CHAPTER 7

Maintaining the VDS-SB

This chapter explains how to perform common administrative tasks including updating system software, hard disk drive maintenance, and rebooting and deleting devices. The following major topics are covered:

For information about database maintenance, see the "Setting Storage Handling" section on page 3-19.

Software Upgrade

The software upgrade section covers the following topics:

Getting a Software File from Cisco.com

To get a software file from Cisco.com, do the following:

Step 1 Launch your web browser and enter the following URL:

http://www.cisco.com/cisco/software/navigator.html

The Select a Product page is displayed if you have recently logged in; otherwise, the Log In page is displayed.

Step 2 Log in to Cisco.com using your designated username and password.

Step 3 Choose **Products > Video > Videoscape > Cisco Videoscape Distribution Suite > Cisco Videoscape Distribution Suite Service Broker**. The Downloads page is displayed.

Step 4 Click the software release you want. The page refreshes and the software image files are displayed.

Step 5 Click the link for the software image file you want.

- If this is the first time you have downloaded a file from Cisco.com, the Cisco Systems Inc., Encryption Software Usage Handling and Distribution Policy is displayed. Read the policy, fill in the unfilled fields, and click **Accept**.
- If you previously filled out the Encryption Software Usage and Handling and Distribution form, the form does not display again.

The Download page is displayed with the information about the software image file and a Download link.

Step 6 Click **Download Now** to download the file, or click **Add to cart** to select more image files before downloading them. The Download Cart page is displayed.

Step 7 Click **Proceed With Download**. The Cisco End User Software License Agreement is displayed.

Step 8 Read the agreement and click **Agree**. The Download Software page is displayed.

Step 9 Choose a download option, either **Download Manger Option** or **Non Java Download Option**. A new window displays the filename of the ISO image file.

Step 10 Click **Download**. The File Download dialog box is displayed.

Step 11 Click **Save**. The Save As dialog box is displayed.

Step 12 Navigate to the location where you want to save the file and click **Save**. The file downloads.

Finding the Software Version of the Devices

The VDSM Home page gives a brief summary of the software versions in use on all the devices in the VDS-SB network.

To view the software version running on a particular device, choose **Devices > Devices**. The Devices Table page displays the software version for each device listed.

Clicking the **Edit** icon next to the device name in the Devices Table page displays the Devices home page, which shows the software version for that device.

Note The software version is not upgraded until a software upgrade has been successfully completed. If a software upgrade is in progress, the version number displayed is the base version, not the upgraded version number.

Configuring the Software Image Settings

To upgrade your VDS-SB software release, you must first configure the software image settings.

To configure the software image settings, do the following:

Step 1 Choose **System > Software Image Management**. The Software Files Table page is displayed.

Step 2 Click the **Create New** icon in the task bar. The Software Image page is displayed.

Step 3 In the **Software Image URL** field, enter the URL for the .bin software file that you downloaded from Cisco.com.

a. Choose a protocol (**http** or **ftp**) from the drop-down list.

b. Enter the URL of the software file; for example, a valid URL might look like this:

http://internal.mysite.com/vos/*VDS-2.x.x-K9*.bin

In this URL, *VDS-2.x.x-K9* is the name of the software upgrade file. (The filename might include the version number.)

Step 4 If your server requires user login authentication, enter your username in the **Username** field and enter your login password in the **Password** field. Enter the same password in the **Confirm Password** field.

Step 5 Enter the software version number in the **Software Version** field. You can copy this number from the version portion of the software filename in the software file URL.

Specify the version in one of two formats: X.Y.Z-bB or X.Y.Z.b.B, where X = major version, Y = minor version, Z = maintenance version, b = build letter, and B = build number.

Step 6 If you want the size of the software file considered during validation, enter a file size (in bytes) in the **File Size** field. If you leave this field blank, the URL is checked without regard to the software file size.

Step 7 To validate the Software Image URL, Username, and Password fields, click the **Validate Software Image Settings** button.

When you click the **Validate Software Image Settings** button, the following occurs:

- Software file URL is resolved.
- Connection to the software file URL is established using the username and password, if specified.
- If a file size is specified, the actual size of the software file is obtained and compared against the value in the File Size field.
- Message is returned, indicating success or errors encountered.

Step 8 In the Advanced Settings section, check the **Auto Reload** check box to automatically reload a device when you upgrade the software.

Step 9 If you want, you can choose one of three download methods:

- **Default**—Uses pre-positioned content but always falls back to direct download.
- **Direct Download Only**—Directly downloads the file using the software file URL.

Step 10 For downgrades only, specify the VDSM IP address to be used for device registration in the **VDSM IP Address** field.

The VDSM IP Address field is the IP address of a VDSM after the software is downgraded. (This field is optional and only applies for downgrades.) After the downgrade, the SB registers with the VDSM with the IP address specified in this field.

Step 11 Click **Submit**.

To delete a software file, click the **Delete** icon in the task bar.

Caution If your browser is configured to save the username and password for the VDSM, the browser auto-populates the Username and Password fields in the Software Image page. You must clear these fields before you click **Submit**.

The software file that you want to use is now registered with the VDSM. When you perform the software upgrade or downgrade, the URL that you just registered becomes one of the choices available in the Update Software page. (See the "Upgrading the Software" section on page 7-4.)

Upgrading the Software

When upgrading software in your VDS-SB network, begin with Service Engines and Service Routers before upgrading the VDSM. The VDSM reboots at the conclusion of the upgrade procedure, causing you to temporarily lose contact with the device and the user interface. After the VDSM has upgraded its software and rebooted, it may be unable to communicate with devices running different versions of the VDS-SB software.

Caution Primary and standby VDSMs must be running the same version of VDS-SB software. If they are not, the standby VDSM detects this and does not process any configuration updates it receives from the primary VDSM. You need to upgrade your standby VDSM first, and then upgrade your primary VDSM. We also recommend that you create a database backup for the primary VDSM and copy the database backup file to a safe place before you upgrade the software.

Caution To upgrade the software image on a server, you first need to offload a server for maintenance. Once the server has been fully offloaded, you can upgrade the software. After updating the software, uncheck the **Server Offload** check box to allow the server to receive client requests from the Service Broker. See the Server Offload field in Table 3-3 on page 3-3 for more information.

Downgrading the Software

For software downgrades of systems with primary and standby VDSMs, you need to do the following:

1. If you are using the VDSM GUI, downgrade the standby VDSM first, followed by the primary VDSM.

   If you are using the CLI, downgrade the primary VDSM first, followed by the standby VDSM.

2. After downgrading the primary and standby VDSMs, using the CLI, log in to each VDSM and run the following commands:

```
cms database downgrade
cms enable
```

Interoperability Considerations

In general, a VDS-SB network is upgraded gradually, so that your network might consist of nodes with different software versions for the duration of time it takes to upgrade all nodes. Dissimilar software versions are not supported in the long term, and only the interoperability considerations listed below are supported until all devices are running the same software version. You can expect the following behavior during an upgrade or downgrade of your network:

- VDS-SB network continues to operate with mixed versions up to one major or minor version difference in a deployed solution.
- New features that depend on device cooperation might not be fully functional until the VDS-SB network upgrade is complete, but no existing features are affected.

- While being upgraded, a node is unavailable for a short time.
- All nodes, other than the node being upgraded, continue to operate at full capacity. The availability of other nodes is not affected during an upgrade.
- Content is preserved during an upgrade or downgrade unless you remove an origin service.
- All logs are preserved during an upgrade or downgrade, unless you change the disk configuration. Anytime disk space is reconfigured, the logs are automatically removed.

We strongly recommend that you upgrade your VDS-SB network devices in the following order:

1. Service Broker
2. Standby VDSMs (Upgrade before primary when using the GUI only.)
3. Primary VDSM

Note When you upgrade VDSMs using the CLI, we recommend that you upgrade your primary VDSM first, and then upgrade your standby VDSM. Primary and standby VDSMs must be operating with exactly the same software release as each other for failover to be successful.

Table 7-1 Upgrade Status Messages

Upgrade Status Message	Condition
Pending	The request has yet to be sent from the VDSM to the device, or receipt of the request has yet to be acknowledged by the device.
Downloading	The download method for the software file is being determined.
Proceeding with Pre-positioned Download	The download method for the software file is detected as pre-positioned. Proceeding with download of a pre-positioned software file.
Proceeding with Download	The download method for the software file is detected as direct download. Proceeding with the request for direct download of the software file.
Download in Progress (Completed …)	Direct download of the software file is being processed. “Completed” indicates the number of megabytes processed.
Download Successful	The direct download of the software file has been successful.
Download Failed	The direct download of the software file cannot be processed. Further troubleshooting is required; see the device system message log.
Proceeding with Flash Write	A request has been made to write the software file to the device flash memory.
Flash Write in Progress (Completed …)	The write of the device flash memory is being processed. “Completed” indicates the number of megabytes processed.
Flash Write Successful	The flash write of the software file has been successful.

Table 7-1 Upgrade Status Messages (continued)

Upgrade Status Message	Condition
Reloading	A request to reload the device has been made to complete the software upgrade. The device may be offline for several minutes.
Reload Needed	A request to reload the device has not been made. The device must be reloaded manually to complete the software upgrade.
Canceled	The software upgrade request was interrupted, or a previous software upgrade request was bypassed from the CLI.
Update Failed	The software upgrade could not be completed. Troubleshooting is required; see the device system message log.

Software Upgrades by Device

Use this upgrade procedure for Service Broker and VDSMs. To upgrade your software on a single device, do the following:

Step 1 Choose **Devices > Devices**. The Devices Table page is displayed.

Step 2 Click the **Edit** icon of the device that you want to upgrade. The Devices home page is displayed.

Step 3 Verify that the device is not already running the version that you plan to upgrade to, and that the current version has an upgrade path to the version that you plan to upgrade to.

Step 4 Click **Update Software**. The Software Update page is displayed.

Step 5 Choose the software file URL from the Software Files list by clicking the radio button next to the filename.

Step 6 Click **Submit**, and then click **OK** to confirm your decision.

The Devices Table page is displayed again. You can monitor the progress of your upgrade from this page.

Software upgrade status messages are displayed in the Software Version column. These intermediate messages are also written to the system log on the Service Engines. See Table 7-1 for a description of upgrade status messages.

Rebooting Devices

You can reboot a device or device group. The VDSM performs a controlled shutdown of all devices and then restarts the operating system on each device.

To reboot an individual device, do the following:

Step 1 Choose **Devices > Devices**.

Step 2 Click the **Edit** icon next to the device name that you want to reboot. The Devices home page is displayed

Step 3 In the task bar, click the **Reload** icon. You are prompted to confirm your decision.

Step 4 To begin rebooting the device, click **OK**.

Deleting a Device

You can delete a device if the device is experiencing unresolvable problems or when its network address or configuration has changed and you need to add the device back to the VDS-SB network using its new address and configuration information.

Caution If you delete the only SB in your VDS-SB network, you are removing the ability of your VDS-SB network to route requests to CDN.

Removing the device from the VDS-SB network involves using the CLI to shut down VDS-SB network services and deregister the node. If you are removing the device because of hardware failure and it cannot be accessed through its CLI, you can remove the device by using the VDSM; however, the device continues to store its registration information until you deregister it by using the CLI.

Before a device can be removed from the VDS-SB network, the following conditions must be met:

- Device must have been activated in the VDSM.
- VDSM must be operating.
- Device must have the correct VDSM IP address or hostname configured.
- VDSM IP address or hostname must be that of the primary VDSM.

Deleting a device from the VDS-SB network involves using the CLI to remove the registration information from the device itself and removing the registration record from the VDSM.

Note Do not use the VDSM to delete a device while the device is still active and registered. The VDSM delete feature removes only the device's registration record from the VDSM; it does not deregister the device. The device retains its registration information and continues to contact the VDSM; however, the VDSM no longer recognizes the device.

If for some reason the VDSM loses the registration record of a device, use the **cms deregister force** command on the device to remove all its registration information. Then use the **cms enable** command to reregister the device with the VDSM as though it were a new node in the VDS-SB network.

To remove and deregister a device, do the following:

Step 1 Open an SSH session to the device CLI.

Step 2 In global configuration mode, enter the **no cms enable** command.

```
SB# configure
SB(config)# no cms enable
```

Note Issuing the **no cms enable** command does not disable acquisition and distribution services on the device; however, issuing the **cms deregister** command does. The **cms deregister** command disables the CMS, all acquisition and distribution services, and all routing communications to and from this device.

Step 3 In EXEC mode, enter the **cms deregister** command.

```
SB(config)# exit
SB# cms deregister
```

Step 4 If for some reason the deregistration fails, you can force the deregistration by using the **cms deregister force** command.

```
SB# cms deregister force
```

Note Take note of any messages stating that the deregistration failed and make sure to resolve them before reregistering the device with the same VDSM or registering the device to another VDSM. The **cms deregister force** command forces the deregistration to continue.

Step 5 To add the device back into the VDS-SB network, reregister the device with the VDSM by using the **cms enable** command in global configuration mode.

```
SB# configure
SB(config)# cms enable
```

In case of a hardware failure, you might need to remove the device from the VDS-SB network routing scheme by using the VDSM.

Before a device can be removed from the VDS-SB network through the VDSM, the following conditions must be met:

- Device must have been activated in the VDSM.
- VDSM must be running.
- Device must have the correct VDSM IP address or hostname configured.
- VDSM IP address or hostname must point to the primary VDSM.
- Device must not be the Acquisition Node for any origin service.

To delete a device using the VDSM, do the following:

Step 1 Choose **Devices > Devices**. The Devices Table page is displayed. The online status of the device is listed in the Status column.

Step 2 Click the **Edit** icon next to the device name you want to delete. The Devices home page is displayed.

Step 3 In the task bar, click the **Delete Device** icon. You are prompted to confirm your decision.

Step 4 To execute your request, click **OK**. The device is removed from the VDSM.

Step 5 If possible, access the device CLI to deregister the device.

Step 6 In the CLI, enter the **cms deregister force** command.

Note You must use the **cms deregister force** command after deleting a device in the VDSM. This is because once the device has been deleted, the VDSM no longer has a record of the device.

Step 7 To add the device back in to the VDS-SB network, reregister the device with the VDSM by using the **cms enable** command in global configuration mode.

Deleting a Warm Standby VDSM

You can delete a warm standby VDSM from the VDS-SB network at any point after you have registered the device and before the device has come online as the primary VDSM. Once the device has been called into use as the primary VDSM, however, you cannot delete it by using the VDSM.

Delete a warm standby VDSM when the device is experiencing unresolvable problems or when its network address or configuration has changed and you need to add the device back to the VDS-SB network by using its new address and configuration information.

To delete a warm standby VDSM, do the following:

Step 1 Log in directly to the VDSM CLI, and enter the **cms deregister** command.

If for some reason the deregistration fails, you can force the deregistration by using the **cms deregister force** command.

Step 2 From the VDSM GUI, choose **Devices > Devices**.

The browser refreshes, listing the VDSMs on your VDS-SB network. The warm standby VDSM is identified as *Standby*.

Step 3 Click the **Edit** icon next to the name of the warm standby VDSM. The Devices home page is displayed.

Step 4 From the left-pane menu, choose **Device Activation**. The Activation page is displayed.

Step 5 In the task bar, click the **Delete** icon. You are prompted to confirm your decision.

Step 6 To execute your request, click **OK**.

Replacing a Device

The procedure to replace a device in the VDS-SB is different depending on the type of the device being replaced. This section covers the following procedures:

- Replacing a VDSM
- Replacing a VDS-SB

Replacing a VDSM

To replace a VDSM in a VDS-SB you must first add the new VDSM into the network as a standby VDSM. For procedural information, see the "Configuring Primary and Standby VDSMs" section on page 2-8.

Note The primary and standby VDSMs must be running the same version of software. You must first add the new VDSM with the same version as the existing VDSM. Once the standby VDSM has been added, you must wait at least two polling intervals (10 minutes) for the databases to synchronize before you can begin the upgrade procedure.

Note After you have activated the standby VDSM using the primary VDSM web interface and the device shows as online in the Devices Table page, wait at least two polling intervals (10 minutes) before changing roles to ensure that the standby VDSM has a record of the most recent configuration changes.

To promote the standby VDSM to primary, first stop the primary VDSM using the **VDSM role standby** command. For procedural information, see the "Changing a Standby to a Primary VDSM" section on page 2-9.

After the primary VDSM has been stopped, and the standby VDSM has taken the role of primary, wait at least two polling intervals (10 minutes) before logging in to the new primary VDSM. The new primary VDSM is accessible by entering the IP address of the VDSM with port 8443 in a web browser. For example, if the IP address of your VDSM is 192.168.0.236, enter **https://192.168.0.236:8443**.

It is now safe to deactivate the old primary VDSM in the VDSM web interface and remove it from the VDS-SB network.

Note Do not try to take a back up of the old VDSM database and restore it on the new VDSM. This may lead to problematic issues.

Replacing a VDS-SB

To replace an SB, do the following:

Step 1 Open an SSH session to the device being replaced.

Step 2 In global configuration mode, enter the **no cms enable** command to disable CMS on the device that needs to be replaced.

```
SE# configure
SE(config)# no cms enable
```

Step 3 From the VDSM, choose **Devices > Devices > Device Activation**. The Device Activation page is displayed.

Step 4 Uncheck the **Activate** check box and click **Submit**. The page refreshes and displays a **Replaceable** check box.

Step 5 Check the **Replaceable** check box and click **Submit**.

Step 6 Choose **System > Configuration > System Properties**. The System Properties page is displayed.

Step 7 Click the edit icon next to the **System.devivce.recovery.key** property. The Modify Config Property page is displayed.

Step 8 In the **Value** field, enter a key and click **Submit**. The default value is default.

Step 9 Follow the instructions for configuring a device using the setup utility.

Note The replacement device must be the same hardware model as that of the device being replaced.

a. When prompted by the setup utility, configure the basic network settings.

b. When prompted by the setup utility for the hostname of the new device, use the same hostname of the device being replaced.

c. When prompted by the setup utility for the IP address of the VDSM, enter the IP address of the VDSM.

Step 10 Open an SSH session to the new device.

Step 11 In EXEC mode, enter the **cms recover identity** command with the key parameter you set in Step 8.

```
SB# cms recover identity <key>
```

On successful registration to the VDSM, a message similar to the following is displayed:

```
DT-7326-4#cms recover identity sr
Registering this node as Service Broker...
Sending identity recovery request with key sr
Node successfully registered with id CrConfig_291
Registration complete.
```

Step 12 Register the device with the VDSM by using the **cms enable** command in global configuration mode.

```
SB# configure
SB(config)# cms enable
```

Step 13 From the VDSM, choose **Devices > Devices > Device Activation**. The Device Activation page is displayed.

Step 14 Check the **Activate** check box and click **Submit**.

After a few minutes, approximately two polling intervals, the device status shows online and all configurations (origin service assignments, programs, and so on) are the same as those on the device that was replaced.

Step 15 Once the new device is up and running, as noted by the online status, the old device can be removed from the VDS-SB network.

Backup and Recovery Procedures

This section provides VDSM database backup and VDS-SB software recovery procedures. This section contains the following sections:

Performing Backup and Restore on the VDSM Database

The VDSM stores VDS-SB network-wide device configuration information in its Centralized Management System (CMS) database. You can manually back up the CMS embedded database contents for greater system reliability.

To back up the CMS database for the VDSM, use the **cms database backup** EXEC command.

Note The naming convention for backup files includes the timestamp.

To back up and restore the CMS database on the VDSM, do the following:

Step 1 Back up the CMS database to a file.

```
SB# cms database backup
creating backup file backup-db-11-06-2007-13-10.dump
backup file local1/backup-db-11-06-2007-13-10.dump is ready.
Please use 'copy' commands to move the backup file to a remote host.
```

Step 2 Save the file to a remote server by using the **copy disk ftp** command. This command copies the file from the local disk to a remote FTP server, as shown in the following example:

```
SB# cd /local1
SB# copy disk ftp 10.86.32.82 /incoming sb-db-9-22-2002-17-36.dump
sb-db-9-22-2002-17-36.dump

Enter username for remote ftp server:ftp
Enter password for remote ftp server:*******
Initiating FTP upload...
Sending:USER ftp
10.86.32.82 FTP server (Version wu-3.0.1-18) ready.
Password required for ftp.
Sending:PASS *******
User ftp logged in.
Sending:TYPE I
Type set to I.
Sending:PASV
Entering Passive Mode (10,86,32,82,112,221)
Sending:CWD /incoming
CWD command successful.
Sending PASV
Entering Passive Mode (10,86,32,82,203,135)
Sending:STOR sb-db-9-22-2002-17-36.dump
Opening BINARY mode data connection for sb-db-9-22-2002-17-36.dump.
Transfer complete.
Sent 18155 bytes
```

Step 3 Delete the existing CMS database.

```
SB# cms database delete
```

Step 4 Restore the CMS database contents from the backup file.

```
SB# cms database restore sb-db-9-22-2002-17-36
```

Step 5 Enable CMS.

```
SB# cms enable
```

Using the Cisco VDS-SB Software Recovery CD-ROM

A software recovery CD-ROM image (.iso file) is available for each software release. The recovery CD-ROM can be used to recover system software that must be completely reimaged. The recovery CD-ROM image contains the system software for a single software release and a single application software.

This section presents instructions for creating and using the software recovery CD-ROM to reinstall your system software if for some reason the software that is installed has failed.

Caution If you upgraded your software with a later release than the software recovery CD-ROM image file you downloaded, using the CD-ROM software recovery images may downgrade your system.

System Software Components

Cisco VDS-SB software consists of three basic components:

- Disk-based software
- Flash-based software
- Hardware platform cookie (stored in flash memory)

All these components must be correctly installed for Cisco VDS-SB software to work properly.

The software is contained in two types of software images provided by Cisco:

- A .bin image containing disk and flash memory components

  An installation containing only the VDS-SB flash memory-based software, without the corresponding disk-based software, boots and operates in a limited mode, allowing for further disk configuration before completing a full installation.

- A .sysimg image containing a flash memory component only

  The .sysimg component is provided for recovery purposes, and allows for repair of flash memory only, without modifying the disk contents.

Getting the Cisco VDS-SB Software Recovery File from Cisco.com

To get a software file from Cisco.com, do the following:

Step 1 Launch your web browser and enter the following URL:

http://www.cisco.com/cisco/software/navigator.html

The Select a Product page is displayed if you have recently logged in; otherwise, the Log In page is displayed.

Step 2 Log in to Cisco.com using your designated username and password.

Step 3 Choose **Products > Video > Videoscape > Cisco Videoscape Distribution Suite > Cisco Videoscape Distribution Suite Service Broker**. The Downloads page is displayed.

Step 4 Click the link for the software recovery file you want to download.

- If this is the first time you have downloaded a file from Cisco.com, the Cisco Systems Inc., Encryption Software Usage Handling and Distribution Policy is displayed. Read the policy, fill in the unfilled fields, and click **Accept**.

- If you previously filled out the Encryption Software Usage and Handling and Distribution form, the form does not display again.

The Download page is displayed with the information about the software image file and a Download link.

Step 5 Click **Download**. The Cisco End User Software License Agreement is displayed.

Step 6 Read the agreement and click **Agree**. The File Download dialog box is displayed.

Step 7 Click **Save**. The Save As dialog box is displayed.

Step 8 Navigate to the location where you want to save the file and click **Save**. The file downloads.

Step 9 Burn the software recovery image file onto a CD-ROM.

Installing the Software Using the Recovery CD-ROM

To install the system software by using the recovery CD-ROM, perform the following steps:

Step 1 Power off the Virtual Machine.

Step 2 Insert the recovery software CD-ROM into the CD-ROM drive, and boot the device.

Step 3 When the installer menu appears, choose **2 Install all Software**.

Step 4 Wait for the process to complete.

Step 5 Before you reboot the device, remove the CD-ROM drive from the USB port so that the device boots from flash memory.

Step 6 Reboot the device.

Recovering a Lost Administrator Password

If an administrator password is forgotten, lost, or misconfigured, you need to reset the password on the device.

Note There is no way to restore a lost administrator password. You must reset the password to a new one, as described in this procedure.

To reset the password, do the following:

Step 1 Establish a console connection to the device and open a terminal session.

Step 2 Reboot the device.

While the device is rebooting, watch for the following prompt and press **Enter** when you see it:

```
Cisco VOS boot:hit RETURN to set boot flags:0009
```

Step 3 When prompted to enter bootflags, enter the **0x800** value.

```
Available boot flags (enter the sum of the desired flags):
0x0000 - exit this menu and continue booting normally
```

```
0x2000 - ignore Carrier Detect on console
0x4000 - bypass nvram config
0x8000 - disable login security

[SB boot - enter bootflags]:0x8000
You have entered boot flags = 0x8000
Boot with these flags? [yes]:yes

[Display output omitted]
Setting the configuration flags to 0x8000 lets you into the system, bypassing all
security. Setting the configuration flags field to 0x4000 lets you bypass the NVRAM
configuration.
```

Step 4 When the device completes the boot sequence, you are prompted to enter the username to access the CLI. Enter the default administrator username (**admin**).

```
Cisco Service Broker Console

Username: admin
```

Step 5 When you see the CLI prompt, set the password for the user using the **username password** command in global configuration mode.

```
SB# configure
SB(config)# username admin password 0 password
```

You can specify that the password be either clear text or encrypted. Zero (0) means the password is displayed as a plain word; one (1) means the password is encrypted.The password strength must be a combination of alphabetic character, at least one number, at least one special character, and at least one uppercase character.

Note Do not set the user ID (uid).

Step 6 Save the configuration change by using the **write memory** command in EXEC mode.

```
SB(config)# exit
SB# write memory
```

Step 7 Optionally, reboot your device by using the **reload** command.

```
SB# reload
```

Rebooting is optional; however, you might want to reboot to ensure that the boot flags are reset, and to ensure that subsequent console administrator logins do not bypass the password check.

Note In VDS-SB software, the bootflags are reset to 0x0 on every reboot.

Recovering VDS-SB Network Device Registration Information

Device registration information is stored both on the device itself and on the VDSM. If a device loses its registration identity or needs to be replaced because of hardware failure, the VDS-SB network administrator can issue a CLI command to recover the lost information or, in the case of adding a new device, assume the identity of the failed device.

To recover lost registration information, or to replace a failed node with a new one having the same registration information, do the following:

Step 1 Mark the failed device as "Inactive" and "Replaceable" in the VDSM.

a. Choose **Devices > Devices**.

b. Click the **Edit** icon next to the name of the Service Engine you want to deactivate. The Devices home page is displayed.

c. From the left-panel menu, choose **Device Activation**.

d. Uncheck the **Activate** check box. The page refreshes, displaying a check box for marking the device as replaceable.

e. Check the **Replaceable** check box and click **Submit**.

Note This check box only displays when the device is inactive.

Step 2 Configure a system device recovery key.

a. Choose **System > Configuration**.

b. Click the **Edit** icon next to the System.device.recovery.key property. The Modifying Config Property page is displayed.

c. Enter a password in the **Value** field and click **Submit**. The default password is **default**.

Step 3 Configure the basic network settings for the new device.

Step 4 Open an SSH session to the device CLI and enter the **cms recover identity** *keyword* EXEC command, where *keyword* is the device recovery key that you configured in the VDSM.

When the VDSM receives the recovery request from the Service Engine, it searches its database for the Service Engine record that meets the following criteria:

- Record is inactive and replaceable.
- Record has the same hostname as given in the recovery request.
- Device is the same hardware model as the device in the existing record.
- File system allocations for the device are the same as or greater than the device in the existing record.

If the recovery request matches the Service Broker record, then the VDSM updates the existing record and sends the requesting Service Broker a registration response. The replaceable state is cleared so that no other device can assume the same identity. When the Service Engine receives its recovered registration information, it writes it to file, initializes its database tables, and starts.

Step 5 Return to the VDSM and activate the device.

a. Choose **Devices > Devices**.

b. Click the **Edit** icon next to the name of the Service Broker you want to activate. The Devices home page is displayed.

c. From the left-panel menu, choose **Device Activation**. The Service Broker status should be Online.

d. Check the **Activate** check box and click **Submit**.

Note If you are replacing an old device with a different hardware model, check the following hardware-related settings and adjust them according to your needs, after the new device is online in VDSM GUI:

- IP Access List settings associated with network interfaces
- Disk quota settings of origin services
- Service Monitor Disk Failure Percent Settings