

Loading data from an LDIF file into a remote DB2 database

If you configured a remote DB2 database with Directory Server in a virtual appliance environment, you can use the remote bulkload scripts to load data from an LDIF file into the remote database for high-speed data transfer.

Before you begin

1. If you are migrating or by using a custom schema, the schema migration must be done before the virtual appliance is configured to the remote DB2.
2. Complete the steps to configure IBM Security Directory Suite virtual appliance with a remote DB2 database. See Configuring the remote DB2 database.

Procedure

1. Stop the Directory Server. See Managing servers with the Server Control widget,
2. Create the required suffixes by using the **idscfgsuf** command.
3. Upload the `ldif` file through the virtual appliance console or command-line interface. See Managing custom files or **idsgetfile**.
4. Run the bulkload utility with remote option **-Y**:

   ```
   sds server_tools idsbulkload -i sample.ldif -a parseonly -Y
   ```

   Note: The **-Y** option for bulkload utility on a remote database must always be used along with the **-a parseonly** option.
5. From the **Custom File Management** page of the virtual appliance console, download the `remote_bulkload.tar.gz` file. See Managing custom files.
6. On the remote database system, upload the `remote_bulkload.tar.gz` file to the home directory of the remote DB2 user.
7. Extract the `remote_bulkload.tar.gz` file.

   This file contains the *instance_name*`_remote.sh` or *instance_name*`_remote.bat`, where *instance_name* is the remote DB2 instance name.
8. Log in to the remote DB2 machine as DB2 instance user.
9. Change directory to the folder that contains the *instance_name*`_remote` scripts.

   Note: The remote bulkload scripts must be run from this containing folder as they use the database table files that are locally present.
10. Change permissions of all the files in the current directory:

    ```
    chmod 777 ./*.*
    ```
11. Run the *instance_name*`_remote` script for your operating system by using the DB2 instance user credentials:

    For example:

    ```
    ./instance_name_remote.sh DB2_instance_username password
    ```

Uninstalling DB2

If you installed the DB2 manually, use the DB2 commands to remove DB2 from the computer.

Before you begin

If your computer contains DB2 instances for the DB2 that you installed, you must manually drop the DB2 instances before the uninstallation of DB2. It is advisable to back up DB2 databases and data before the uninstallation.

About this task

For more information about the uninstallation of DB2, see the DB2 product documentation at the IBM Knowledge Center for DB2.

Procedure

If you manually installed DB2 in a custom location with DB2 commands, use DB2 commands for uninstallation of DB2.

Limitations and known issues with remote DB2

Refer to the limitation and known issues with remote DB2 that are listed in the troubleshooting section of IBM Security Directory Suite Knowledge Center.

See Remote DB2 with virtual appliance limitations and issues.

Chapter 4. IBM Global Security Kit Installation

To use Secure Sockets Layer (SSL) and Transaction Layer Security (TLS) with IBM Security Directory Suite, your computer must contain a supported version of IBM Global Security Kit (GSKit).

The IBM Security Directory Suite ISO installation package provides a virtual appliance that includes the installed GSKit. However, if you want to generate your own Directory Server instance stash files or custom CA signed certificates, you can use GSKit, Version 8.0.50.xx.

To install GSKit, Version 8.0.50.xx, complete the following steps:

1. Use the part number that is provided in the IBM Security Directory Suite, Version 8.0.1.x - Download Document to download the GSKit, Version 8.0.50.xx installation package from IBM Passport Advantage website.
2. Follow the steps in the next topics for each operating system.

The GSKit crypt package is required for low-level encryption support. The GSKit SSL package is required for secure communication handshake operations. The GSKit crypt package is a prerequisite for the GSKit SSL package.

Installing GSKit with `installp`

You can use the **`installp`** command to complete the GSKit installation on an AIX® system.

Before you begin

Access the IBM Security Directory Suite installation media to obtain the GSKit installable.

About this task

The **`installp`** installation program installs GSKit on an AIX system.

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Change the current working directory to the `gskit` directory where the GSKit installable is stored.
4. Run the **`installp`** command to install the GSKit64-bit packages.

```
installp -acgXd . GSKit8.gskcrypt64.ppc.rte
installp -acgXd . GSKit8.gskssl64.ppc.rte
```

5. Run the following command to verify whether the GSKit installation is successful:

```
lslpp -aL GSKit8*
```

Results

The installation program installs GSKit in the following locations on an AIX system:

```
/usr/opt/ibm/gsk8_64/
```

Installing GSKit with Linux utilities

Use the **rpm** command to complete the GSKit installation on a Linux system.

Before you begin

Access the IBM Security Directory Suite installation media to obtain the GSKit installable.

About this task

The **rpm** command installs GSKit on a Linux system. In the example, installation of GSKit on AMD64 Opteron/EM64T Linux is shown. For System z®, System i® or System p, or System x Linux, you must substitute with the appropriate package names.

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Change the current working directory to the `gskit` directory where the GSKit installable is stored.
4. Run the **rpm** command to install the GSKit packages.
   a) To install GSKit 64-bit packages, run the following commands:

```
rpm -ivh gskcrypt64-8.0.50.xx.linux.x86_64.rpm
rpm -ivh gskssl64-8.0.50.xx.linux.x86_64.rpm
```

5. Run the following command to verify whether the GSKit installation is successful:

```
rpm -qa | grep -i gsk
```

Results

The installation program installs GSKit in the following locations on a Linux system:

```
/usr/local/ibm/gsk8_64/
```

Installing GSKit with Solaris utilities

Use the **pkgadd** command to complete the GSKit installation on a Solaris system.

Before you begin

Access the IBM Security Directory Suite installation media.

About this task

The **pkgadd** command installs GSKit on a Solaris SPARC system.

Procedure

1. Log in as the root user.
2. Access the root user login shell.
3. Change the current working directory to the `gskit` directory where the GSKit installable is stored and unpack it by running the following commands.

```
uncompress gskcrypt64-8.0.50.xx.sun.sparc.tar.Z
tar -xf gskcrypt64-8.0.50.xx.sun.sparc.tar
uncompress gskssl64-8.0.50.xx.sun.sparc.tar.Z
tar -xf gskssl64-8.0.50.xx.sun.sparc.tar
```

4. Run the **pkgadd** command to install the GSKit 64-bit packages.

```
echo "instance=overwrite">/tmp/.gsk8_installadmin
pkgadd -d . -a/tmp/.gsk8_installadmin gsk8cry64.pkg
pkgadd -d . -a/tmp/.gsk8_installadmin gsk8ssl64.pkg
```

5. Run the following command to verify whether the GSKit installation is successful:

```
pkginfo | grep -i gsk
pkgparam package_name VERSION
```

Substitute the `package_name` value with the GSKit package name to verify the version.

Installing GSKit on Windows

Run the GSKit installation program to complete the GSKit installation on a Windows system.

Before you begin

Access the IBM Security Directory Suite installation media to obtain the GSKit installable.

About this task

In the example, installation of GSKit crypt 64-bit and GSKit SSL 64-bit is shown.

Procedure

1. Log in as a member of the administrator group.
2. Change the current working directory to the `gskit` directory where the GSKit installable is stored.
3. To install GSKit 64-bit packages, run the GSKit installation program.
   a) Run the GSKit8 crypt installation package, `gsk8crypt64.exe`.
   b) On the GSKit8 crypt installation window, complete the following steps:
      i) Specify the installation path for GSKit8 crypt.
      ii) Click **Next**.
      iii) Click **Install**.
      iv) Click **Finish**.
   c) Run the GSKit8 SSL installation package, `gsk8ssl64.exe`.
   d) On the GSKit8 SSL installation window, complete the following steps:
      i) Specify the installation path for GSKit8 SSL.
      ii) Click **Next**.
      iii) Click **Install**.
      iv) Click **Finish**.
4. To run GSKit commands from the command-line, set the *PATH* variable with the `bin` and `lib64` directories on Windows x86_64 system.
   If the GSKit installation location is `C:\Program Files\IBM\gsk8`, set the *PATH* variable with the following values:

```
set PATH="C:\Program Files\IBM\gsk8\bin";%PATH%
set PATH="C:\Program Files\IBM\gsk8\lib64";%PATH%
```

Installing GSKit silently on Windows

Run the GSKit installation program from the command prompt to complete the GSKit installation silently on a Windows system.

Before you begin

Access the IBM Security Directory Suite installation media to obtain the GSKit installable.

About this task

In the example, installation of GSKit crypt 64-bit and GSKit SSL 64-bit is shown.

Procedure

1. Log in as a member of the administrator group.
2. Access the command prompt.
3. Change the current working directory to the `gskit` directory where the GSKit installable is stored.
4. To install GSKit 64-bit packages silently, run the following commands:

```
gsk8crypt64.exe /s /v"/quiet"
gsk8ssl64.exe /s /v"/quiet"
```

5. To run GSKit commands from the command-line, set the *PATH* variable with the `bin` and `lib64` directories on Windows x86_64 system.

   If the GSKit installation location is `C:\Program Files\IBM\gsk8`, set the *PATH* variable with the following values:

```
set PATH="C:\Program Files\IBM\gsk8\bin";%PATH%
set PATH="C:\Program Files\IBM\gsk8\lib64";%PATH%
```

Chapter 5. IBM Global Security Kit uninstallation with operating system utilities

If you used operating system utilities for the installation of GSKit, use operating system utilities for the uninstallation of GSKit.

If IBM Security Directory Suite is installed on your computer, you must not remove GSKit if it is in use. If you want to use the latest GSKit version, you must first remove the installed GSKit from its registry. You can then run GSKit uninstallation.

Uninstalling GSKit with SMIT

Use the **smit** command to complete the uninstallation of GSKit from an AIX system.

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Run the **smit** command.

   The **Software Installation and Maintenance** window opens.
4. Select **Software Installation and Maintenance** > **Software Maintenance and Utilities**.
5. Select **Remove Installed Software**.
6. In the **Software Name** field, press **F4** to show the list of installed software. You can provide the `GSKit` value in the field to list all the GSKit packages.
7. Set the value for **REMOVE dependent software** to YES to remove software products and updates that are dependent upon the product you are removing.
8. Select the packages that you want to remove and press Enter.
9. Verify whether the GSKit uninstallation is successful.

```
lslpp -l 'GSK*'
```

Uninstalling GSKit with `installp`

Use the **installp** command to complete the uninstallation of GSKit from an AIX system.

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Run the following command to determine the GSKit packages that you want to remove:

```
lslpp -l 'GSK*'
```

4. To remove a GSKit package, run the following command:

```
installp -u package_name
```

   To remove GSKit completely, remove all the GSKit packages of the same version. For uninstallation of GSKit, you must first remove the GSKit SSL package and then the GSKit crypt package.

   To remove the `GSKit8.gskssl64` and `GSKit8.gskcrypt64` packages, run the following command:

```
installp -u GSKit8.gskssl64
installp -u GSKit8.gskcrypt64
```

5. Verify whether the GSKit uninstallation is successful.

```
lslpp -l 'GSK*'
```

Uninstalling GSKit with Linux utilities

Use the **rpm** command to complete the uninstallation of GSKit from a Linux system.

About this task

The following example shows the uninstallation of GSKit packages from an AMD64 Opteron/EM64T Linux system. For System z, System i or System p, or System x Linux, you must substitute with the appropriate package names.

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Run the following command to determine the GSKit packages that you want to remove:

```
rpm -qa | grep -i gsk
```

4. To remove a GSKit package, run the following command:

```
rpm -ev package_name
```

To remove GSKit completely, remove all the GSKit packages of the same version. For uninstallation of GSKit, you must first remove the GSKit SSL package and then the GSKit crypt package.

To remove the `gskssl64-8.0-14.26.x86_64` and `gskcrypt64-8.0-14.26.x86_64` packages, run the following command:

```
rpm -ev gskssl64-8.0-14.26.x86_64
rpm -ev gskcrypt64-8.0-14.26.x86_64
```

5. Verify whether the GSKit uninstallation is successful.

```
rpm -qa | grep -i gsk
```

Uninstalling GSKit with Solaris utilities

Use the **pkgrm** command to complete the uninstallation of GSKit from a Solaris system.

Procedure

1. Log in as the root user.
2. Access the command prompt.
3. Run the following command to determine the GSKit packages that you want to remove:

```
pkginfo | grep -i gsk
```

4. To remove a GSKit package, run the following command:

```
pkgrm package_name
```

To remove GSKit completely, remove all the GSKit packages of the same version. For uninstallation of GSKit, you must first remove the GSKit SSL package and then the GSKit crypt package.

To remove the `gsk8ssl64` and `gsk8cry64` packages, run the following command:

```
pkgrm gsk8ssl64
pkgrm gsk8cry64
```

5. Verify whether the GSKit uninstallation is successful.

```
pkginfo | grep -i gsk
```

Uninstalling GSKit on Windows

Use the GSKit commands to complete the uninstallation of GSKit from a Windows system.

About this task

In the example, silent uninstallation of the GSKit SSL 64-bit and GSKit crypt 64-bit packages from a Windows system on an AMD64/EM64T architecture is shown.

Note: You can also use **Start** > **Control Panel** > **Add or Remove Programs** to remove the GSKit packages.

Procedure

1. Log in as a member of the administrator group.
2. Access the command prompt.
3. Change the current working directory to the `gskit` directory where the GSKit installable is stored.
4. To remove GSKit 64-bit packages silently, run the following commands:

   To remove GSKit completely, remove all the GSKit packages of the same version. For uninstallation of GSKit, you must first remove the GSKit SSL package and then the GSKit crypt package.

```
gsk8ssl64.exe /s /x /v"/quiet"
gsk8crypt64.exe /s /x /v"/quiet"
```

Chapter 6. Manual deployment of Web Administration Tool

To manage and administer Directory Server instances with **Web Administration Tool**, it must be deployed in a supported version of WebSphere® Application Server.

WebSphere Application Server is the IBM runtime environment for applications that are based on Java™.

The Web Administration Tool provides a graphical user interface for configuring IBM Security Directory Server.

The IBM Security Directory Suite ISO installation package provides a virtual appliance with a ready-to-use Directory Server instance and Web Administration Tool that is already deployed. However, if you want to manually deploy the Web Administration Tool in WebSphere Application Server, you can install WebSphere Application Server, Version 8.5.5.

Follow the steps in the next topics to install and configure WebSphere Application Server, Version 8.5.5, and to manually deploy Web Administration tool.

For more information, see the IBM Knowledge Center for WebSphere Application Server.

Installing WebSphere Application Server

To manually deploy **Web Administration Tool**, you must complete the installation of WebSphere Application Server on your computer.

Procedure

1. Use the part number that is provided in the IBM Security Directory Suite, Version 8.0.1.x - Download Document to download the WebSphere Application Server, Version 8.5.5 installation package from IBM Passport Advantage website.
2. Log in with administrator privileges.
3. Access the command prompt.
4. Change the current working directory to the directory that contains the WebSphere Application Server installable.
5. Complete the WebSphere Application Server installation. and install it on your system. Search for *Installing and configuring your application server environment* in the IBM Knowledge Center for WebSphere Application Server.

What to do next

Complete the deployment of **Web Administration Tool**. See "Deploying Web Administration Tool in WebSphere Application Server" on page 49.

Default ports for the Web Administration Tool

To avoid port conflicts of ports between **Web Administration Tool** and other applications, you must know the default ports that are used by **Web Administration Tool**.

WebSphere Application Server uses the following default port settings for **Web Administration Tool**.

Note: These default ports are used only if the **deploy_IDSWebApp** script or batch file is used to deploy the `IDSWebApp.war` file into the WebSphere Application Server profile. If the typical deployment method is used from the WebSphere administrative console, the default port set of that specific profile is used.

- HTTP Transport (port 1): 12100
- HTTPS Transport (port 2): 12101

- Admin Console (for administering WebSphere Application Server) port: 12104
- Secure Admin Console (for administering WebSphere Application Server) port: 12105

WebSphere Application Server uses the following default port settings for other applications:

- Bootstrap/rmi port: 12102
- Soap connector port: 12103

The other port numbers that might be used by WebSphere Application Server: 9405, 9406, 9407, 9375, 9105, 7276, 7286, 5558, 5577, 5075, 5076.

If a port conflict exists with another application that might be using one or more of the default ports, take one of the following actions that is appropriate for your environment:

- Change the default ports to unused ports, and start the application the unused port.
- If the application that is using the default ports is not an important service or server, change its port number and free the default port.

To change the default port numbers that WebSphere Application Server initializes for application, you must set appropriate port number in the `portdef.props` file. The `portdef.props` file is in the `profiles\TDSWebAdminProfile\properties` directory of the WebSphere Application Server installation location.

HTTP Transport port 1
To modify the port for HTTP Transport port 1, change the entry with the port number 12100 to the port number that is not in use.

HTTPS Transport port 2
To modify the port for HTTPS Transport port 2, change the entry with the port number 12101 to the port number that is not in use.

Bootstrap/rmi port
To modify the port for Bootstrap/rmi port, change the entry with the port number 12102 to the port number that is not in use.

Soap connector port
To modify the port for Soap connector port, change the entry with the port number 12103 to the port number that is not in use.

Admin Console port
To modify the port for Admin Console port, change the entry with the port number 12104 to the port number that is not in use.

Admin Secure Console port
To modify the port for Admin Secure Console port, change the entry with the port number 12105 to the port number that is not in use.

Downloading Web Administration Tool

You must download the `IDSWebApp.war` and other files from the virtual appliance console. These files are required to deploy the Web Administration Tool.

Procedure

1. Log onto the IBM Security Directory Suite virtual appliance console. See Logging on to the virtual appliance console.
2. From the top-level menu of the virtual appliance console, select **Configure** > **Advanced Configuration** > **Custom File Management**.
3. In the left pane, on the **All Files** tab, expand **idstools**.
4. In the right pane, select **DirectoryServerWebAdministrationTool.zip**.
5. Click **Download**.
6. Extract the contents of the `DirectoryServerWebAdministrationTool.zip` compressed file.

It contains the following files, which are required for deploying, undeploying, and starting the Web Administration Tool.

a. `IDSWebApp.war`

b. `deploy_IDSWebApp`

c. `deploy_IDSWebApp.bat`

d. `TDSWEBPortDef.props`

Deploying Web Administration Tool in WebSphere Application Server

If you want to manage applications on your computer with WebSphere Application Server, you can deploy **Web Administration Tool** in WebSphere Application Server.

Before you begin

Before you deploy **Web Administration Tool** in WebSphere Application Server, you must complete the following steps:

1. Ensure that your computer contains a supported version of WebSphere Application Server.
2. Complete the steps in "Downloading Web Administration Tool" on page 48.

About this task

To deploy **Web Administration Tool** in WebSphere Application Server, you must deploy the `IDSWebApp.war` file that is contained in the `DirectoryServerWebAdministrationTool.zip` compressed file, which you downloaded by using the **Custom File Management** page in virtual appliance.

Procedure

1. Use the URL `http://`*`hostname_WAS_server`*`:9060/ibm/console` to log in the WebSphere Application Server Admin console.

   Substitute the *hostname_WAS_server* variable with the host name or IP address of your computer on which WebSphere Application Server is installed. If you specified a custom port to access WebSphere Application Server Admin console, substitute the default port, `9060`, with your port number.
2. Enter the user ID and password of the user.

   The user must contain the required permission to run operations on WebSphere Application Server.
3. On the left navigational pane, click **Application** > **New Application**.
4. In the **New Application** page, click **New Enterprise Application**.
5. In the **Path to the new application** page, choose one of the following options that are based on from where you accessed the WebSphere Application Server Admin console:
   - If you accessed the WebSphere Application Server Admin console from a local computer, select **Local file system**, and enter the path of the `IDSWebApp.war` file in the **Full path** field. You can also click **Browse** to specify the path.
   - If you accessed the WebSphere Application Server Admin console from a remote computer, select **Remote file system**, and enter the path of the `IDSWebApp.war` file in the **Full path** field. You can also click **Browse** to specify the path.
6. In the **How do you want to install the application** page, select the **Fast Path** option and click **Next**.
7. In the **Select installation options** page, the default options are selected.
8. Click **Next**.
9. In the **Map modules to server** page, you can map modules to the servers that are specified in the **Clusters and servers** field.

   a) Select the check box for the required module, and click **Apply**.

   b) After you complete the mapping, click **Next**.

10. In the **Map virtual hosts for Web modules** page, you can map the web application to the specific virtual servers.

    If there are more virtual hosts, the server requires information about the WebSphere Application Server environment to select the right module. In this example, the `default_host` option is available for selection.
11. Click **Next**.
12. In the **Map context roots for Web modules** page, enter the context root as `/IDSWebApp` in the field.
13. A summary with your selection is shown.
14. Click **Finish**.

    It initiates the installation of your application. A summary of installation is shown.
15. To save the changes to the master configuration, click **Save**.
16. On the left navigational pane, click **Applications** > **Application Types** > **WebSphere enterprise applications**.
17. In the **Enterprise Applications** page, select the check box next to `IDSWebApp_war`, and click **Start**.
18. Start **Web Administration Tool**.
19. To access **Web Administration Tool**, open a browser and enter the following address:

    - For non-secured access (HTTP), enter `http://WAS_server_hostname:9080/IDSWebApp`.
    - For secured access (HTTPS), enter `https://WAS_server_hostname:9443/IDSWebApp`

    The port, 9080, is the default HTTP port for WebSphere Application Server, and port, 9443, is the default HTTPS port. If these ports are not the configured port for your WebSphere Application Server, provide the appropriate port number.

    If Global or Administrative security is configured for WebSphere Application Server, then you must meet the following requirements:

    a. Deploy **Web Administration Tool** in WebSphere Application Server as a new profile.

    b. Configure SSL for **Web Administration Tool**.

    c. If it is not possible to deploy **Web Administration Tool** in a profile, add the Directory Server certificate to the truststore of the profile. For the server-client authentication, add the WebSphere Application Server profile certificate to the truststore of the directory server.

Starting WebSphere Application Server to use Web Administration Tool

Start the web application server that is associated with **Web Administration Tool** to add, manage, and administer directory server instances.

Before you begin

You must complete the following tasks before you start web application server that is associated with **Web Administration Tool**:

1. Install WebSphere Application Server.
2. Download the Web Administration Tool.
3. Deploy **Web Administration Tool**.

Procedure

1. To start the application server that is associated with **Web Administration Tool**, run the following command on your operating system:

   Windows

   Use any of the following methods:

- Go to **Start** > **Programs** > **IBM WebSphere** > **Application Server V8.5.5** > **Profiles** > ***profile_name*** > **Start the server**.
- Start the Windows service that is associated with the IBM WebSphere Application Server V8.5.5 *profile*.
- Run this command:

  ```
  was_install_dir\bin\startServer.bat server1 –profileName profile.
  ```

- Run this command:

  ```
  Run this command: profile_dir\bin\startServer.bat server1
  ```

AIX, Linux, and Solaris
Run any of the following commands:

- ```
  was_install_dir/bin/startServer.sh server1 –profileName profile
  ```
- ```
  profile_dir/bin/startServer.sh server1
  ```

2. Open a web browser.
3. Enter the following URL on the address bar of web browser:

   Note: If you installed and deployed **Web Administration Tool** on a remote system, substitute the host name or IP address of the system instead of `localhost`.

   ```
   http://localhost:12100/IDSWebApp
   ```

   If the **deploy_IDSWebApp** script or batch file was used to deploy the `IDSWebApp.war` file into the WebSphere Application Server profile, use the following URLs.

   If you are using the default Web Admin ports, use the following URLs.

   For non-secure access (HTTP)

   ```
   http://WAS_server_hostname:12100/IDSWebApp
   ```

   For secure access (HTTPS)

   ```
   https://WAS_server_hostname:12101/IDSWebApp
   ```

   If you are using the default WebSphere Application Server profile ports, use the following URLs.

   For non-secure access (HTTP)

   ```
   http://WAS_server_hostname:9080/IDSWebApp
   ```

   For secure access (HTTPS)

   ```
   https://WAS_server_hostname:9443/IDSWebApp
   ```

What to do next

- For more information, see the following topics in the IBM Knowledge Center for WebSphere Application Server:
  - For the default installation and profile directory locations, see Directory conventions.
  - For more information about starting the server, see startServer command.
- To manage and administer Directory Server instances, add servers in the **Web Administration Tool** console. See “Accessing Web Administration Tool” on page 52.

Accessing Web Administration Tool

To manage Directory Server instances remotely, open **Web Administration Tool** and configure Directory Server instance for remote management.

Before you begin

You must complete the following tasks before you can access **Web Administration Tool**:

1. Install WebSphere Application Server.
2. Download the Web Administration Tool.
3. Deploy **Web Administration Tool**.
4. Start the WebSphere Application Server that is associated with Web Administration Tool.

Procedure

1. To access **Web Administration Tool**, open a web browser and enter the following URL:

   ```
   https://hostname:12101/IDSWebApp.
   ```

2. Log in to the **Web Administration Tool** console as the console administrator.
   a) In the **User ID** field, enter `superadmin`.
   b) In the **Password** field, enter **secret**.

   Note: You must change the console administrator password after you log in for the first time.

   c) Click **Login**.
3. To add a Directory Server to the console, complete the following steps:
   a) On the **Introduction** page, click **Manage console servers**.
   b) On the **Manage console servers** page, click **Add**.
   c) In the **Server name** field, enter a unique name to identify your server.

   If you do not provide a value, the application assigns a `hostname:port` value or an `IP_address:port` value.

   d) In the **Hostname** field, the host name or the IP address of the Directory Server.
   e) In the **Port** field, enter the server port number.
   f) To specify whether the console must communicate with the server securely, select **Enable SSL encryption**.
   g) To enable the Administration port control, select **Administration server supported**.
   h) In the **Administration port** field, enter the Administration Server port number.
   i) To apply changes, click **OK**.
4. To logout of the **Web Administration Tool** console, click **Logout**.

Stopping WebSphere Application Server

Before the uninstallation of **Web Administration Tool**, you must logout of **Web Administration Tool** and stop the web application server that is associated with it.

Procedure

To stop a WebSphere Application Server profile, use any of the methods applicable for the operating system:

Windows

Use one of the following methods:

- Go to **Start** > **Programs** > **IBM WebSphere** > **Application Server V8.5.5** > **Profiles** > ***profile*** > **Stop the server**.
- Stop the Windows service associated with IBM WebSphere V8.5.5 *profile*.
- Run this command:

```
was_install_dir\bin\stopServer.bat server1 -profileName profile
```

- Run this command:

```
profile_dir\bin\stopServer.bat server1
```

AIX, Linux, and Solaris
Run one of the following commands:

- ```
  was_install_dir/bin/stopServer.sh server1 -profileName profile_name
  ```
- ```
  profile_dir/bin/stopServer.sh server1
  ```

What to do next

For more information, see the following topics in the IBM Knowledge Center for WebSphere Application Server:

- For the default installation and profile directory locations, see Directory conventions.
- For more information about stopping the server, see stopServer command

HTTPS with WebSphere Application Server

To secure web access to your application, you can configure and start your application in HTTPS mode.

After you deploy **Web Administration Tool** in WebSphere Application Server, you can start your application. You can connect to **Web Administration Tool** securely by providing HTTPS web address and the secure port.

To use HTTPS, provide the following web address to access**Web Administration Tool**:

`https://hostname:12101/IDSWebApp`

To use non-HTTPS connection, provide the following web address to access**Web Administration Tool**:

`http://hostname:12100/IDSWebApp`

You can also change the default JKS files with certificates that are provided with the web application server for SSL/TLS secure communication. You can create new key and truststore database files to use with application that is deployed in WebSphere Application Server. The default key and truststore database files are separate and are in the *WAS_HOME*`/profiles/TDSWebAdminProfile/etc/` directory. The *WAS_HOME* variable is the installation location of WebSphere Application Server. The default key database file is `key.p12`, and the default truststore database file is `trust.p12`.

If you created your JKS files, you can change the key and truststore database files. To configure your JKS files, passwords, and file formats, add, or modify the following entries (highlighted in **bold**) in the *WAS_HOME*`/profiles/TDSWebAdminProfile/config/cells/DefaultNode/security.xml` file:

```
<keyStores xmi:id="KeyStore_DefaultNode_10"
 name="key.p12"
 password="{xor}CDo9Hgw="
 provider="IBMJCE"
 location="${WAS_HOME}/profiles/TDSWebAdminProfile/etc/key.p12"
 type="JKS"
 fileBased="true"
 hostList=""
 managementScope="ManagementScope_DefaultNode_1"/>
<keyStores xmi:id="KeyStore_DefaultNode_11"
 name="trust.p12"
 password="{xor}CDo9Hgw="
```

```
provider="IBMJCE"
location="${WAS_HOME}/profiles/TDSWebAdminProfile/etc/trust.p12"
type="JKS"
fileBased="true"
hostList=""
managementScope="ManagementScope_DefaultNode_1"/>
```

Undeploying the Web Administration Tool from WebSphere Application Server

To replace an existing **Web Administration Tool** (`IDSWebApp.war` file) with a later version, you must undeploy the existing **Web Administration Tool**.

Before you begin

- You must have the necessary permissions to run operations on the WebSphere Application Server.
- You must stop the WebSphere Application Server that is associated with Web Administration Tool. See Stop the WebSphere Application Server.

Procedure

1. Log in to the WebSphere Application Server administrative console by using the URL `http://`*`hostname_WAS_server`*`:9060/ibm/console`.

   Where *hostname_WAS_server* is the host name or IP address of the computer where the WebSphere Application Server is installed.

   Note: If you specified a custom port to access the WebSphere Application Server administrative console, you must substitute your custom port number for the default port number, 9060.
2. Enter your ID and password.
3. Click **Application** > **Application Types** > **WebSphere enterprise applications** in the navigation pane.

   The Enterprise Applications pane is displayed.
4. Select the **IDSWebApp_war** application check box.
5. Click **Stop**.

   A message is displayed confirming that the server is stopped. The pane is refreshed. The check box is cleared and the status icon is changed.
6. Select the **IDSWebApp_war** application check box again.
7. Click **Uninstall**.
8. Click **OK** to confirm that you want to uninstall the application.

   A message is displayed confirming that the application was successfully uninstalled.
9. Click **Save** to commit the changes to the configuration.

Chapter 7. Migration

The migration roadmap provides a list of tasks that you must complete to migrate a Directory Server instance or a Federated Directory Server to IBM Security Directory Suite.

Note: If you have an earlier version of IBM Security Directory Suite installed, you must do a firmware upgrade to migrate to a later release, for example from IBM Security Directory Suite version 8.0 to 8.0.1. See Chapter 9, "Firmware upgrades," on page 65.

Migration is done as a first step after you install the IBM Security Directory Suite appliance.

Note: You must not execute any migration tasks when support mode is activated. Support mode activation is indicated by a message on the title banner of the virtual appliance console. See Activating support mode on virtual appliance.

Use the following roadmap as a guide to execute migration.

Table 13. Migration Roadmap

	Procedure	Reference
1	Before you begin the migration process, ensure that you backup the current state of the virtual appliance.	"Backing up the virtual appliance" on page 55
2	Migrate a Directory Server instance to IBM Security Directory Suite.	"Migration of a Directory Server instance" on page 55
3	Migrate a Federated Directory Server to IBM Security Directory Suite.	"Migration of a Federated Directory Server" on page 59

Backing up the virtual appliance

As a precautionary measure, back up the schema and configuration files of the IBM Security Directory Suite appliance before you begin the migration.

Procedure

Back up the active partition by using one of the following methods:

- Virtual appliance local management interface (LMI). See Managing the firmware settings.
- Virtual appliance command-line interface (CLI). See Firmware commands.

Note: To revert to the older state, set the inactive partition as active.

See Managing the firmware settings.

Migration of a Directory Server instance

Use this topic to migrate a Directory Server instance to IBM Security Directory Suite.

Migration of the Directory Server instance with premium features configured are not allowed in IBM Security Directory Suite Limited Edition. You must activate license to Standard or Enterprise editions.

Run the **idsimigr** utility to migrate the schema and configuration files of a Directory Server instance. Upon successful migration of the files, you might be required to run the following utilities if the Directory Server instance type is Relational Database Management (RDBM):

idscfgdb
Configures a database for a Directory Server instance. See **idscfgdb**.

Note:

1. You can also configure the existing database of the older Directory Server instance as the back-end to the Directory Server instance that is in IBM Security Directory Suite, Version 8.0.1.x. See **idscfgdb** and "Configuration of a remote DB2 database for the virtual appliance" on page 18.
2. Once the existing database of the older directory server instance is configured as the back-end to the Directory server instance in IBM Security Directory Suite, Version 8.0.1.x, you cannot operate on old Directory server instance and the Directory server instance from IBM Security Directory Suite. This leads to data inconsistency.

idscfgchglg
Configures a change log for a Directory Server instance. See **idscfgchglg**.

idsldif2db
Loads entries from an LDIF file to a database. See **idsldif2db**, **ldif2db**

The following utilities are optional to migrate a Directory Server instance from version 6.x.x to IBM Security Directory Suite, Version 8.0.1.x:

idswmigr
Migrates the Directory Server Web Administration tool settings.

idssnmpmigr
Migrates the Directory Server SNMP agent settings.

idslogmgmtmigr
Migrates the Directory Server QRadar or Cognos integration settings.

Migrating the schema and configuration files of a Directory Server instance

Migrate the schema and configuration files of a Directory Server instance from IBM Security Directory Server Version 6.x.x to IBM Security Directory Suite with the **idsimigr** utility.

Procedure

1. Run the *sds_installdir***/sbin/migbkup** utility to backup of the schema and configuration files from the older Directory Server instance.
   In these examples, `ldap2` is the LDAP instance and `/home/ldapdb2` is the instance location. Change V6.4 to the version that you have, such as V6.3.1 or V6.3.

   AIX and Solaris systems

   ```
   ==> mkdir /home/ldapdb2/ldapsaveconf
   ==> chmod g+w /home/ldapdb2/ldapsaveconf
   ==> chown ldapdb2:idsldap /home/ldapdb2/ldapsaveconf
   ==> cd /opt/IBM/ldap/V6.4/sbin
   ==> ./migbkup /home/ldapdb2/idsslapd-ldapdb2 /home/ldapdb2/ldapsaveconf
   ==> cp /home/ldapdb2/idsslapd-ldapdb2/etc/<customschemafiles>
          /home/ldapdb2/ldapsaveconf/etc
   ```

   Linux systems

   ```
   ==> mkdir /home/ldapdb2/ldapsaveconf
   ==> chmod g+w /home/ldapdb2/ldapsaveconf
   ==> chown ldapdb2:idsldap /home/ldapdb2/ldapsaveconf
   ==> cd /opt/ibm/ldap/V6.4/sbin
   ==> ./migbkup /home/ldapdb2/idsslapd-ldapdb2 /home/ldapdb2/ldapsaveconf
   ==> cp /home/ldapdb2/idsslapd-ldapdb2/etc/<customschemafiles>
          /home/ldapdb2/ldapsaveconf/etc
   ```

   Windows systems

   ```
   > mkdir C:\ldapsaveconf
   > cd C:\Program Files\IBM\LDAP\V6.4\sbin
   > .\migbkup C:\idsslapd-ldapdb2 C:\ldapsaveconf
   > cp C:\idsslapd-ldapdb2/etc/<customschemafiles> C:\ldapsaveconf/etc
   ```

2. Archive the directory contents that are generated by the *sds_installdir***/sbin/migbkup** utility (on the system where a previous version of Directory Server was installed).

UNIX systems

Run the following command.

```
==> cd /home/ldapdb2; tar -cvf ldapsaveconf.tar ldapsaveconf
```

Windows systems

a. Open Windows Explorer.

b. Right-click on the `ldapsaveconfig` folder.

c. Click **Send to** > **Compressed (zipped) folder**. An `ldapsaveconf.zip` file is created in the `C:` drive.

3. Upload the archive file and the LDIF file to IBM Security Directory Suite virtual appliance by using one of the following methods:

- Local management interface (LMI)

  a. Access the LMI web interface.

  b. Click **Configure Directory Suite** .

  c. Click **Custom File Management** under **Advanced Configuration** .

  d. Click the **CustomIn** folder under **directories** on the **All Files** tab.

  e. Click **Upload**.

  f. Use the **Browse** utility on the **File Upload** window to select the `ldapsaveconf.tar` file or the `ldapsaveconf.zip` file and click **Save Configuration**.

- Command-line interface (CLI) **idsgetfile** command (for UNIX systems only)

  a. Use puTTy or ssh to log in to the IBM Security Directory Suite virtual appliance system as `admin`.

  b. Run the following command to download the `ldapsaveconf.tar` file directly onto the virtual appliance form the remote directory server system.

  ```
  sds801va > sds client_tools idsgetfile -h <previous_version>
   -u root -f /home/ldapdb2/ldapsaveconf.tar
  ```

  Where *previous_version* is the host name or IP address of the previous system.

Note: If the Directory Server instance was configured with any custom schema, the post-migration of the Directory Server instance might fail to start. Ensure that all the custom schema files are uploaded to the applianceCustomIn location.

4. Run the **idsimigr** command from the CLI.

```
sds migration_tools idsimigr -u  archive_filename
```

Where *archive_filename* is the schema configuration archive file from the previous version, such as 6.4.

For the **-u** option, provide the uploaded `ldapsaveconf.tar` file without any path. For example,

```
sds801va > sds migration_tools idsimigr -u ldapsaveconf.tar
```

Note: This utility stops the Directory Server instance and its administrative server if it is running and proceeds with the migration. This utility performs the following actions:

a. Removes the existing SDS instance, DB2 instance, and DB2 database.

b. Creates an SDS instance and migrates the configuration, encryption seed, encryption salt, and schema from the 6.4 tar file.

c. Creates a DB2 instance.

5. Run the **idscfgdb** command to configure the Directory Server instance to a new blank local or embedded DB2 database.

```
sds801va1 > sds server_tools idscfgdb -I sdsinst1 -a sdsinst1 -w sdsinst1 -t sdsinst1
 -l /home/sdsinst1 -n
```

6. Start the Directory Server instance from the Local Management Interface dashboard.

What to do next

After migration, you might need to do the following tasks:

1. Reconfigure the SSL settings. See Managing SSL certificates for Directory Server.
2. Reconfigure database for the Directory Server instance. See **idscfgdb**.
3. Reconfigure changelog database for the Directory Server instance. See **idscfgchglg**.
4. Load the LDIF data into the Directory Server. See **idsldif2db**, **ldif2db**.

Migrating the Directory Server Web Administration Tool

Migrate the Directory Server web administration tool configuration files from IBM Security Directory Server Version 6.x.x to IBM Security Directory Suite with the **idswmigr** utility.

Procedure

1. On the system where an older version of the Directory Server Web Administration Tool was deployed, copy the following files from `deployed_webadmin_profile_dir` to an empty folder and archive:
   - `console_passwd`
   - `logging.properties`
   - `idswebapp.properties`
   - `IDSAppReg.xml`
   - `IDSSchemaSettings.xml`
   - `IDSSessionMgmt.xml`
   - `IDSServersInfo.xml`
   - `IDSSearchMgmt.xml`
2. Upload the archive file to the IBM Security Directory Suite virtual appliance by using one of the following methods:
   - Local Management Interface
   - **CLI**, "idsgetfile"
3. Run **CLI**.
   For example, **sds migration_tools idswmigr -u** *archive_filename*

   Note: This utility stops the Directory Server instance and its administrative server if it is running and proceeds with the migration.
4. Start the Directory Server instance from the Local Management Interface dashboard.

What to do next

You might be required to reconfigure SSL settings. See Managing SSL certificates for Directory Server Web Administration Tool

Migrating the Directory Server Log Management Tool

Migrate the Directory Server log management tool configuration files (that are required for integration with QRadar/Cognos) from IBM Security Directory Server Version 6.3.1 and above to IBM Security Directory Suite with the **idslogmgmtmigr** utility.

Procedure

1. Copy the following files to an empty folder and archive:
   - *sds_install_dir*`/idstools/idslogmgmt/add.map`

- *sds_install_dir*/idstools/idslogmgmt/bind.map
- *sds_install_dir*/idstools/idslogmgmt/compare.map
- *sds_install_dir*/idstools/idslogmgmt/delete.map
- *sds_install_dir*/idstools/idslogmgmt/modify.map
- *sds_install_dir*/idstools/idslogmgmt/modifydn.map
- *sds_install_dir*/idstools/idslogmgmt/search.map
- *sds_install_dir*/idstools/idslogmgmt/unbind.map
- *sds_instance_home_dir*/etc/logmgmt/OIDDescriptors.properties
- *sds_instance_home_dir*/etc/logmgmt/idsauditdb.properties

2. Upload the archive file to the IBM Security Directory Suite virtual appliance by using one of the following methods:
   - Local Management Interface
   - **CLI**, "idsgetfile"
3. Run **CLI**.
   For example, **sds migration_tools idslogmgmtmigr -u** *archive_filename*

   Note: This utility stops the Directory Server instance and its administrative server if it is running and proceeds with the migration.
4. Start the service from **CLI sds server_tools idslogmgmt -n**.

Migrating the Directory Server SNMP agent

Migrate the Directory Server SNMP agent configuration files from the IBM Security Directory Server Version 6.x.x to IBM Security Directory Suite with the **idssnmpmigr** utility.

Procedure

1. Copy the following files to an empty folder and archive:
   - *sds_install_dir*/idstools/snmp/IBM-DIRECTORYSERVER-MIB
   - *sds_install_dir*/idstools/snmp/INET-ADDRESS-MIB
   - *sds_install_dir*/idstools/snmp/idssnmp.conf
   - *sds_install_dir*/idstools/snmp/ idssnmp.properties
2. Upload the archive file to the IBM Security Directory Suite virtual appliance by using one of the following methods:
   - Local Management Interface
   - **CLI**, "idsgetfile"
3. Run **CLI**.
   For example, **sds migration_tools idssnmpmigr -u** *archive_filename*

   Note: This utility stops the Directory Server instance and its administrative server if it is running and proceeds with the migration.
4. Start the service from **CLI** by using **idssnmp -n** .

Migration of a Federated Directory Server

Use this topic to migrate a Federated Directory Server to IBM Security Directory Suite.

The following utilities are required to migrate a Federated Directory Server configuration from IBM Security Directory Integrator Version 7.2 to IBM Security Directory Suite, Version 8.0.1.x:

- fdsmigr
- fdsscimmigr

Migrating the Federated Directory Server with Directory Server as target

Migrate the Federated Directory Server configuration from IBM Security Directory Integrator Version 7.2 to IBM Security Directory Suite with the **fdsmigr** utility.

Procedure

1. Copy the following files to an empty folder and archive:
   - *fds_solution_dir*/configs/SE_DefaultFDS.xml
   - *fds_solution_dir*/solution.properties
   - *fds_solution_dir*/LDAPSync/FDS_ISAM_Plugin.map
   - *fds_solution_dir*/LDAPSync/QRadar.map
   - *fds_solution_dir*/LDAPSync/group.map
   - *fds_solution_dir*/LDAPSync/SNMP.map
   - *fds_solution_dir*/LDAPSync/container.map
   - *fds_solution_dir*/LDAPSync/organization.map
   - *fds_solution_dir*/LDAPSync/country.map
   - *fds_solution_dir*/LDAPSync/organizationalunit.map
   - *fds_solution_dir*/LDAPSync/LDAPSync.properties
   - *fds_solution_dir*/LDAPSync/customScript.js
   - *fds_solution_dir*/LDAPSync/person.map
   - *fds_solution_dir*/LDAPSync/dcobject.map
   - *fds_solution_dir*/*.map files
2. Upload the archive file to the IBM Security Directory Suite virtual appliance by using one of the following methods:
   - Local Management Interface
   - **CLI**, "idsgetfile"
3. Run **CLI**.
   For example, **sds migration_tools fdsmigr -u** *archive_filename*

   Note: This utility stops the Directory Server instance and its administrative server if it is running and proceeds with the migration.
4. Start the Federated Directory Server from the Local Management Interface dashboard.

What to do next

You might be required to reconfigure SSL settings. See Managing SSL certificates for Federated Directory Server.

Migrating a Federated Directory Server configuration for SCIM as Target

Migrate the Federated Directory Server configuration from IBM Security Directory Integrator Version 7.2 to IBM Security Directory Suite with the **fdsscimmigr** utility.

Procedure

1. Copy the following files to an empty folder and archive:
   - *fdsscim_solution_dir*/configs/SE_DefaultFDS.xml
   - *fdsscim_solution_dir*/solution.properties
   - *fdsscim_solution_dir*/LDAPSync/FDS_ISAM_Plugin.map
   - *fdsscim_solution_dir*/LDAPSync/QRadar.map

- *fdsscim_solution_dir*/LDAPSync/group.map
- *fdsscim_solution_dir*/LDAPSync/SNMP.map
- *fdsscim_solution_dir*/LDAPSync/container.map
- *fdsscim_solution_dir*/LDAPSync/organization.map
- *fdsscim_solution_dir*/LDAPSync/country.map
- *fdsscim_solution_dir*/LDAPSync/organizationalunit.map
- *fdsscim_solution_dir*/LDAPSync/LDAPSync.properties
- *fdsscim_solution_dir*/LDAPSync/customScript.js
- *fdsscim_solution_dir*/LDAPSync/person.map
- *fdsscim_solution_dir*/LDAPSync/dcobject.map
- *fdsscim_solution_dir*/LDAPSync/Flow_sun2ids_WriteBack.map
- *fdsscim_solution_dir*/SCIM/GroupMapping.json
- *fdsscim_solution_dir*/SCIM/QRadarLogging.map
- *fdsscim_solution_dir*/SCIM/SCIM.properties
- *fdsscim_solution_dir*/SCIM/UserMapping.json
- *fdsscim_solution_dir*/SCIM/GroupSchema.json
- *fdsscim_solution_dir*/SCIM/ServiceProviderConfig.json
- *fdsscim_solution_dir*/SCIM/UserSchema.json

2. Upload the archive file to the IBM Security Directory Suite virtual appliance by using one of the following methods:
   - Local Management Interface
   - **CLI**, "idsgetfile"
3. Run **CLI**.
   For example, **sds migration_tools fdsmigr -u** *archive_filename*

   Note: This utility stops the Directory Server instance and its administrative server if it is running and proceeds with the migration.
4. Start the Federate Directory Server SCIM service from the Local Management Interface dashboard.

What to do next

- After you migrate, you must change the default port to 2098. For a list of all default ports, see "Default settings for IBM Security Directory Suite virtual appliance" on page 12
- You might be required to reconfigure SSL settings. See Managing SSL certificates for Federated Directory Server with SCIM as target.

Chapter 8. Fix pack installation

You can install a fix pack on the virtual appliance by using the virtual appliance console or the local management interface (LMI) commands.

Important: If FIPS mode is enabled for the virtual appliance, see Chapter 10, “FIPS compliance,” on page 67 for important information before you install a fix pack on a FIPS-compliant virtual appliance.

To install a fix pack from the virtual appliance console, see Installing a fix pack.

To install a fix pack by using the command-line interface, see Fix pack installation.

Chapter 9. Firmware upgrades

Install the firmware update to upgrade the IBM Security Directory Suite virtual appliance.

Important: If FIPS mode is enabled for the virtual appliance, see FIPS compliance for important information before you install a firmware upgrade on a FIPS-compliant virtual appliance.

Note:

- As a precautionary measure to avoid issues, you must ensure that all processes are in the stopped state before you proceed with firmware upgrade.
- You must not apply a firmware upgrade when support mode is activated. Support mode activation is indicated by a message on the title banner of the virtual appliance console. See Activating support mode on virtual appliance.

Before you apply the firmware update to upgrade the IBM Security Directory Suite virtual appliance, you must back up your Directory Server and Federated Directory Server data, which includes all the databases and the directory server.

The virtual appliance has two partitions with separate firmware on each partition. The partitions are swapped during the firmware updates to roll back the firmware updates when required. Either of the partitions can be active on the 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 virtual appliance restarts the system by using Partition 2, which is now the active partition.

The virtual appliance version upgrade can be installed only by using the virtual appliance command-line interface (CLI).

1. Download the `*.pkg` build.
2. Copy the firmware package to the virtual appliance system by using the **`upload_firmware_tool.zip`** that is provided under the `idstools` folder of **Custom File Management** page of the virtual appliance console. This tool is the only way to copy a firmware upgrade package to the virtual appliance.
   a. Log in to the IBM Security Directory Suite virtual appliance console.
   b. Click **Configure** > **Custom File Management**.
   c. Click **`idstools`** folder on the left pane.
   d. Select **`upload_firmware_tool.zip`** on the right pane.
   e. Click **Download** and save the `upload_firmware_tool.zip` file to a location on a system where Java 1.7 is installed.
   f. Extract the contents of the `upload_firmware_tool.zip` tool.
   g. Follow the usage instructions in the `ReadMe.txt` file that is provided in this ZIP file to copy the firmware package. For example:

```
# java -jar FileUpload.jar <Hostname> <AdminId> <AdminPassword> temptrust.jks WebAS
<firmware upgrade>.pkg
File size: 1659255515
SERVER REPLIED:
upload completed successfully.
```

   Note: After the `File size` response, progress is not indicated on the screen until the file upload is completed and the tool displays the `SERVER REPLIED` message. This process takes a few minutes, but might take longer depending on your network speed.
3. Access the virtual appliance command-line interface by using either an `ssh` session or the console.
4. In the virtual appliance command-line interface, run the **sds** command to display the `sds` prompt.

5. At the `sds` prompt, run the **`firmware_update`** command.
6. At the `firmware_update` prompt, run the following commands:
   a. Run the **`install_firmware`** command to install the available firmware update to the system.

      Note:

      - You can run the **`list_firmware`** command to list the firmware updates that are available at the download location.
      - You can run the **`delete_firmware`** command to delete the existing or unwanted firmware updates from the system.

   b. Select the index of the firmware update that you want to install to the virtual system and press `Enter`. The following results take place:

      i) The upgrade process formats Partition 2 and installs the new firmware update on it.

      ii) When you apply the firmware update, your policies and settings are copied from Partition 1 to Partition 2.

      iii) On completion, the process indicates that you must restart the virtual system.

   c. Type **`reboot`** and press `Enter` to restart the virtual system by using Partition 2. Partition 2 is now the active partition.

      The following results take place:

      i) After the virtual appliance restarts from the Partition 2, all of the configuration that was part of Partition 1 is applied to the Partition 2.

      ii) After the configuration is applied to the virtual appliance, the process indicates that you must restart the virtual appliance.

   d. Restart the virtual appliance to complete the upgrade process.

   e. Restart the Directory services.

   f. Clear the browser cache and restart browser, if you want to access the virtual appliance console.

   g. Configure the application interface only after you upgrade. For more information, see Managing application interfaces.

   h. 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.

      Take the following actions:

      i) Check and fix any errors if the upgrade process failed.

      ii) Set Partition 1 as the active partition and restart it.

Note: When you upgrade from IBM Security Directory Suite version 8.0 to 8.0.1, you must manually start the Federated Directory Server and Federated Directory Server SCIM Target servers.

Chapter 10. FIPS compliance

You can enable FIPS 140-2 mode when you install IBM Security Directory Suite virtual appliance.

Federal Information Processing Standards (FIPS) are guidelines that are set for software and hardware computer security products. Products that support FIPS standards can be set into a mode where the product uses only FIPS approved algorithms and methods. FIPS 140-2 is a National Institute of Standards and Technology standard.

Security toolkits typically support both FIPS approved and non-FIPS approved functions. In FIPS mode, the product is incapable of using any non-FIPS approved methods.

You can enable FIPS compliance when you are initially setting up virtual appliance after installation. See steps 5 and 6 in the topic, "Setting up the virtual appliance" on page 8.

Before you enable the FIPS compliance on the virtual appliance, take note of the following limitations:

- FIPS-compliant mode can be enabled only on new virtual appliance installations.
- Virtual appliances that are operating in FIPS-compliant mode can only securely connect to FIPS-compliant systems.

When you enable FIPS 140-2 mode for virtual appliance, FIPS compliance is applied for Directory Server and IBM Security Directory Integrator instances.

FIPS mode status

To check whether FIPS is enabled, use one of the following methods:

- In the virtual appliance console, go to the **Manage** > **Maintenance** > **About** page. The **FIPS Mode Status** indicates whether FIPS mode is enabled. For more information see, Viewing information about the product.
- In the virtual appliance command-line interface, enter `fips status` to verify whether FIPS is enabled. If the following message is displayed, then FIPS mode is enabled.

```
FIPS 140-2 Status: OK
Appliance has enabled FIPS mode successfully.
```

If FIPS mode is not enabled, the `fips status` command is not available in the virtual appliance command-line interface. For more information, see FIPS commands.

Fix packs and firmware updates

Before you install a fix pack or firmware update on a FIPS-compliant system, you must take a snapshot at the virtual machine level, so that you can go back to the previous state, if required.

Fix pack installation

If FIPS mode is enabled on the virtual appliance, when you attempt to install a fix pack, a message is displayed stating that the appliance is currently running in FIPS 140-2 mode.

Before you proceed with the fix pack installation, confirm with IBM Support to ensure that the fix pack to be applied is safe to install in FIPS mode.

You must not apply a fix pack that is not FIPS-compliant on a virtual appliance where FIPS mode is enabled. If you do so, the FIPS certification of the appliance is invalidated and the virtual appliance goes into an error state.

In the virtual appliance command-line interface, enter `fips status`. If the virtual appliance is an error state, the following message is displayed:

```
FIPS 140-2 Status: Error
Appliance has entered FIPS error state.
```

The appliance cannot be recovered because all data is encrypted on a FIPS enabled system and an attempt to replace any file would break the checksum. IF you took a backup at the virtual machine level, you can use this backup to restore the appliance.

Firmware updates

Upgrade from a FIPS enabled system is possible. However, upgrade is not supported from a system where FIPS is not enabled to a system where FIPS is enabled.

Appendix A. Accessibility features for IBM Security Directory Suite

Accessibility features assist users who have a disability, such as restricted mobility or limited vision, to use information technology content successfully.

Overview

The following list includes the major accessibility features in IBM Security Directory Suite.

- Supports interfaces commonly used by screen readers. This feature applies to applications on Windows operating systems only.
- Can be operated by using only the keyboard.
- Communicates all information independently of color.
- Supports interfaces commonly used by screen magnifiers. This feature applies to applications on Windows operating systems only.
- Allows the user to access the interfaces without inducing seizures due to photosensitivity.

IBM Security Directory Suite uses the latest W3C Standard, WAI-ARIA 1.0, to ensure compliance with US Section 508 and Web Content Accessibility Guidelines (WCAG) 2.0. To take advantage of accessibility features, use the latest release of your screen reader and the latest web browser that is supported by IBM Security Directory Suite.

The IBM Security Directory Suite online product documentation in IBM Knowledge Center is enabled for accessibility. The accessibility features of IBM Knowledge Center are described in the Accessibility section of the IBM Knowledge Center help.

Keyboard navigation

This product uses standard navigation keys.

Interface information

The IBM Security Directory Suite user interfaces do not have content that flashes 2 - 55 times per second.

The IBM Security Directory Suite web user interface relies on cascading style sheets to render content properly and to provide a usable experience. The application provides an equivalent way for low-vision users to use system display settings, including high-contrast mode. You can control font size by using the device or web browser settings.

The IBM Security Directory Suite web user interface includes WAI-ARIA navigational landmarks that you can use to quickly navigate to functional areas in the application.

Related accessibility information

In addition to standard IBM help desk and support websites, IBM has a TTY telephone service for use by deaf or hard of hearing customers to access sales and support services:

TTY service
800-IBM-3383 (800-426-3383)
(within North America)

For more information about the commitment that IBM has to accessibility, see IBM Accessibility.

Index

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

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 grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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

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 jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide 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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

The client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

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-IBMproducts. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

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 actual people or business enterprises 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. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

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_.

Trademarks

IBM, the IBM logo, and 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 "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

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.