SR 9.0 Installation and Migration Guide

Please Read

Important

Read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgments

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: **www.cisco.com/go/trademarks**.

Third party trademarks mentioned are the property of their respective owners.

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing or later issued patent.

Copyright

Contents

About This Guide

Purpose

This guide provides step-by-step instructions for the following System Release (SR) 9.0 installation scenarios.

- Initial installation of SR 9.0
- Migration from SR 8.0/7.x to SR 9.0
- Upgrade to a newer version of SR 9.0

SR 9.0 Features Forklift Migration

The upgrade involves the migration from either SR 8.0/7.x to SR 9.0 on the CentOS version 7.4 Linux platform. The migration to SR 9.0 allows engineers to migrate the system without having to shut the system down until the activation of the new system software.

Cisco engineers have expended great effort to make sure that the migration causes minimal system impact. However, there are times during the migration where Digital Home Communication Terminals (DHCTs) will not be able to boot and where some functions (Broadcast File System [BFS], billing system control of set-top-boxes [STBs], and so on) are interrupted. These outages will likely go unnoticed by most of your subscribers.

How Long to Complete the Migration?

The migration to SR 9.0 is completed within a maintenance window that usually begins at midnight. Engineers have determined that a typical site can be upgraded within one 6-hour maintenance window. The maintenance window should begin when you stop system components in ***Migrate the Key Files and Database to SR 9.0*** (on page 69).

System Performance Impact

Interactive services are not available and billing transactions will be suspended during the maintenance window.

Audience

This guide is written for field service engineers and system operators who are responsible for creating virtual machines (VMs) and installing, migrating or upgrading to SR 9.0.

Read the Entire Guide

Please review this entire guide before beginning the installation. If you are uncomfortable with any of the procedures, contact Cisco Services for assistance.

Important: Complete all of the procedures in this guide in the order in which they are presented. Failure to follow all of the instructions may lead to undesirable results.

Required Skills and Expertise

System operators or engineers who upgrade the Explorer Controller (EC) software need the following skills:

- Advanced knowledge of Linux.
  - Experience with the vi editor. Several times throughout the system upgrade process, system files are edited using the vi editor. The vi editor is not intuitive. The instructions provided in this guide are no substitute for an advanced working knowledge of vi.
  - The ability to review and edit cron files.
- Knowledge of VMware.
- Extensive EC and DBDS system expertise.
  - The ability to identify keyfiles that are unique to the site being upgraded.
  - The ability to add and remove user accounts.

Revisions

Date	Section Updated or Added
20181219	■ ***Software Requirements*** (on page 7) ■ ***Migrating the Database and Key Files*** (on page 73)
20190121	■ ***Hardware*** (on page 2) ■ ***Reset the Password for the admin User*** (on page 245)
20190228	■ ***Creating an Admin User on the SR 7.x System*** (on page 64) ■ ***Update the Network Post-Application Installation or Post-Migration*** (on page 77) ■ ***CentOS cron and anacrontab Overview*** (on page 135) ■ ***Verifying the crontab Entries Managed by cron*** (on page 138) ■ ***Adding the IPG Collector Crontab Entry*** (on page 140) ■ ***Adding Site-Specific crontab Entries*** (on page 141)
20190426	■ ***Promoting the Upgraded Secondary VM to the New Primary VM*** (on page 211) ■ ***Configuring the VM as the New Secondary System*** (on page 216)

Document Version

This is the first formal release of this document.

1

Planning the Install or Migration

Introduction

This chapter contains information that helps you and Cisco engineers plan the installation or migration to minimize system downtime.

In This Chapter

Site Requirements

Your site requires the following requirements. Ensure that these requirements are met prior to deploying virtual machines.

Hardware

This section provides guidelines, recommendations and requirements for your NextX SR 9.0 system.

General Guidelines

The following list provides general guidelines for the SR 9.0 EC hardware.

- Cisco cannot validate co-residency combinations of Cisco application VMs and non-Cisco VMs running on the same hosts; therefore, Cisco application performance guarantees cannot be provided. However, by configuring the system as outlined in this section, Cisco applications should perform per expectations, and if not, Cisco can work with you on determining a root cause.
- Cisco used a specific ***Test Reference Configuration*** (on page 4) (TRC) to verify performance on the SR 9.0 EC.
- Since it was not feasible to test all system configurations and loads, Cisco applied a high transaction load to a system configured with a high number of elements as shown in the **System Configuration for the EC Test Configuration** table in ***System Configuration*** (on page 5).
- The Virtualization Resource Requirements are the same regardless of whether the server configuration is per the TRC or a non-TRC. Cisco verified that the product successfully handled the high transaction load when provided the VM resources as shown in the **System Load** table in ***System Configuration*** (on page 5).
- In order to ensure performance, Cisco mandates no over-subscription of platform resources. Further details are provided for each component of the hardware as documented in this section.

CPU Guidelines

The following guidelines apply to the CPUs (central processing units) that will be configured on the SR 9.0 VM:

- There is no over-subscription rule for CPUs. You must a have one-to-one correspondence of a virtual CPU (vCPU) to a physical CPU (pCPU).
- Hyperthreading is recommended; however, logical CPUs (lCPU) cannot be used for vCPU quantities.
- Cisco did not verify CPU architectures other than what is specified in the ***Test Reference Configuration*** (on page 4).
- VMware CPU affinity must be disabled.

Memory Guidelines

The following guidelines apply to the memory that will be configured on the SR 9.0 VM:

- There is no over-subscription rule for memory. The sum of vRAM of all VMs must be less than the total physical RAM of the host.
- You must adhere to the VMware memory overhead guidelines to ensure that the host has sufficient additional physical memory for the ESXi host and the VM overhead.

Storage Guidelines

The following guidelines apply to the storage that will be configured on the SR 9.0 VM:

Note: These guidelines apply to direct attached storage (DAS), network attached storage (NAS) and storage area network (SAN) devices.

- **Storage Quantity**
  - There is no over-subscription rule for storage:
    - You must map 1 GB of VM vDisk to 1 GB of physical storage.
    - The sum of virtual machines' vDisks may not exceed the physical disk space of the physical server's logical volume capacity (i.e. capacity net of overhead for the VM itself, VMFS in vSphere and physical RAID configuration).
  - Storage thin provisioning is not recommended at the VM layer or the storage array layer.
  - The total storage allocated per product includes vDisk + swap size (which is equal to the physical vRAM).

- **Performance**
  - There must be sufficient input/output operations per second (IOPS) to handle the sum of the VMs running on each host.
  - IO wait time should not be consistently above 20 ms; however, intermittent spikes above 20 ms are not a concern.

Network Guidelines

The following guidelines apply to the network that will be configured on the SR 9.0 VM:

- There is no over-subscription rule for the network. The aggregate networking load of the co-resident virtual machines must be met with the physical networking interface(s) on the host.
- Deployments leveraging non-FC-storage (iSCSI, NFS or Unified Fabric/FCoE including UCS B-Series FEX) must account for network traffic from both the VM LAN access and the VM storage access.

Test Reference Configuration

Platform Hardware Specifications

The following table lists the platform hardware specifications used in the TRC.

Platform	Form Factor and Physical Specifications
UCS C240 M3S	■ 2RU rack-mount server ■ Dual E5-2690 (16 total physical cores, 2.899 GHz) ■ 128 GB RAM ■ 16 x 300 GB 15K RPM drives (14 x drives form a RAID10 group + 2 hot spares) ■ Network ports – Chassis: ▪ 1 10/100/1000 RJ-45 management port ▪ Quad 1Gb ports – PCIe: 2 Quad 1Gb port NICs

Platform Software Versions

The following table lists the platform software versions used in the TRC.

Platform Software	Version
UCS Firmware	3.0(4j)
ESXi Host	6.0.0-20170604 (U3a)

System Configuration

This section provides the relevant system configuration used in the TRC.

System Configuration for the EC Test Configuration

Parameter	Value
Versions	■ **EC**: 9.0.12-1.201809061741 (Informix: 12.10.FC8W1-3) ■ **TED IV**: SAIted-4.0.1.0-1 (crossover cable)
DHCTs in database	10,250,871
EMMs in database	27932755 (equivalent to 4M IS2W DHCTs at 7 EMMs/DHCT)
QPSK/DSG Bridges	194
QAM devices	948 GQAMs
Service Groups	6148
In-Band BFS	36 Mbps
Out-of-Band BFS	104 Mbps (cumulative)
CF Sessions	18,929
Hubs	75
Sources	579
SI generating Source Definitions	16,964

System Load (with a 100% response rate)

Load Name	Description
Back office/BOSS	■ 60 transactions/sec ■ Transaction type: modDhctConfiguration
DHCT Sign-On	200 requests/sec
VOD encrypted sessions	80 requests/sec
Debug Configuration	EC processes under load set to "debug"

Virtual Resource Requirements

The following table lists the resource requirements for each SR 9.0 VM.

Parameter	Values
Number of CPUs	8 x 2900 MHz
Memory	64 GB
Average IOPS (input/output operations per second defined in "transactions per second" [tps])	2220 tps
Disk Storage	**VM Disk Storage** ■ Disk1 (sda): 64 GB ■ Disk2 (sdb): 512 GB **Swap File Storage** ■ 64 GB
Average Network Utilization for each IP interface	■ ens192 (back office): <1 Mbps ■ ens224 (dncsatm): 150 Mbps ■ ens256 (TED): 2 Mbps ■ ens161 (RepDB): 15 Mbps

Software Requirements

The following software prerequisites are required for an SR 9.0 installation.

- VMware vSphere (6.0u1 or later) and vCenter infrastructure (software, license, and a running vCenter machine).
  - vSphere Web UI 6.0 is used for the procedures and examples throughout this guide.
- A VMware vCenter 6.0 Web UI or a VMware vSphere 6.0 client login to connect and perform management tasks.
  - vCenter login must have admin privileges to deploy VMs.
- Admin Node installed (refer to the ***Admin Node 2.0 Installation Guide***).
- Linux platform template saved via vCenter Server (created from a procedure in the ***Admin Node 2.0 Installation Guide***).
- Admin Node access to copy the following files to your VM:
  - cisco-vcs-deployment-2.0.4.zip
  - ec-system-release- 9.0.14-1-201903251331.tar
  - cisco-vcs-infra-2.0.5.tar
  - SSL certificates created for each unique SR 9.0 EC node
- Migration only:
  - You are currently running SR 8.0/7.x.
  - EC Backup and Restore scripts available from Cisco.
  - EC pre-upgrade checks TAR file (e.g. ecpuc_8.0.4.tar) available from your customer-specific forum on Cisco's File Exchange Server.
  - You have a complete list of all third-party tools and scripts currently in use on the EC.
  - You have a complete list of key files and directories where you store site-specific information that you want to keep, such as:
    - EMM files
    - Log files
    - Scripts
    - Service logo files or MSO logo files

    Note: No files on the active EC are deleted as part of the migration.

- Putty version 0.7.1 or later (required for the CentOS 7.4 platform)
- DTACS 5.2 is supported.
- At least one external Network Time Protocol (NTP) server, version 4.x or later, configured and accessible on the network.

Web Browser Requirements

The Web UIs have been tested and verified against Mozilla Firefox version 50 and ESR version 52.1 browsers. Due to unpredictable results with other browsers, we highly recommend that you only use Mozilla Firefox on your system when you work with the EC.

X.509 CA Certificate and Associated Private Key Requirements

Important: During the installation and configuration of the Admin Node, you should have created an internal root CA or configured for an external CA. You should have created environment (.env) files for each node in your NextX system. If you configured the Admin Node for an external CA then you should have also generated the certificate files for each node in your NextX system. If you have not created these files, refer to Chapters 5 through 6 in the ***Admin Node 2.0 Installation Guide*** to create them now.

Each EC node in your NextX system requires a NextX X.509 certificate along with an associated private key. The X509 certificates must be signed by a Certification Authority (CA). The CA can be either an external entity or an internal CA.

Using this guide, and dependent upon your certificate authority, you will perform one of the following tasks:

- **Internal Certificate Authority**
  - Generate and install HTTPS X.509 certificates for the EC using an internal root CA
  - Configure the certificate/key pairs on the EC
- **External Certificate Authority**
  - Configure the certificate/key pairs on the EC

SSH Availability with CentOS 7

Due to the security features in CentOS 7.4, you will not be able to SSH from nodes running CentOS 6.x to nodes running CentOS 7.4. However, backward compatibility is permitted which allows you to SSH from nodes running CentOS 7.4 to nodes running CentOS 6.x.

Additional IP Address and NAS Interface Requirements

In addition to inheriting all of the IP address of the existing EC, the SR 9.0 EC will require the following additional IP addresses.

- Static IP address (for access to the Admin Node).
- IP address for the Network Attached Storage (NAS) interface (if a dedicated interface will be used).

  Notes:

  - The ESXi/EC does not support backing up to tape. Backups of the key files and the database are performed to the NAS.
  - VM cloning is also an option to save a full file system backup; however, you must have vSphere to do so.

Accessing the root and dncs User Accounts

Important:

- Role-Based Access Control (RBAC) is not supported in SR 9.0. Please follow the steps below to switch between different user accounts.
- The **ecadmin** user is used in examples for all Cisco DBDS documents pertaining to EC 8.0 or later.
- Commands run as **root** user are shown with a **#** symbol.

  Example:

  ```
  [root@ecnextx9 ~]#
  ```

- Commands run as an **admin**, **dncs**, or any **Administrator** user are shown with a **$** symbol.

  Example:

  ```
  [admin@ecnextx9 ~]$
  [ecadmin@ecnextx9 ~]$
  [dncs@ecnextx9 ~]$
  ```

Once the EC application installation is complete, you can only log in with the **admin** user account.

The ***admin*** account is created by default during the installation, and is granted privileges to access the root user account, as root login is not permitted. These privileges allow the admin user to execute root commands by preceding the command with "sudo". For example, if you want to modify a network configuration file, the command will resemble the following:

Example: Executing a root command as admin user:

```
[admin@ecnextx9 ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-ens192
```

As **admin** user, you can also change to the root user account by entering the following command.

Important: For any procedure in this guide that states "As root user", you must be logged into a terminal window as admin user and switch to the root user.

Command syntax: Changing to root user:

```
[admin@ecnextx9 ~]$ sudo –i
```

Any ***Administrator*** account that you create using the useradmin script (see the next section) has privileges to log into the EC from a terminal window. Administrator accounts do not have privileges to access the root user account, but should be used to access the dncs user account.

Important: Do not access the dncs user account using the root user account.

To switch to the **dncs** user, type the following command from the terminal window where you are logged in as an Administrative user.

Important: For any procedure that states "As dncs user", you need to execute this command from the terminal window where you are logged in with your Administrator account.

Command syntax: Changing to the dncs user:

```
[ecadmin@ecnextx9 ~]$ sudo su – dncs
```

Overview:

Terminal Window Logged in as:	Use Account to change to:	Command to execute:
admin	root	sudo -i
[Administrator] **Example:** ecadmin	dncs	sudo su - dncs

About the EC Pre-Upgrade Checks Scripts

The purpose of the EC pre-upgrade checks (EC PUC) scripts is to perform pre-upgrade checks related to the EC that you are migrating or upgrading to SR 9.0 to ensure that it is seamless and successful.

The EC PUC scripts are packaged in the ecpuc_[VERSION].tar (for example, ecpuc_8.0.4.tar) file. The tar file must be downloaded from your customer-specific forum on Cisco's File Exchange Server and then saved to a shared (NFS) storage device accessible by the EC.

The EC PUC validates your system for migration eligibility. These scripts should be run two or more weeks prior to your migration/upgrade to allow enough time to resolve any major issues or incompatibilities that may affect your ability to upgrade the EC. The EC PUC should be run again just before your migration/upgrade to validate the system.

Important: The EC PUC scripts must be run on each EC that will be migrated or upgraded.

Important Points About the Upgrade

Performance Impact

Interactive services will not be available and billing transactions will be suspended while you are within the maintenance window after EC processes are stopped.

Estimated Timeline

Estimated Time to Complete the Upgrade

The upgrade to SR 9.0 features the forklift upgrade, which provides the ability to stage the Cisco UCS server with the upgraded operating system and application software before entering the maintenance window.

Most sites should be able to complete an upgrade within a typical 6-hour maintenance window. However, depending on the size of your system, it could take longer. Key factors are the size of your database and the number of headend elements.

Post-upgrade procedures involve resetting the modulators. Cisco recommends that you never reset more than eight modulators at a time. Refer to the following table for estimated times for resetting the modulators.

Number of Modulators	Minutes (approx. 4 minutes per modulator, 8 at a time)
60	30 to 38
100	50 to 63
150	75 to 94
200	100 to 125
250	125 to 157

Non-Cisco Application Server and/or Third Party Application Servers

If the site you are upgrading supports a non-Cisco application server, contact the vendor of that application server to obtain upgrade requirements, and upgrade and rollback procedures.

If the site you are upgrading runs a third-party software application, contact the supplier of that application to obtain any upgrade requirements.

Important: Make sure that all third-party vendors are aware that the SR 9.0 upgrade is built upon the CentOS 7.4 (x86) software platform.

Plan What Optional Features Will be Supported

Optional Features in SR 9.0

An upgrade can contain additional optional features that you can enable on your system. Some of these features require that you obtain a special license for the feature to be activated; others can simply be activated by Cisco engineers without a special license.

Determine which optional features (licensed or unlicensed) need to be enabled as a result of this upgrade. You can activate these optional features later during the upgrade, while the system processes are down.

If any licensed features are to be enabled as a result of this upgrade, contact Cisco Services to purchase the required license.

Important:

- If this is a new install to SR 9.0 and features need to be enabled, contact Cisco Services.
- Any features that have been previously enabled or licensed as part of an earlier upgrade do not have to be re-enabled.
- If the upgraded system that is to support any of the following new features, Cisco Services needs to enable the feature. Contact Cisco Services.
  - Remote PHY Support
  - Network TED Support
  - BFS-QAM Dependency Removal
  - VDCM Support

2

System Release Pre-Upgrade Checks

Important: If this is a new SR 9.0 installation, skip this chapter and go to ***Deploy the EC Virtual Machine*** (on page 29).

This chapter describes the procedures that must be completed prior to migrating or upgrading to SR 9.0.

In This Chapter

Preparing to Run the Pre-Upgrade Checks Script

Complete the following steps to download and extract the EC pre-upgrade checks (ecpuc) tar file to the SR 8.0/7.x system.

Note: Although the commands in the examples are for an SR 8.0 EC, the commands are the same for any SR version you are migrating from.

1 As **root** user, enter the following command to copy the ecpuc tar (for example, ecpuc_8.0.4.tar) file from your local PC to the **/var/tmp** directory on the active EC.

2 Enter the following command on the SR 8.0/7.x EC to extract the ecpuc tar file.

```
[admin@ecnextx8 tmp]$ tar -xvf ecpuc_8.0.4.tar
```

Results: The following directory and files are extracted.

- ECPUC/
- ECPUC/checkstrandedseg.sh
- ECPUC/del_nummap_dupes
- ECPUC/dncsDbCheckBoss
- ECPUC/ecpuc
- ECPUC/nondncsatmvasps.sh
- ECPUC/README

Checking the .profile Exit Status

In this procedure, you will check the exit status when sourcing the dncs user .profile settings. The exit status must be 0 (zero). If the status is not 0 upon exit, there is a problem in the .profile file that will prevent the EC processes from starting after the upgrade.

1 As **dncs** user, type the following command and press **Enter** to source the dncs .profile settings.

Notes:

- For SR 8.0 systems, make sure you are in the **/home/dncs** directory.
- For SR 7.x systems, make sure you are in the **/export/home/dncs** directory.

SR 8.0 system:

```
[dncs@ecnextx8 dncs]$ . ./.profile
```

SR 7.x system:

```
$ . ./.profile
```

2 Type the following command and press **Enter** to verify that the exit status from step 1 is **0** (zero).

```
echo $?
```

Result: The system displays the exit status of the command executed in step 1.

3 Is the exit status **0**?

- If **yes**, go to the next procedure in this chapter.
- If **no**, continue with the next step.

4 Open the dncs user **.profile** file in a text editor and review the file for problems. Check especially for the following condition:

If the last statement (bottom) in the .profile is an "unset" statement, verify that it unsets a variable that was set earlier in the .profile file. If it does not, remark or delete this entry, and repeat steps 1-3.

Note: If this solution does not produce an exit status of 0 in the dncs user .profile file, contact Cisco Services for assistance.

Checking the EAS Configuration

Before installing the new EC system release software, refer to the ***EC Online Help*** to verify that your EAS equipment is working correctly by testing the system's ability to transmit EAS messages.

Note: You will check the EAS configuration after the installation of the new software, as well.

Determining if the System Uses DSG BFS

In this section, you will determine whether or not your SR 8.0/7.x system is setup for DSG BFS. This information will be used during post-upgrade procedures if DSG BFS is configured on your system.

1 As **dncs** user, enter one of the following commands to verify if DSG BFS is defined on the system.

SR 8.0 system:

```
[dncs@ecnextx8 dncs]$ grep -i dncsdsg /home/dncs/.profile
```

SR 7.x system:

```
$ grep -i dncsdsg /dvs/dncs/bin/dncsSetup
```

2 Did **dncsdsg** display in the output?

- If **yes**, you must execute ***Modify the .profile File for DSG*** (on page 95) during the post upgrade procedures later in this guide.

  Note: Do not go to that procedure now. You will get there as a matter of course while following the procedures in this guide.

- If **no**, you will skip the ***Modify the .profile File for DSG*** procedure in the post-upgrade chapter.

Checking for the IPG_TVDATA_NEW Variable in appservSetup

Note: This procedure is executed on the SR 8.0/7.x EC.

Complete the following steps to check for the IPG_TVDATA_NEW variable in the appservSetup file.

1 As **dncs** user, type one of the following commands and press **Enter** to check for the "IPG_TVDATA_NEW" variable:

SR 8.0 system:

```
[dncs@ecnextx8 dncs]$ grep "IPG_TVDATA_NEW"
/dvs/appserv/bin/appservSetup
```

SR 7.x system:

```
$ grep "IPG_TVDATA_NEW" /dvs/appserv/bin/appservSetup
```

2 Is the IPG_TVDATA_NEW variable present?

- If **yes**, record the variable setting. You will need to put this variable back into the appservSetup file after the migration.
- If **no**, continue with the next procedure.

Checking the Number of BFS Sessions

The number of BFS sessions post-upgrade needs to equal the number of pre-upgrade sessions. Use this procedure to determine and record the number of pre-upgrade BFS sessions. Then, after the upgrade, you will determine the number of post-upgrade BFS sessions.

Follow this procedure to check and record the number of pre-upgrade BFS sessions.

1. Press the **Options** button on the front panel of the BFS QAM until the **Session Count** total appears.

   Record the **Session Count** total in the space provided. _____

2. As **dncs** user, enter the following command and press **Enter**.

   Command syntax:

   ```
   auditQam -query <QAM IP> <port #>
   ```

   Example — SR 8.0 system:

   ```
   [dncs@ecnextx8 dncs]$ auditQam -query 192.0.2.65 16
   ```

   Example — SR 7.x system:

   ```
   $ auditQam -query 192.0.2.65 16
   ```

3. Complete the following steps to check the number of BFS sessions directly from the GQAM device.

   a. Type the following command and press **Enter**.

      Command syntax:

      ```
      telnet [GQAM IP address]
      ```

      Example:

      ```
      $ telnet 192.0.2.65
      ```

   b. When prompted, enter the user name and password for the GQAM.

   c. Press the **Ctrl** and **]** keys simultaneously to go to the telnet prompt.

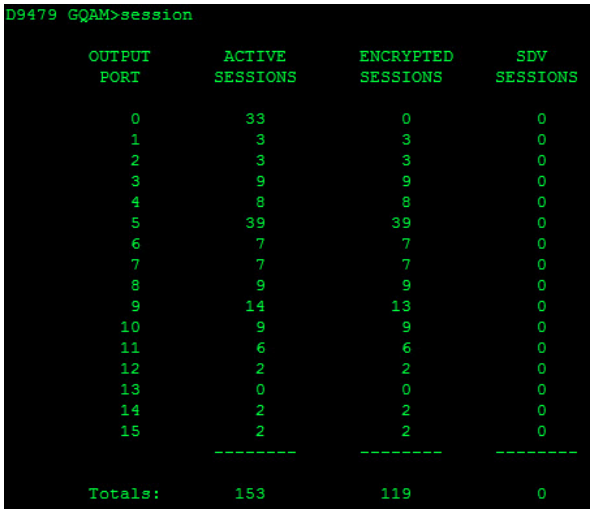
   d. Type the following command and press **Enter** twice.

      ```
      telnet> mode ch
      ```

e Type the following commands and press **Enter** after each to display the GQAM sessions on the specified port.

Example:

```
D9479 GQAM> session
```



```
D9479 GQAM>session

       OUTPUT       ACTIVE       ENCRYPTED      SDV
        PORT       SESSIONS      SESSIONS     SESSIONS

          0          33            0            0
          1           3            3            0
          2           3            3            0
          3           9            9            0
          4           8            8            0
          5          39           39            0
          6           7            7            0
          7           7            7            0
          8           9            9            0
          9          14           13            0
         10           9            9            0
         11           6            6            0
         12           2            2            0
         13           0            0            0
         14           2            2            0
         15           2            2            0
                   --------     --------     --------

       Totals:      153          119            0
```

Command syntax:

```
print_session_status <port #>
```

Example:

```
D9479 GQAM> print_session_status 0
```

Note: In this example, the BFS sessions are built on GQAM channel 1. The GQAM numbers ports 0 through 15; the EC numbers them 1 through 16.

Result: The system displays the BFS session built upon the specified IP address and port.

4 Do the number of sessions shown in steps 1 through 3 match the number of sessions built on the BFS QAM?

- If **yes**, go to the next procedure in this chapter.
- If **no**, contact Cisco Services for assistance.

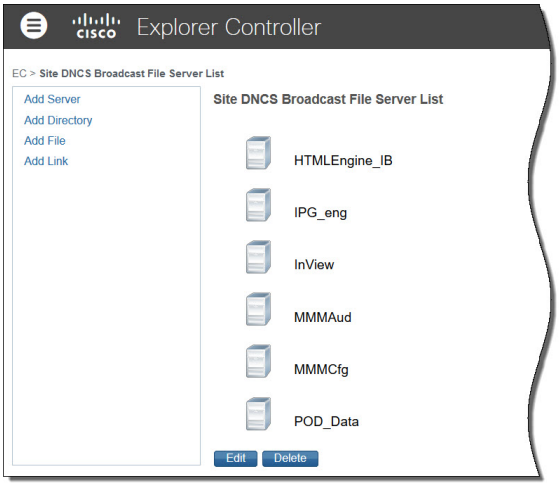
Recording Third Party BFS Application Cabinet Data

In this procedure, you will record third-party BFS application cabinet data so that you have a record of it in the event that the data is not preserved during the upgrade. Following the upgrade, during post-upgrade activities, you will confirm that this data has been preserved.

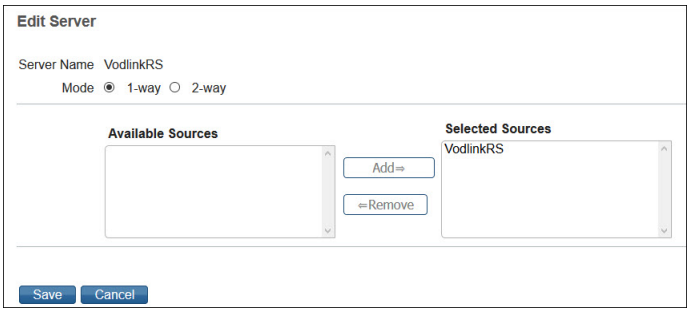
Note: You do not need to record this data for all BFS application cabinets, only those that are NOT created by default.

1 From the EC Web UI, execute one of the following options:

- **SR 8.0 system** — click the **Navigation** icon ( ) and then select **App Interface Modules > BFS Client**. The DNCS Broadcast File Server List window opens.
- **SR 7.x system** — click **Application Interface Modules > BFS Client**. The Site DNCS Broadcast File Server List opens.



2 Select a third-party application cabinet and select **Edit**. The Edit Server window opens for the selected cabinet.



3. On a sheet of paper, record the **Server Name**, the **Mode** (whether 1-way or 2-way), and the **Selected Source(s)** used to regulate the cabinet.

   Note: In this example, the **Server Name** is **VodlinkRS**, the **Mode** is **1-way**, and the **Selected Source** is **VodlinkRS**.

   Important: Do not lose this sheet of paper. You will need it when completing post-upgrade instructions.

4. Click **Cancel** to close the Edit Server window.
5. Record all folders, files, and link information in the cabinet, as needed.
6. Repeat steps 2 through 5 for each third-party BFS application cabinet in the Site DNCS Broadcast File Server List.
7. Close the Site DNCS Broadcast File Server List window when you are finished.

Running the EC PUC

This section describes how to run a system check on the SR 8.0/7.x EC to determine if the system is acceptable for an upgrade. If it is, you can continue with the upgrade; if it is not, you must correct any errors that are found and then rerun this procedure

Complete the following steps to execute the ecpuc script on the SR 8.0/7.x EC.

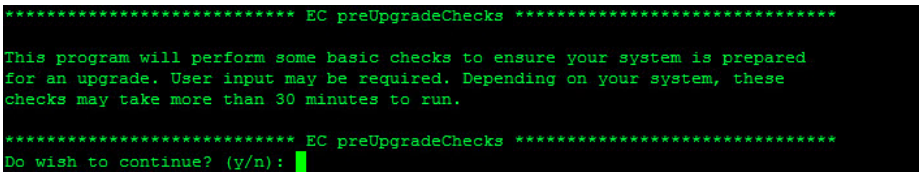
Note: Although the examples show command prompts for an SR 9.0 system, the commands are the same for SR 8.0/7.x ECs.

1. As **root** user, go to the **ECPUC** directory.

   ```
   [root@ecnextx8 ~]# cd /var/tmp/ECPUC
   ```

2. Enter the following command to execute the **ecpuc** script.

   ```
   [root@ecnextx9 ECPUC]# ./ecpuc
   ```

3. When prompted to continue with the preUpgradeChecks, type **y** and press **Enter**. The PUC begins the system checks and includes the following checks:
   - Runs a series of checks.
   - Clears completed database sessions.
   - Runs the doctor report.
4. Did any errors or warnings appear?
   - If **yes**, correct the issues and repeat this procedure.
   - If **no**, go to the next step.
5. Review the EC PUC log in **/var/log/preUpgradeChecks** directory for any errors or warnings.

   Command syntax:

   ```
   less /var/log/preUpgradeChecks/puclog_[date]_[time]
   ```

   Example:

   ```
   [root@ecnextx9 tmp]# less
   /var/log/preUpgradeChecks/puclog_201809426_103158
   ```

6. Did you run the EC PUC on a SR 7.x system?
   - If **yes**, go to the next step.
   - If **no**, go to step 8.

7 Is a warning about **.bashrc** present in the log?

- If **no**, go to the next step.
- If **yes**, make sure to complete the steps in ***Clean Up the .bashrc File*** (on page 116) during post installation instructions and before starting system processes.

8 Review the doctor output in the **/dvs/dncs/Utilities/doctor** directory for any errors or warnings.

Command syntax:

```
less /dvs/dncs/Utilities/doctor/report_[most recent].doc
```

Example:

```
[root@ecnextx9 tmp]#  less
/dvs/dncs/Utilities/doctor/report_16695.170924_1115.doc
```

9 Review all WARNINGS and ERRORS in the PUC and doctor output prior to upgrading your system.

Important: If the Distributed DNCS check ***does not*** pass and the following warning is present in any of the logs, contact Cisco Systems. They will then remove and disable Distributed DNCS from your system.

```
2018_04_26 170604: ------------------------------------------------------------------------
2018_04_26 170604: Distributed DNCS check WARNING.
2018_04_26 170604:
2018_04_26 170604: *** This system is currently licensed for the Distributed DNCS feature.      ***
2018_04_26 170604: *** The Distributed DNCS feature IS NO longer SUPPORTED in releases 8.0 and  ***
2018_04_26 170604: *** above.  Please ensure ALL RNCS systems are removed and licensing for     ***
2018_04_26 170604: *** this feature is disabled BEFORE UPGRADING.                               ***
2018_04_26 170604: *** Please call customer support if you have any questions.                  ***
2018_04_26 170604:
2018_04_26 170604: ------------------------------------------------------------------------
```

3

Deploy the EC Virtual Machine

Introduction

This chapter provides the procedure to deploy an EC VM from a Linux platform template. This template was created when the Admin Node was built. You will need the password for the admin user that was configured for this template.

Note: If you did not deploy and configure the Admin Node or the Linux platform template, ask your site administrator for the IP address and location of the Admin Node along with the admin password defined for the Linux platform template.

In This Chapter

Deploying the VM From the Linux Platform Template

Important:

- Execute this procedure for either a new install or a migration.
- If this is a migration, execute this procedure on the *secondary* EC.

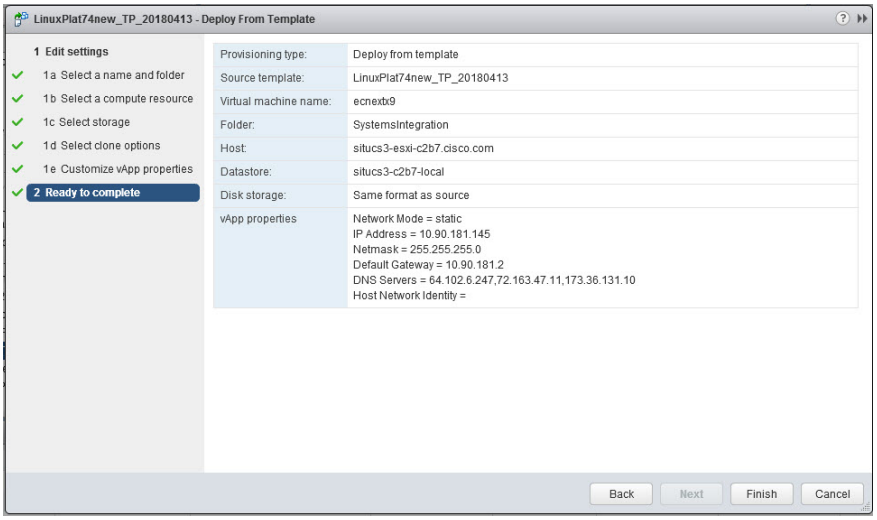
Follow these steps to deploy a VM from your Linux platform template.

Note: This procedure is written based on vSphere Web UI 6.0. If you are using a different version of the vSphere Web UI or if you are using vSphere client, the steps may differ.

1. From vCenter Web UI, click **VMs and Templates**.
2. Locate and select the **CSCOlxplat** template that was created from the procedures in the ***Admin Node 2.0 Installation Guide***.
3. Right-click the template and select **New VM from this Template**. The Select a name and folder window opens.
4. In the **Enter a name for the virtual machine** text box, type a name for the VM you are creating.
5. From the **Select a location for the virtual machine** area, select the datacenter or VM folder where the VM will reside. Click **Next**. The Select a compute resource view opens.
6. Select the compute resource (e.g. cluster, host) where the VM will run. A validation check occurs and when the compatibility succeeds message appears, click **Next**. The Select storage window opens.
7. From the **Select virtual disk format** dropdown menu, maintain the **Same format as source** selection.
8. Select the appropriate datastore to store the VM configuration files and virtual disks.
9. Click **Next**. The Select clone options window opens.
10. Click **Next**. The Customize vApp properties window displays.

    Important: Do ***not*** make any changes to fields in this screen as the ifcfg-ens192 configuration file defined on the Linux platform template overrides the settings in this window.
11. Click **Next**.

12 Review the settings.



13 Click **Finish** to deploy the VM.

14 Monitor the **Recent Tasks** area to ensure that the VM is created successfully.

Reconfigure the Virtual Hardware Settings on the SR 9.0 VM

Depending on your network setup, go to one of the following sections to reconfigure the virtual hardware for the EC 9.0 VM.

- *Reconfiguring the Virtual Hardware for Systems Using Unique dncseth and dncsatm Interfaces* (on page 32)
- *Reconfiguring the Virtual Hardware for Systems Using a Collapsed Interface for dncseth and dncsatm* (on page 33)

Reconfiguring the Virtual Hardware for Systems Using Unique dncseth and dncsatm Interfaces

Important: Execute this procedure for either a new install or a migration.

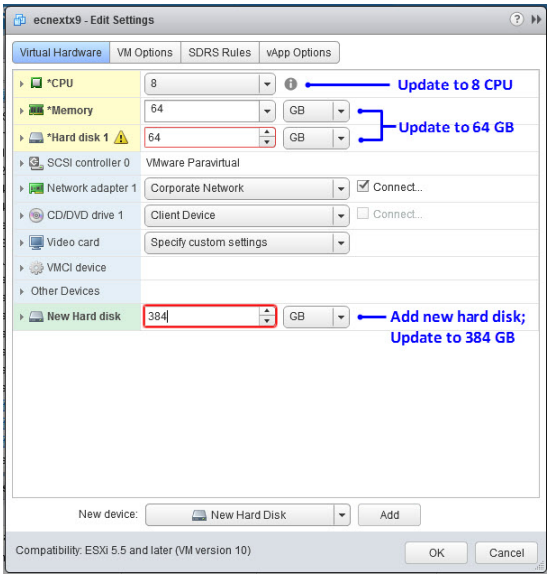
Complete the following steps to modify the virtual hardware configuration on the VM.

1. Go to the **Hosts and Clusters** view.
2. Locate and select the VM you just cloned from the Linux platform template.
3. Right-click the VM and select **Edit Settings**. The Edit Settings window appears.
4. From the **CPU** dropdown menu, select **8**.
5. From the **Memory** entry, modify the memory to **64 GB**.

   Important: Make sure that you change MB to **GB**.
6. From the **Hard disk 1** entry, modify the disk size to **64 GB**.
7. From the **New device** dropdown menu at the bottom of the window, select **New Hard Disk**.
8. Click **Add**. The New Hard Disk entry is added to the list of virtual hardware.
9. Modify the disk size to **384 GB**.

10 From the **Network adapter 1** entry, click the dropdown menu to select the appropriate network label.

Important: Do ***not*** add any additional network interfaces at this time.



11 Click **OK**. The Edit Settings window closes and the VM is reconfigured.

12 Monitor the **Recent Tasks** area to ensure the VM is successfully reconfigured.

13 Go to *Setting the Power Policy* (on page 35).

Reconfiguring the Virtual Hardware For Systems Using a Collapsed Interface for dncseth and dncsatm

Important:

- Execute this procedure for either a new install or a migration.
- A temporary IP address is required to communicate with the Admin Node.

Complete the following steps to modify the virtual hardware configuration on the VM.

1 Go to the **Hosts and Clusters** view.

2 Locate and select the VM you just cloned from the Linux platform template.

3 Right-click the VM and select **Edit Settings**. The Edit Settings window appears.

4 From the **CPU** dropdown menu, select **8**.

5 From the **Memory** entry, modify the memory to **64 GB**.

Important: Make sure that you change MB to **GB**.

6 From the **Hard disk 1** entry, modify the disk size to **64 GB**.

7 From the **New device** dropdown menu at the bottom of the window, select **New Hard Disk**.

8 Click **Add**. The New Hard Disk entry is added to the list of virtual hardware.

9 Modify the disk size to **384 GB**.

10 Complete the following steps for the **Network adapter 1** entry:

a Click the dropdown menu to select the appropriate network label (for example, Headend).

b Unselect the **Connect** check box.

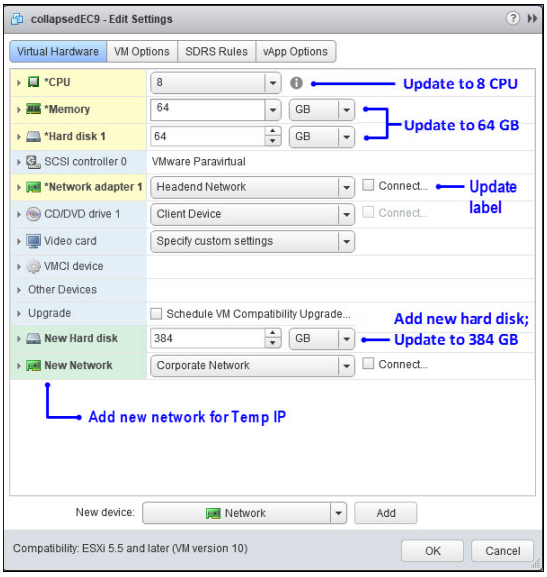
11 From the **New device** dropdown menu, select **Network** and then click **Add**. The new network is added to the list of virtual hardware.

12 Select the appropriate network label (for example, Corporate) and then ***unselect*** the **Connected** check box.

Important:

- This network will be connected in a later procedure. It is a temporary network that will be used to communicate to the Admin Node.
- Do ***not*** add any additional network interfaces at this time.

Example for a migration:



13 Click **OK**. The Edit Settings window closes and the VM is reconfigured.

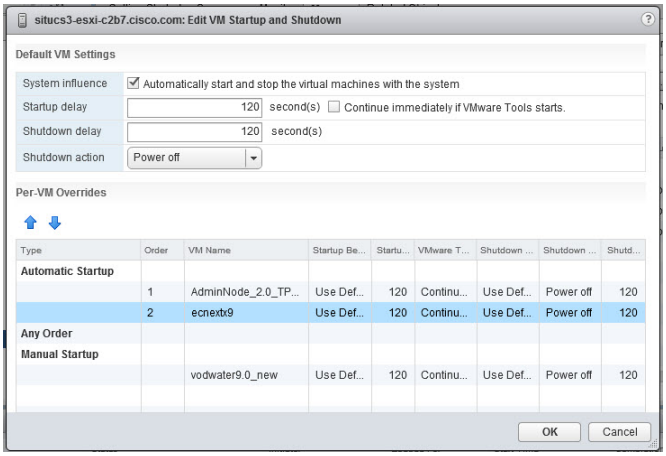
14 Monitor the **Recent Tasks** area to ensure the VM is reconfigured successfully.

Setting the Power Policy

Important: Execute this procedure for either a new install or a migration.

Complete the following steps to set the power policy for the new VM.

1. Select the **ESXi** host where the VM was created.
2. Click the **Manage** tab.
3. Click the **Settings** tab and from the Virtual Machines dropdown menu, click **VM Startup/Shutdown**.
4. Click **Edit**.
5. Ensure that the **Automatically start and stop the virtual machines with the system** check box is selected.
6. From the **Per-VM Overrides** table, select the VM you just created. The up arrow ( ) becomes active.
7. Click the up arrow until the VM is moved to the **Automatic Startup** area.



8. Click **OK**.
9. Are you using DNS in your NextX system?
   - If **yes**, go to the next step to verify that the DNS configuration is correct.
   - If **no**, you have completed this procedure. Go to ***Power on the New SR 9.0 VM*** (on page 36).
10. Click the **Networking** tab and then click **TCP/IP configuration**.
11. Click the **pencil** icon ( ) and then click **DNS configuration**.
12. Are the DNS server IP addresses correct?
    - If **yes**, click **OK**.
    - If **no**, update the IP addresses and then click **OK**.
13. Monitor the **Recent Tasks** area to confirm that the VM reconfigured successfully.

Power on the New SR 9.0 VM

Complete the following steps to power on and log into the new VM.

1. Select and right-click the SR 9.0 VM and select **Power > Power On**.
2. Right-click the VM and select **Open Console**.
3. Log into the VM as **admin** user.

   Important: You can only log in as admin user on the Cisco Linux platform. Direct root access is not permitted; however, the admin user has full root privileges via the sudo command.

   User Name: admin

   Password: [password defined for the Linux Platform template]
4. Go to the next section to configure the appropriate network configuration files for your system environment.

Update the Network Configuration File for the Corporate Interface

Depending on your network setup, go to one of the following sections to update the network configuration file(s) on the SR 9.0 VM.

- ***Updating the Configuration File for Systems Using Unique dncseth and dncsatm Interfaces*** (on page 37)
- ***Updating the Configuration Files for Systems Using a Collapsed Interface for dncseth and dncsatm*** (on page 39)

Updating the Configuration File for Systems Using Unique dncseth and dncsatm Interfaces

Complete the following procedure to update the configuration file for the corporate/management interface (ens192) on the SR 9.0 VM.

Important:

- The corporate interface is also known as the ***dncseth*** interface.
- Your network administrator should have provided you with a static IP address, default gateway and a network mask bit. If you plan to execute a migration, the static IP address should be a temporary IP address.

1 Enter the following command to edit the **ifcfg-ens192** configuration file in a text editor.

Important: The interface configuration file for the corporate/dncseth network is now **ifcfg-ens192**. This replaces the ifcfg-eth0 interface in SR 8.0 and the ifcfg-e1000g2 file in SR 7.x.

```
[admin@platform ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-ens192
```

2 Open a line after the **TYPE=Ethernet** entry and add the following entries.

Note: Replace the values in brackets with values specific to your system. Do not include the brackets.

- `IPADDR=[EC_IP_address/temporary_EC_IP_address]`
- `PREFIX=[mask bit for netmask]`
- `GATEWAY=[Gateway IP address]`
- `DEFROUTE=yes`

Example ifcfg-ens192 file *with* DNS entries:

```
BOOTPROTO=none
DEVICE=ens192
ONBOOT=yes
TYPE=Ethernet
USERCTL=no
PROXY_METHOD=none
BROWSER_ONLY=no
IPADDR=10.90.46.16
PREFIX=22
GATEWAY=10.90.44.2
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=no
RES_OPTIONS="rotate timeout:1 attempts:1"
NAME="System ens192"
DNS1=64.102.6.247
DNS2=72.163.47.11
DOMAIN=cisco.com
PEERDNS=yes
NM_CONTROLLED=no
```

Example ifcfg-ens192 file *without* DNS entries:

```
BOOTPROTO=none
DEVICE=ens192
ONBOOT=yes
TYPE=Ethernet
USERCTL=no
PROXY_METHOD=none
BROWSER_ONLY=no
IPADDR=10.90.46.16
PREFIX=22
GATEWAY=10.90.44.2
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=no
RES_OPTIONS="rotate timeout:1 attempts:1"
NAME="System ens192"
PEERDNS=no
NM_CONTROLLED=no
```

3. Save and close the file.
4. Enter the following command to reboot the VM.

   ```
   [admin@platform ~]$ sudo reboot now
   ```

5. From a SSH terminal window, log back into the VM as **admin** user using the IP address you just configured.
6. Enter the following command to view the network interface configuration.

   Note: Only ifcfg-ens192 should indicate an established interface with an IP address.

   ```
   [admin@platform ~]$ ifconfig ens192
   ```

   Example output:

   ```
   ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
           inet 10.90.46.16  netmask 255.255.252.0  broadcast 10.90.47.255
           inet6 fe80::250:56ff:feb8:121b  prefixlen 64  scopeid 0x20<link>
           ether 00:50:56:b8:12:1b  txqueuelen 1000  (Ethernet)
           RX packets 3043299  bytes 198180487 (188.9 MiB)
           RX errors 0  dropped 541  overruns 0  frame 0
           TX packets 8282  bytes 1420522 (1.3 MiB)
           TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
   ```

7 Enter the following command to verify that the gateway is correct.

```
[admin@platform ~]$ netstat -nrv
```

Example output:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.90.44.2      0.0.0.0         UG        0 0          0 ens192
10.90.44.0      0.0.0.0         255.255.252.0   U         0 0          0 ens192
```

8 Is your system using DNS?

- If **no**, go to the next step.
- If **yes**, enter the following command to verify that the DNS IP addresses are listed in the **/etc/resolv.conf** file. Then go to the next step.

  ```
  [admin@platform ~]$ cat /etc/resolv.conf
  ```

  Example output:

  ```
  # Generated by NetworkManager
  nameserver 64.102.6.247
  nameserver 72.163.47.11
  search cisco.com
  ```

9 Can you can ping the Admin Node.

- If **yes**, go to *Adding Additional Network Interfaces* (on page 42).
- If **no**, troubleshoot your network (for example, you may need to create a route) or contact your system administrator.

Updating the Configuration Files for Systems Using a Collapsed Interface for dncseth and dncsatm

Complete the following procedure to update the configuration file for the corporate/management interface (ens192) on the SR 9.0 VM.

Important:

- The collapsed interface for ***dncseth*** and the ***dncsatm*** interface is defined as **ens192**.
- Your network administrator should have provided you with a temporary IP address, netmask and gateway for the **ens224** interface. This interface is used to talk to the Admin Node.

1 Enter the following command to go to the **/etc/sysconfig/network-scripts** directory.

```
[admin@platform ~]$ cd /etc/sysconfig/network-scripts
```

2 Enter the following command to copy the ifcfg-ens192 configuration file to **ifcfg-ens224**.

```
[admin@platform ~]$ sudo cp ifcfg-ens192 ifcfg-ens224
```

3 Enter the following command to open the **ifcfg-ens224** file in a text editor.

Important: Do ***not*** edit the ifcfg-ens192 file at this time. This will be updated in a later procedure.

```
[admin@platform ~]$ sudo vi ifcfg-ens224
```

4 Update the following settings:

Note: Substitute values for your network for the terms shown in brackets. Do not include the brackets.

- `DEVICE=ens224`
- `IPADDR=[temporary_IP_Address]`
- `PREFIX=[mask bit for netmask]`
- `DEFROUTE=yes`
- `NAME="System ens224"`
- `GATEWAY=[Gateway_for_temporary_IP_address]`

Example:

```
BOOTPROTO=none
DEVICE=ens224
ONBOOT=yes
TYPE=Ethernet
USERCTL=no
PROXY_METHOD=none
BROWSER_ONLY=no
IPADDR=10.90.46.16
PREFIX=22
DEFROUTE=yes
GATEWAY=10.90.44.2
IPV4_FAILURE_FATAL=no
IPV6INIT=no
RES_OPTIONS="rotate timeout:1 attempts:1"
NAME="System ens224"
PEERDNS=no
NM_CONTROLLED=no
```

5 Save and close the file.

6 Enter the following command to reboot the VM.

```
[admin@platform ~]$ sudo reboot now
```

7 Log back into the VM as **admin** user.

8 Execute the following command to view the network interface configuration.

```
[admin@platform ~]$ ifconfig -a
```

Example output:

```
ens192: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 00:50:56:b8:5c:57  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens224: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 10.90.46.16  netmask 255.255.252.0  broadcast 10.90.47.255
        ether 00:50:56:b8:3e:30  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

9 Enter the following command to verify that the gateway is correct.

```
[admin@platform ~]$ netstat -nrv
```

Example output:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.90.44.2      0.0.0.0         UG        0 0          0 ens224
10.90.44.0      0.0.0.0         255.255.252.0   U         0 0          0 ens224
```

10 Is your system using DNS?

- If **no**, go to the next step.
- If **yes**, enter the following command to verify that the DNS IP addresses are listed in the **/etc/resolv.conf** file. Then go to the next step.

  ```
  [admin@platform ~]$ cat /etc/resolv.conf
  ```

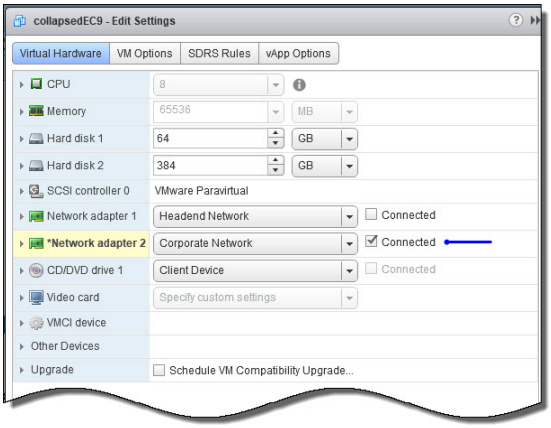
  Example output:

  ```
  # Generated by NetworkManager
  nameserver 64.102.6.247
  nameserver 72.163.47.11
  search cisco.com
  ```

11 From the vSphere Web UI, select the SR 9.0 VM and click **Edit Settings**.

12 For **Network adapter 2**, click the **Connected** check box.

Example:



13 Click **OK**.

14 Can you can ping the Admin Node.

- If **yes**, go to the next step.
- If **no**, troubleshoot your network (for example, you may need to create a route) or contact your system administrator.

15 From an SSH window, log into the SR 9.0 VM as **admin** user.

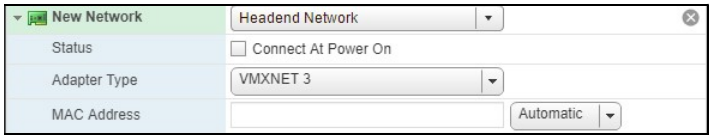
Adding Additional Network Interfaces

Complete the following procedure to add the network adapters for all interfaces you plan to configure for your system (for example, headend, nTED/TED, RepDB, billing).

1. From the vSphere Web UI, right-click the VM and select **Edit Settings**. The Edit Settings window appears.
2. From the **New Device** dropdown menu, select **Network**.
3. Click **Add**. The new network entry is added to the list of virtual hardware.
4. From the **New Network** dropdown menu, select the appropriate network for this interface.

   Note: For this example, we will create a network for the headend interface (dncsatm).
5. Click the dropdown arrow to the left of the **New Network** entry. Details for the network display.
6. Is this a migration from SR 8.0/7.x to SR 9.0?
   - If **no** and this is a Greenfield installation, go to the next step.
   - If **yes**, unselect the **Connect At Power On** box.

     Note: Unselecting this option in the vSphere Web UI will also unselect the **Connect** option. If you are using vSphere client, unselect the **Connect** and the **Connect at Power On** options.



7. Repeat steps 3 through 6 to add a network adapter for the following interfaces.

   Important: Make sure that you select the appropriate network for each new adapter in step 4.
   - nTED/TED network
   - RepDB network
8. Do you need to add any other network interfaces?
   - If **yes**, repeat steps 3 through 6 for each additional network you plan to configure.

     Important: Make sure that you select the appropriate network for each new adapter in step 4.
   - If **no**, go to the next step.

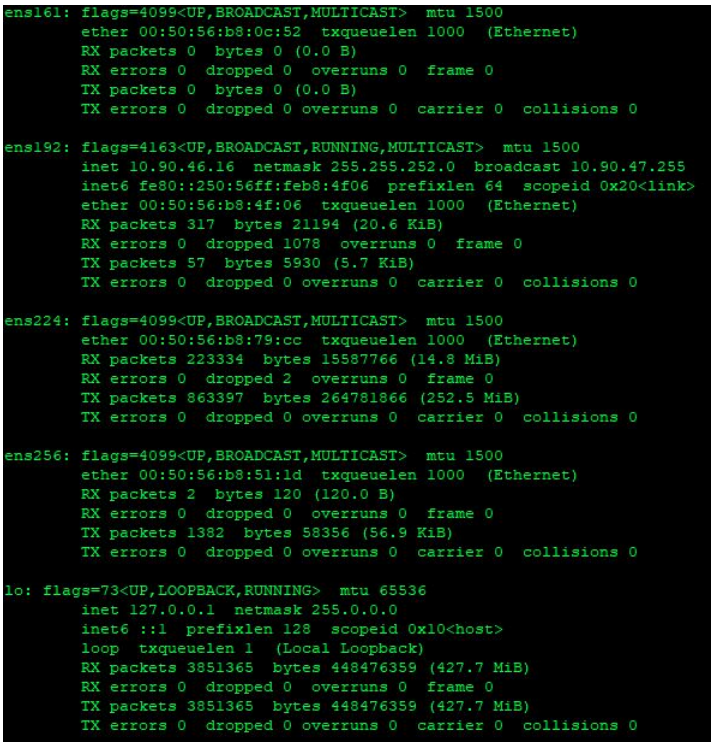
9 Click **OK**.

10 Monitor the **Recent Tasks** area to ensure that the task completes successfully.

11 From the terminal window, enter the following command to verify that the additional interfaces are now present.

```
[admin@platform ~]$ ifconfig -a
```

Example: shows four network interfaces (corporate, headend, TED and RepDB)



4

SR 9.0 Application Installation

Important: Execute these procedures for either a new install or a migration.

This chapter provides step-by-step instructions to install the SR 9.0 application.

In This Chapter

Generating and Installing HTTPS X.509 Certificates for the EC Using an Internal Root CA

Important: If you are using an *external* Certificate Authority for your HTTPS X.509 certificate/key pair, skip this procedure and go to ***Installing EC 9.0*** (on page 55).

Before continuing with this section, make sure that you have created the appropriate .env environment file for your EC node. If you have not yet done so, refer to **Create Environment Files for NextX Nodes** in the ***Admin Node 2.0 Installation Guide*** to create them now.

Go to one of the following sections to generate and install the certificates on the SR 9.0 VM.

- ***Corporate Interface (ens192) on the VM Includes a Temporary IP Address*** (on page 46)
- ***Corporate Interface (ens192) on the VM Includes a New IP Address*** (on page 49)
- ***Collapsed Interface on the VM*** (on page 52)

Corporate Interface (ens192) on the VM Includes a Temporary IP Address

Complete the following procedure if you are executing a migration from SR 8.0/7.x and you have defined a temporary IP address for the corporate network (dncseth).

Important: If this is a Greenfield installation or if this is a migration that will use a new, unique IP address, go to ***Corporate Interface (ens192) on the VM Includes a New IP Address*** (on page 49).

Note: This procedure is executed on the Admin Node and on the SR 9.0 VM. Please pay attention to the directions to complete this procedure successfully.

1. From a terminal window, log into the ***Admin Node*** as **admin** user.
2. Enter the following command to go the **/opt/cisco/ca** directory.

   ```
   [admin@adminnodenextx90 ~]$ cd /opt/cisco/ca
   ```

3. Open the **.env** file for the EC and make sure that the **IP.1** entry is correct.

   Important: The IP.1 entry should be the actual IP address of the *primary* EC on the SR 8.0/7.x system. It should *not* be the temporary IP address of the new SR 9.0 VM.

4 Enter the following command and press **Enter** to create the certificates for the EC.

Command syntax:

```
sudo ./manageCerts -s [hostname].env
```

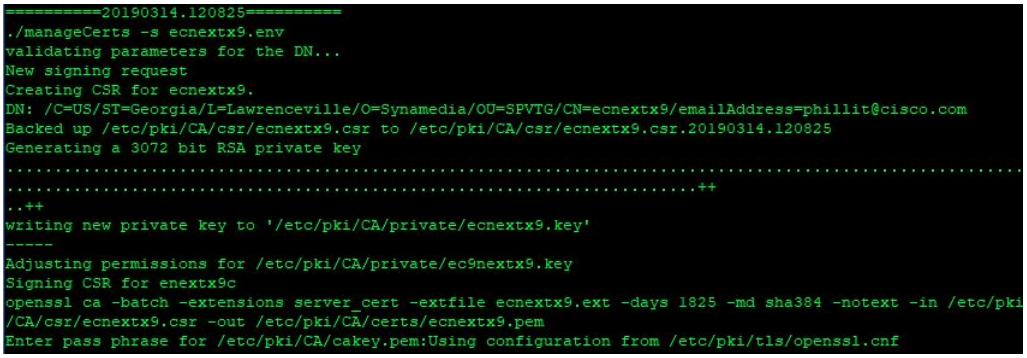
Example:

```
[admin@adminnodenextx90 ~]$ sudo ./manageCerts -s
ecnextx90.env
```

Results:

- The parameters for the distinguished name (DN) are validated.
- The CSR for the node is created.
- The RSA private key is generated and saved to the **/etc/pki/CA/private** directory on the Admin Node.
- The certificate is created and saved to the **/etc/pki/CA/certs** directory on the Admin Node.

Example output:



5 When prompted, enter the passphrase for the root CA key, cakey.pem, and then press **Enter**.

Results:

- The certificate details are displayed.
- The database is updated with a new entry.
- The CSR for [hostname].[FQDN] is successfully signed.

6 When prompted to transfer the private key and certificate to the EC, type **n** and press **Enter**. A **Done** message displays and you are returned to the admin prompt.

7 Enter the following command to verify that the certificate was successfully created.

Command syntax:

```
sudo ls /etc/pki/CA/certs | grep -i [hostname]
```

Example:

```
[admin@adminnodenextx90 ~]$ sudo ls /etc/pki/CA/certs | grep
-i ecnextx90
```

Example output:

```
ecnextx90.pem
```

8 Enter the following command to verify that the private key was successfully created.

Command syntax:

```
sudo ls /etc/pki/CA/private | grep -i [hostname]
```

Example:

```
[admin@adminnodenextx90 ~]$ sudo ls /etc/pki/CA/private | grep
-i ecnextx90
```

Example output:

```
ecnextx90.key
```

9 Enter the following command to install the certificate/key pair on the EC.

Command syntax:

```
sudo ./manageCerts -I [absolute_path_to_cert]
[absolute_path_to_key] [EC_temporary_IP_address]
```

Example:

```
[admin@adminnodenextx90 ~]$ sudo ./manageCerts -I
/etc/pki/CA/certs/ecnextx90.pem
/etc/pki/CA/private/ecnextx90.key 10.90.46.16
```

Result: The connection from the Admin Node to the EC is tested.

```
manageCerts -I /etc/pki/CA/certs/ecnextx9.pem /etc/pki/CA/private/ecnextx9 10.90.46.16
/etc/pki/CA/certs/certtest.pem: OK
Testing connection to 10.90.46.16
The authenticity of host '10.90.46.16 (10.90.46.16)' can't be estabilised.
ECDSA key fingerprint is SHA256:hCQugmdfvHmXvS7eig+4j2cDkwKB+YvNC18n1N9ATQM.
ECDSA key fingerpring is MD5:04:1c:57:9d:60:f2:46:fd:f4:76:4a:77:93:b6:a8:5d.
Are you sure you want to continue connecting (yes/no)?
```

10 When prompted to continue, type **yes** and press **Enter**.

11 When prompted for the **admin** password of the EC, type the password and press **Enter**.

12 When prompted again to continue, type **yes** and press **Enter**. The certificate/key pair are installed (copied) to the EC and a **./manageCerts finished** message displays.

13 Review the log in **/var/log** for any errors.

Note: The log file is displayed near the end of the output. The log will indicate that the certificate/key pair was copied to the EC but has not yet been configured. This configuration step will be executed in a procedure later in this chapter.

14 From the terminal window for the ***EC***, enter the following commands to verify that the certificate/key pair was successfully copied from the Admin Node to the EC.

```
[admin@platform ~]$ sudo ls -ltr /etc/pki/tls/certs
[admin@platform ~]$ sudo ls -ltr /etc/pki/tls/private
```

15 Go to ***Installing EC 9.0*** (on page 55).

Corporate Interface (ens192) on the VM Includes a New IP Address

Complete the following procedure if you are executing a Greenfield installation or a migration from SR 8.0/7.x in which the IP address for the corporate network (dncseth) on the SR 9.0 VM is a new, unique IP address.

Important: If this is a migration from SR 8.0/7.x in which you have defined a temporary IP address for the corporate network, skip this procedure. You should have completed the ***Corporate Interface (ens192) on the VM Includes a Temporary IP Address*** (on page 46) procedure.

Note: This procedure is executed on the Admin Node and on the SR 9.0 VM. Please pay attention to the directions to complete this procedure successfully.

1 From a terminal window, log into the ***Admin Node*** as **admin** user.

2 Enter the following command to go the **/opt/cisco/ca** directory.

```
[admin@adminnodenextx90 ~]$ cd /opt/cisco/ca
```

3 Open the **.env** file for the EC and make sure that the **IP.1** entry is correct.

Important: The IP.1 entry should be the actual IP address defined for the SR 9.0 VM.

4 Enter the following command and press **Enter** to create the certificates for the EC.

Command syntax:

```
sudo ./manageCerts -s [hostname].env
```

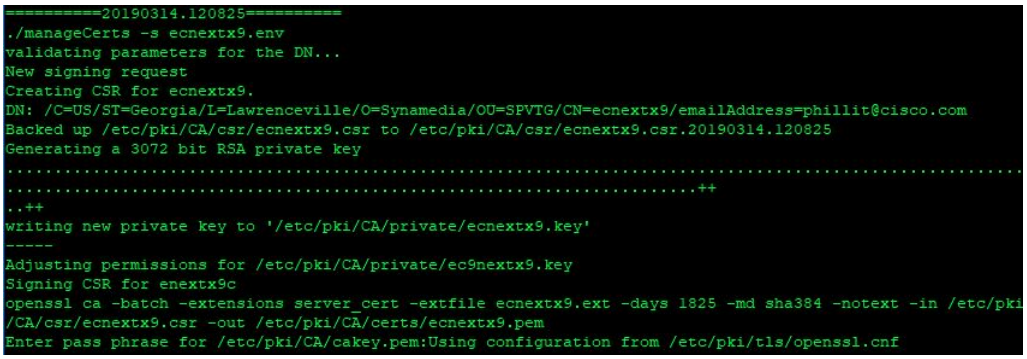
Example:

```
[admin@adminnodenextx90 ~]$ sudo ./manageCerts -s
ecnextx90.env
```

Results:

- The parameters for the distinguished name (DN) are validated.
- The CSR for the node is created.
- The RSA private key is generated and saved to the **/etc/pki/CA/private** directory on the Admin Node.
- The certificate is created and saved to the **/etc/pki/CA/certs** directory on the Admin Node.

Example output:



5 When prompted, enter the passphrase for the root CA key, cakey.pem, and then press **Enter**.

Results:

- The certificate details are displayed.
- The database is updated with a new entry.
- The CSR for [hostname].[FQDN] is successfully signed.

6 When prompted to transfer the private key and certificate to the EC, type **y** and press **Enter**.

7 When prompted to continue connecting to the EC, type **yes**.

8 When prompted, enter the **admin** password for the EC.

9 When prompted to continue connecting to the EC again, type **yes**.

Results:

- The key file is pushed from the /etc/pki/CA/private directory to the **/etc/pki/tls/private** directory on the EC.
- The certificate file is pushed to the /etc/pki/CA/certs directory to the **/etc/pki/tls/certs** directory on the EC.
- A log file is generated and saved to **/var/log**.
- A **./manageCerts finished** message displays.

Important: If a timeout or a connection to the EC fails, you must run the following command to transfer the private key and certificate to the EC.

Command syntax:

```
sudo ./manageCerts -I [absolute_path_to_cert]
[absolute_path_to_key] [EC_IP_address]
```

Example:

```
[admin@adminnodenextx90 ~]$ sudo ./manageCerts -I
/etc/pki/CA/certs/ecnextx90.pem
/etc/pki/CA/private/ecnextx90.key 10.90.46.16
```

10 Review the log in **/var/log** for any errors.

Note: The log file is displayed near the end of the output. The log will indicate that the certificate/key pair was copied to the EC but has not yet been configured. This configuration step will be executed in a procedure later in this chapter.

11 Enter the following command to verify that the certificate was successfully created.

Command syntax:

```
sudo ls /etc/pki/CA/certs | grep -i [hostname]
```

Example:

```
[admin@adminnodenextx90 ~]$ sudo ls /etc/pki/CA/certs | grep
-i ecnextx90
```

Example output:

```
ecnextx90.pem
```

12 Enter the following command to verify that the private key was successfully created.

Command syntax:

```
sudo ls /etc/pki/CA/private | grep -i [hostname]
```

Example:

```
[admin@adminnodenextx90 ~]$ sudo ls /etc/pki/CA/private | grep
-i ecnextx90
```

Example output:

```
ecnextx90.key
```

13 From the terminal window for the ***EC***, enter the following commands to verify that the certificate/key pair were successfully copied from the Admin Node to the EC.

```
[admin@platform ~]$ sudo ls -ltr /etc/pki/tls/certs
[admin@platform ~]$ sudo ls -ltr /etc/pki/tls/private
```

14 Go to ***Installing EC 9.0*** (on page 55).

Collapsed Interface on the VM

Complete the following procedure if you are executing a Greenfield installation or a migration on an EC 9.0 VM that includes a collapsed interface.

Note: This procedure is executed on the Admin Node and on the SR 9.0 VM. Please pay attention to the directions to complete this procedure successfully.

1. From a terminal window, log into the ***Admin Node*** as **admin** user.
2. Enter the following command to go the **/opt/cisco/ca** directory.

   ```
   [admin@adminnodenextx90 ~]$ cd /opt/cisco/ca
   ```

3. Open the **.env** file for the EC and make sure that the DNS and IP entries are correct.

   Important:

   - The **DNS.1** entry is the fully qualified domain name.
   - The **DNS.2** entry if **dncsatm**.
   - The **IP.1** entry is the actual IP address of the SR 9.0 system (ens192).
   - The **IP.2** entry is the temporary IP address on the SR 9.0 system (ens224) that is configured to communicate with the Admin Node.

4. Enter the following command and press **Enter** to create the certificates for the EC.

   Command syntax:

   ```
   sudo ./manageCerts -s [hostname].env
   ```

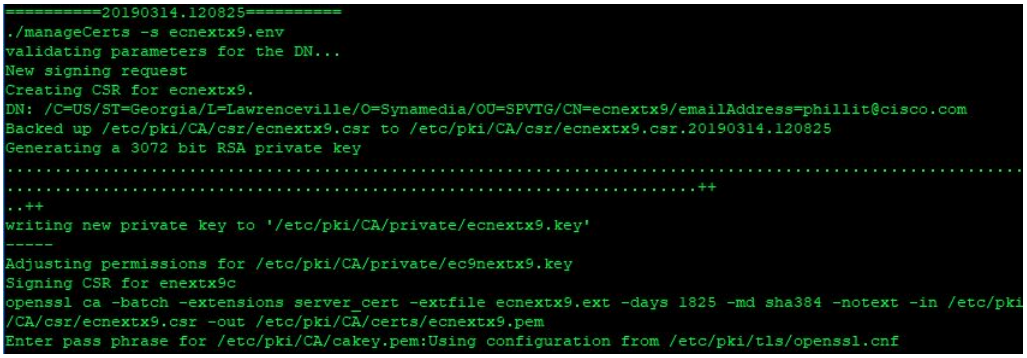
   Example:

   ```
   [admin@adminnodenextx90 ~]$ sudo ./manageCerts -s
   ecnextx90.env
   ```

   Results:

   - The parameters for the distinguished name (DN) are validated.
   - The CSR for the node is created.
   - The RSA private key is generated and saved to the **/etc/pki/CA/private** directory on the Admin Node.
   - The certificate is created and saved to the **/etc/pki/CA/certs** directory on the Admin Node.

Example output:



5 When prompted, enter the passphrase for the root CA key, cakey.pem, and then press **Enter**.

Results:

- The certificate details are displayed.
- The database is updated with a new entry.
- The CSR for [hostname].[FQDN] is successfully signed.

6 When prompted to transfer the private key and certificate to the EC, type **n** and press **Enter**. A **Done** message displays and you are returned to the admin prompt.

7 Enter the following command to verify that the certificate was successfully created.

Command syntax:

```
sudo ls /etc/pki/CA/certs | grep -i [hostname]
```

Example:

```
[admin@adminnodenextx90 ~]$ sudo ls /etc/pki/CA/certs | grep
-i ecnextx90
```

Example output:

```
ecnextx90.pem
```

8 Enter the following command to verify that the private key was successfully created.

Command syntax:

```
sudo ls /etc/pki/CA/private | grep -i [hostname]
```

Example:

```
[admin@adminnodenextx90 ~]$ sudo ls /etc/pki/CA/private | grep
-i ecnextx90
```

Example output:

```
ecnextx90.key
```

9 Enter the following command to install the certificate/key pair on the EC.

Command syntax:

```
sudo ./manageCerts -I [absolute_path_to_cert]
[absolute_path_to_key] [EC_temporary_IP_address]
```

Example:

```
[admin@adminnodenextx90 ~]$ sudo ./manageCerts -I
/etc/pki/CA/certs/ecnextx90.pem
/etc/pki/CA/private/ecnextx90.key 10.90.46.16
```

Example output: The connection from the Admin Node to the EC is tested.

```
manageCerts -I /etc/pki/CA/certs/ecnextx9.pem /etc/pki/CA/private/ecnextx9 10.90.46.16
/etc/pki/CA/certs/certtest.pem: OK
Testing connection to 10.90.46.16
The authenticity of host '10.90.46.16 (10.90.46.16)' can't be established.
ECDSA key fingerprint is SHA256:hCQugmdfvHmXvS7eig+4j2cDkwKB+YvNC18n1N9ATQM.
ECDSA key fingerpring is MD5:04:1c:57:9d:60:f2:46:fd:f4:76:4a:77:93:b6:a8:5d.
Are you sure you want to continue connecting (yes/no)?
```

10 When prompted to continue, type **yes** and press **Enter**.

11 When prompted for the **admin** password of the EC, type the password and press **Enter**.

12 When prompted again to continue, type **yes** and press **Enter**. The certificate/key pair are installed (copied) to the EC and a **./manageCerts finished** message displays.

13 Review the log in **/var/log** for any errors.

Note: The log file is displayed near the end of the output. The log will indicate that the certificate/key pair was copied to the EC but has not yet been configured. This configuration step will be executed in a procedure later in this chapter.

14 From the terminal window for the ***EC***, enter the following commands to verify that the certificate/key pair was successfully copied from the Admin Node to the EC.

```
[admin@platform ~]$ sudo ls -ltr /etc/pki/tls/certs
[admin@platform ~]$ sudo ls -ltr /etc/pki/tls/private
```

15 Go to the next section.

Installing EC 9.0

Complete the following steps to install the EC 9.0 application on the VM.

1. As **admin** user, enter the following command to copy the VCS deployment zip file from the /home/admin directory to the **/var/tmp** directory.

   Note: When the Linux platform template was created, the VCS deployment zip file was saved to the /home/admin directory.

   Command syntax:

   ```
   cp -a /home/admin/cisco-vcs-deployment-[VERSION].zip /var/tmp
   ```

   Example:

   ```
   [admin@platform ~]$ cp -a
   /home/admin/cisco-vcs-deployment-2.0.4.zip /var/tmp
   ```

2. Enter the following command to change to the **/var/tmp** directory.

   ```
   [admin@platform ~]$ cd /var/tmp
   ```

3. Enter the following command to unzip the **cisco-vcs-deployment** zip file.

   ```
   [admin@platform tmp]$ unzip cisco-vcs-deployment*.zip
   ```

4. Enter the following command to change to **scripts** directory.

   Command syntax:

   ```
   cd cisco-vcs-deployment-[VERSION]/scripts
   ```

   Example:

   ```
   [admin@platform tmp]$ cd cisco-vcs-deployment-2.0.4/scripts
   ```

5. Enter the following command to verify that the following EC-specific files are present.

   - **deploy-ec.sh**
   - **ec.envfile**

   ```
   [admin@platform scripts]$ ls | grep ec
   ```

6. Enter the following command to edit the **ec.envfile** file.

   ```
   [admin@platform scripts]$ vi ec.envfile
   ```

   Default ec.envfile

   ```
   admin_node=
   cisco_appserver=false
   default_gateway=
   ec_headend_interface=
   ec_headend_ip=
   ec_headend_netmask=
   lab_setup=false
   ted_interface=
   hostname=
   ```

7 Enter values specific to your system.

Important:

- If you are using the Cisco application server, change the **cisco_appserver** value from false to **true**.
- Leave the **default_gateway** field empty.
- The **ec_headend_interface** (dncsatm) is a user-defined interface.
- If you are using an nTED, leave the **ted_interface** field empty.
- If you are using a legacy TED, then the interface is a user-defined interface (for example, ens256).
- The **hostname** ***cannot*** contain hyphens (-) or underscores (_). If it does, the installation will fail.

  Note: If this is a migration from SR 8.0/7.x to SR 9.0 and you want to change the hostname to a new hostname, append the new name to the "hostname=" entry. Ensure that you execute the steps in ***Update the site_info Database Table for a Hostname Change*** (on page 97) procedure, post upgrade, or dncsInit.d will not start.

Example: ec.envfile with ted_interface for a ***legacy TED***:

```
admin_node=10.90.181.139
cisco_appserver=true
default_gateway=
ec_headend_interface=ens224
ec_headend_ip=204.3.1.97
ec_headend_netmask=255.255.255.240
lab_setup=false
ted_interface=ens256
hostname=ecnextx90
```

Example: ec.envfile without ted_interface defined for a ***nTED***:

```
admin_node=10.90.181.139
cisco_appserver=true
default_gateway=
ec_headend_interface=ens224
ec_headend_ip=204.3.1.97
ec_headend_netmask=255.255.255.240
lab_setup=false
ted_interface=
hostname=ecnextx90
```

Example: ec.envfile for system with a ***collapsed interface without an nTED***

```
admin_node=10.90.181.139
cisco_appserver=true
default_gateway=
ec_headend_interface=ens192
ec_headend_ip=204.3.1.97
ec_headend_netmask=255.255.255.240
lab_setup=false
ted_interface=ens256
hostname=ecnextx90
```

Example: ec.envfile for system with a ***collapsed interface with an nTED***

```
admin_node=10.90.181.139
cisco_appserver=true
default_gateway=
ec_headend_interface=ens192
ec_headend_ip=204.3.1.97
ec_headend_netmask=255.255.255.240
lab_setup=false
ted_interface=
hostname=ecnextx90
```

8 Save and close the file.

9 Execute the following command to deploy the EC application. This will take approximately 45 minutes.

```
[admin@platform scripts]$ sudo ./deploy-ec.sh
--envfile=ec.envfile 2>&1 | sudo tee /var/log/deploy-ec.out
```

Result: An **ec installation completed** message will display. The VM will then reboot.

Important: If the deploy-ec.sh script fails, troubleshoot the issue. Once the issue is resolved/recognized, execute the deploy-ec.sh script again.

10 From the terminal window, log back into the EC as **admin** user.

11 Verify that the network interfaces are present by entering the following command.

```
[admin@ecnextx90 ~]$ ifconfig -a
```

12 Enter the following command to verify that the RPM packages are installed. A list of the installed packages is displayed.

```
[admin@ecnextx90 ~]$ rpm -qa | egrep -i
"puppet|cscoec|cscoapsrv"
```

13 Do any patches to the installation exist?

- If **yes**, go to ***EC SR 9.0 Patch Installs*** (on page 219). Once the patch is installed, go to the next section in this chapter.
- If **no**, go to the next section.

Creating the config.json File on the EC

Important: If you do ***not*** plan to regionalize the EC to an Explorer Controller Suite (ECS) NextX system, skip this section and go to ***Configuring the Certificate/Key Pair on the EC*** (on page 60).

Complete the following steps to create the config.json file on the EC.

1 As **admin** user on the EC, enter the following command to change to the **/etc/consul** directory.

```
[admin@ecnextx90 ~]$ cd /etc/consul
```

2 Enter the following command to copy the client.json.template file to the **config.json** file.

```
[admin@ecnextx90 consul]$ sudo cp client.json.template
config.json
```

3 Open the **/etc/consul/config.json** file in a text editor.

```
[admin@ecnextx90 consul]$ sudo vi config.json
```

4 In the **"bind_addr"** line, replace <client_ip> with the actual IP address of the EC node.

Example:

```
"bind_address": "10.90.46.17",
```

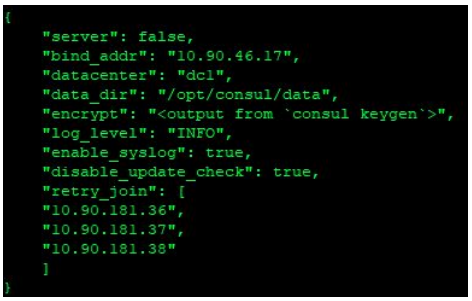
5 Move to the **"encrypt"** line and replace <output from <`consul keygen`> with the Consul encryption key.

Important: This key was generated when the Admin Node was deployed in the ***Deploying the Repos for the Application Packages*** section of the **Admin Node 2.0 Installation Guide**.

6 In each of **server_ip** entries, substitute the appropriate IP address for the Consul nodes in your ECS NextX system.

- "<server_ip1>" IP Address of Consul 1
- "<server_ip2>" IP Address of Consul 2
- "<server_ip3>" IP Address of Consul 3

Example:



7 Save and close the **config.json** file.

8 Enter the following command to restart the consul service.

```
[admin@ecnextx90 consul]$ sudo systemctl restart consul
```

9 Enter the following command to verify that the consul service is active and running.

```
[admin@ecnextx90 consul]$ systemctl status consul
```

Example output:

```
consul.service - Consul daemon
   Loaded: loaded (/usr/lib/systemd/system/consul.service; disabled; vendor
preset: disabled)
   Active: active (running) since Wed 2019-02-20 13:53:19 EST; 1s ago
 Main PID: 21801 (consul)
   CGroup: /system.slice/consul.service
           └─21801 /usr/sbin/consul agent -config-dir=/etc/consul
```

Configuring the Certificate/Key Pair on the EC

Complete the following procedure to configure the certificate/key pair on the EC.

Important: This procedure is executed on the Admin Node and must be completed for systems using an ***internal*** or an ***external*** CA.

Notes:

- If an *internal* CA was used, then the EC certificate files were created in ***Generating and Installing HTTPS X.509 Certificates for the EC Using an Internal Root CA*** (on page 46).
- If an *external* CA was used, then the EC's certificate files were created in the **Configure the Admin Node for an External CA** section of the ***Admin Node 2.0 Installation Guide***.

1. As **admin** user, enter the following command to configure the certificate/key pair created on the Admin Node for the EC.

   Note: Substitute the ***IP address/temporary IP address*** of the SR 9.0 EC for [EC_IP_address]. Do not include the brackets.

   Command syntax:

   ```
   sudo ./manageCerts -P [absolute_path_to_cert]
   [absolute_path_to_key] [EC_IP_address]
   ```

   Example:

   ```
   [admin@adminnodenextx90 ca]$ sudo ./manageCerts -P
   /etc/pki/CA/certs/ecnextx90.pem
   /etc/pki/CA/private/ecnextx90.key 10.90.46.16
   ```

2. When prompted for the **key store password**, enter the password and press **Enter**.
3. When prompted to re-enter the key store password, enter the password and press **Enter**.
4. When prompted for the **trust store password**, enter the password and press **Enter**.
5. When prompted to re-enter the trust store password, enter the password and press **Enter**. When the script completes, a **./manageCerts finished** message displays.

   Note: Two log files are displayed at the end of the output. The first log, /var/log/configure_certs_ec.log, is on the EC. The second log, /var/log/manageCerts[date].log is on the Admin Node.
6. Review the logs for any errors.

7 Is the following error present in the log on the Admin Node?

```
ERROR, if regionalized, failed to edit /etc/consul/config.json, if
regionalization is enabled please manually correct /etc/consul/config.json to
the following settings
"ca_file": "/etc/pki/tls/cacert.pem",
"cert_file": "/etc/pki/tls/certs/server.crt",
"key_file": "/etc/pki/tls/private/server.key",
"verify_outgoing": true,
"verify_incoming": true,
```

- If **no**, go to the next step.
- If **yes** and you ***are not*** regionalizing the EC to an ECS, ignore this error and go to the next step.
- If **yes** and you ***are*** regionalizing the EC to an ECS, open the **consul.json** file on the EC and update the first five lines as described in the output of the log.

8 On the ***EC***, type the following command to view the certificates, Java key stores (.jks files) and soft links that were configured on the EC.

```
[admin@ecnextx9 ~]$ sudo ls -ltr /etc/pki/tls/certs
```

```
total 28
-rwxr-xr-x. 1 root root  829 Aug  4  2017 renew-dummy-cert
-rw-r--r--. 1 root root 2516 Aug  4  2017 Makefile
-rwxr-xr-x. 1 root root  610 Aug  4  2017 make-dummy-cert
lrwxrwxrwx. 1 root root   55 Aug 14  2018 ca-bundle.trust.crt -> /etc/pki/ca-trust/extracted/openssl/ca-bu
ndle.trust.crt
lrwxrwxrwx. 1 root root   49 Aug 14  2018 ca-bundle.crt -> /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.p
em
-rw-r--r--. 1 root root    0 Sep  6  2018 vdcmrootcerts.crt
drwxr-xr-x. 2 root root    6 Sep  6  2018 vdcmrootcerts
-rw-------. 1 root root 1440 Mar  4 12:13 localhost.crt
-r--r--r--. 1 root root 2061 Mar  4 14:23 ecnextx9.pem
lrwxrwxrwx. 1 root root   39 Mar  4 14:23 server.crt -> /etc/pki/tls/certs/ecnextx9.pem
-rw-r--r--. 1 root root 4545 Mar  4 14:23 ecnextx9.client.pem
lrwxrwxrwx. 1 root root   46 Mar  4 14:23 bossclient.key -> /etc/pki/tls/certs/ecnextx9.client.pem
lrwxrwxrwx. 1 root root   46 Mar  4 14:23 rpoclient.key -> /etc/pki/tls/certs/ecnextx9.client.pem
lrwxrwxrwx. 1 root root   46 Mar  4 14:23 ldsclient.key -> /etc/pki/tls/certs/ecnextx9.client.pem
lrwxrwxrwx. 1 root root   46 Mar  4 14:23 tedclient.key -> /etc/pki/tls/certs/ecnextx9.client.pem
lrwxrwxrwx. 1 root root   41 Mar  4 14:23 genericKeystore.jks -> /etc/pki/tls/ecnextx9.jks
lrwxrwxrwx. 1 root root   43 Mar  4 14:23 genericTruststore.jks -> /etc/pki/tls/ecnextx9.jks
lrwxrwxrwx. 1 root root   23 Mar  4 14:23 cachain.crt -> /etc/pki/tls/cacert.pem
lrwxrwxrwx. 1 root root   23 Mar  4 14:23 cacert.pem -> /etc/pki/tls/cacert.pem
lrwxrwxrwx. 1 root root   31 Mar  4 14:23 server.key -> /etc/pki/tls/private/server.key
```

9 Type the following command to list the keys that were configured on the EC.

```
[admin@ecnextx9~]$ sudo ls -ltr /etc/pki/tls/private
```

```
total 8
-rw-------. 1 root root   1679 Mar  4 12:13 localhost.key
-r--r--r--. 1 root consul 2484 Mar  4 14:23 ecnextx9.key
lrwxrwxrwx. 1 root root     41 Mar  4 14:23 server.key -> /etc/pki/tls/private/ecnextx9.key
```

10 Do you need to execute a system migration to your SR 9.0 server?

- If **yes**, go to ***Migrate to SR 9.0*** (on page 63).
- If **no** and this is a Greenfield installation that is configured with ***unique interfaces*** for dncseth and dncsatm, go to ***SR 9.0 Post Upgrade Procedures*** (on page 85).
- If **no** and this is a Greenfield installation that is configured with a ***collapsed interface*** for dncseth and dncsatm, go to ***Update the Network Post-Application Installation or Post-Migration*** (on page 77).

5

Migrate to SR 9.0

Important: If you are executing a new SR 9.0 installation, skip this section and go to ***SR 9.0 Post Upgrade Procedures*** (on page 85).

This section provides the procedure to migrate to SR 9.0 from one of the following system releases:

- SR 8.0 running on a CentOS release 6.8 Linux platform
- SR 7.x running on a Solaris_x86-10 platform

In This Chapter

Creating an Admin User on the SR 7.x System

Important: If you are not migrating from SR 7.x, skip this procedure and go to *Delete the EC Registration to an ECS* (on page 66).

To successfully migrate from SR 7.x to SR 9.0, you must create an **admin** user on the SR 7.x EC. The admin user is used to assist in the migration activities.

Note: This procedure is executed on the SR 7.x system.

1. From a terminal window, log into the SR 7.x EC as an Administrative user.
2. Does a user defined as **admin** exist on the SR 7.x system?
   - If **no**, go to step 9.
   - If **yes**, go to the next step.
3. Review the **/export/home/admin** directory and back up any necessary files.
4. As **root** user, enter the following command. The USER ADMINISTRATION MENU displays.

   ```
   # /dvs/admin/useradmin
   ```
5. Type **b** and press **Enter**.
6. When prompted, type **admin** and press **Enter**.
7. Were you prompted to confirm the removal of the admin user?
   - If **yes**, type **y** and press **Enter** and then type **q** and press **Enter** to exit the script. Go to step 9.
   - If **no** and the admin user was not found, type **q** and press **Enter** to exit the script. Go to step 8.
8. Enter the following command remove the user account. The user account is deleted from the system.

   ```
   # userdel -r admin
   ```
9. As **root** user, execute the following command to create a migration user called **admin**.

   ```
   # useradd -c "Cisco Linux Platform Migration User" -s
   /bin/bash -d /export/home/admin -m admin
   ```
10. Enter the following command to set the password for the **admin** user.

    ```
    # passwd -r files admin
    ```
11. When prompted for the new password, enter the same password defined for the admin user on the newly deployed SR 9.0 EC.

    Important: The password for the admin user on the SR 7.x and SR 9.0 systems ***must*** match.
12. When prompted, re-enter the password. A successful message appears.

13 Complete the following steps to allow sudo root access for the admin user.

a Enter the following command to edit the **/usr/local/etc/sudoers** file.

```
# /usr/local/sbin/visudo
```

b Open a line under the **# User privilege specification** entry in the file and type the following entry.

```
admin ALL=(ALL) NOPASSWD: ALL
```

c Save and close the file.

14 Complete these steps to verify that the admin user as sudo root access.

a In a new terminal window, log into the SR 7.x EC as **admin** user.

b When prompted, enter the admin password.

c Enter **/usr/local/bin/sudo –i** and press **Enter**. If the command line changes to a root prompt (#), then the admin user has sudo root access.

Note: If errors appear, verify the entries that you added in the sudoers command performed in step 13.

Delete the EC Registration to an ECS

Important: Skip this procedure if the EC system you are migrating from is not regionalized to an ECS.

If the SR 8.0/7.x EC is registered to an ECS, you ***must*** first unregionalize and delete the registration. Depending on your system, go to one of the following sections:

- ***Deleting an EC 8.0 Registration from ECS 3.0*** (on page 66)
- ***Deleting an EC 7.x Registration from ECS 2.0*** (on page 67)

Deleting an EC 8.0 Registration from ECS 3.0

1. As **dncs** user, enter the following command to tail the **eventManager** log and monitor the registration deletion process.

   EC 8.0 system:

   ```
   [dncs@ecnextx8 ~]$ qtail eventM
   ```

2. Log into the EC Web UI as an Administrative user.
3. Click the **Navigation** menu ( ) and then select **Service Provisioning > Regionalization Configuration**. The Regionalization Configuration Web UI opens.
4. Click **Unregister**.
5. When prompted to enter the Web UI credentials for the EC server, enter your Administrative username and password.
6. Then click **Log in**. You are directed to the EC Web UI where a deleted successfully message appears in the lower right corner of the window.

   Note: The status is updated to **UnRegistered**.

Registration Status	UnRegistered
Status Comment	Unregistered Successfully
Last Updated Time	2017-03-31T12:11:37-04:00

7. From the terminal window for the EC, enter the following command to verify that the registration status in the database is now **Unregistered Successfully**.

   Command for EC:

   ```
   [dncs@ecnextx8 ~]$ echo "select * from registration_config" |
   dbaccess dncsdb -
   ```

   Example output:

   ```
   status_comment      Unregistered Successfully
   ```

8. From the Regionalization Configuration Web UI, click **Delete** to delete the registration record from the database and to delete the registration from the ECS.
9. When prompted to confirm the deletion, click **OK**.

10 Repeat step 7 to verify that the registration is removed from the database.

Example output:

```
Database selected.
No rows found.
Database closed.
```

11 Enter the following command to verify that the **rpa.config** file was deleted from the /dvs/dvsFiles/rpa directory:

```
[dncs@ecnextx8 ~]$ ls –ltr /dvs/dvsFiles/rpa
```

12 Log into the ECS Web UI. The Service Instance List page opens.

13 Verify that the five instances associated with EC you deleted are no longer present in the list.

14 Click the **Navigation** icon () and then select **Control Plane > ECS Dashboard**.

15 Drill down in the ECS directory tree to verify that the EC server you deleted is no longer in the list.

16 Go to *Migrate the Key Files and Database to SR 9.0* (on page 69).

Deleting an EC 7.x Registration from ECS 2.0

1 Log into the EC 7.x Web UI as an Administrative user.

2 Click **EC > Service Provisioning > Regionalization Configuration**. The Regionalization Configuration page opens.

3 Click **Unregister**. The Registration Status on the Web UI should update to UnRegistered.

4 From a terminal window as **dncs** user , enter the following command to verify that the registration was deleted from the registration_status table in the database:

```
$ echo "select * from registration_config" | dbaccess dncsdb -
```

5 Browse through the output for the status_comment entry and verify that it is updated to **Successfully Unregistered**.

Example status_comment output:

```
status_comment      Successfully Unregistered. Stopping
                    Register Service
```

6 Enter the following command to verify that the **rpa.config** file was deleted from the system.

```
$ ls -ltr /dvs/dvsFiles/rpa
```

Expected output:

```
total 0
```

7 Is the **rpa.config** file present?

- If **no**, go to the next step.
- If **yes**, enter the following command to delete the file. Then go to the next step.

```
$ rm /dvs/dvsFiles/rpa/rpa.config
```

8 Log into the ECS Web UI where the EC was unregistered and then click **Message Infrastructure > Service Infrastructure > Service Instance**.

9 Verify that all SIs for this EC host are **OOS**.

10 From the EC Web UI, click **EC > Service Provisioning > Regionalization Configuration** and click **Delete**. The following warning message appears.

11 Read the warning and click **OK**. Because SSO changes to *disabled*, you are prompted for the username and password to the EC.

12 Enter your username and password and click **OK**. The Regionalization Configuration Web UI refreshes.

13 Click **Delete** and click **OK** in the warning message. The Web UI fields are cleared.

14 Repeat step 4 to verify that there is no registration entry present in the database.

Expected output:

```
Expected output:
Database selected.
No rows found.
Database closed.
```

15 From the ECS Web UI where the EC was deleted, click **Message Infrastructure > Service Infrastructure > Service Instance** and verify that all SIs for this EC have been deleted.

16 From the ECS Web UI where the EC was deleted, click **Message Infrastructure > Service Infrastructure > Virtual Service** and verify that all virtual services for this EC have been deleted.

17 From the ECS Web UI where the EC was deleted, click **Message Infrastructure > Service Infrastructure > Account JID** and verify that all JIDs for this EC have been deleted.

18 Go to the next section.

Migrate the Key Files and Database to SR 9.0

This section provides the procedure to migrate the key files and database from SR 8.0/7.xto SR 9.0.

Important: If the SR 8.0/7.x EC is registered to an ECS you must first unregionalize and delete the registration. Return to ***Delete the EC Registration to an ECS*** (on page 66) to delete the registration now.

Descriptions and Options for the Migrate Scripts

Each migration script includes a description and a list of options that may be used along with the script command. Complete the following steps to view the descriptions for each migration script.

1 On the ***SR 9.0 EC***, enter the following command to view the description of the **migrateKeyFiles** script.

```
[admin@ecnextx9 ~]$ sudo
/opt/cisco/backup_restore/migrateKeyFiles -h
```

```
NAME
     migrateKeyFiles - migrate remote key files

DESCRIPTION
     This script will rsync key files from remote host specified

     Usage: migrateKeyFiles [-vh] [-I keyfiles_include ] [ -E keyfiles_exclude ] [ -S keyf
iles_staging ] [ -F force copy ] -l username -r remote_host

OPTIONS
     The following options are supported:
     -I     Specify the file that lists all the files that need to
            be included in the backup.

     -E     Specify the file that lists all the files that need to
            be excluded from the backup.

     -S     Specify the file that lists all the files that need to
            be moved to the staging dir for reference on remote_host.

     -F     Force copy on SunOS to Linux migration.

     -l     Remote login user.

     -r     Remote host/ip.

     -h     Display this help message then exit.

     -v     Operate verbosely.
```

2 Enter the following command to view the description of the **migrateUsers** script.

```
[admin@ecnextx9 ~]$ sudo
/opt/cisco/backup_restore/migrateUsers -h
```

```
./migrateUsers -h
usage: migrateUsers [-h] --source [SRC_HOST] [--all_users]

Migrate Unix and WUI users from Unix host to this Linux host

optional arguments:
  -h, --help           show this help message and exit
  --source [SRC_HOST]  IP address of machine to be migrated
  --all_users          Migrate ALL users without prompting
```

3 Enter the following command to view the description of the **migrateDBKF** script.

```
[admin@ecnextx9 ~]$ sudo /opt/cisco/backup_restore/migrateDBKF
-h
```

```
usage: migrateDBKF [-h] --source [SRC_HOST] --db [SYS_TYPE]
                   [-I [INCLUDE_FILE]] [-E [EXCLUDE_FILE]] [-S [EXCLUDE_FILE]]

optional arguments:
  -h, --help            show this help message and exit
  --source [SRC_HOST]   IP address of machine to be migrated
  --db [SYS_TYPE]       [dncs or dtacs] Migrate DTACS or EC and AppSrv database
                        to this machine
  -I [INCLUDE_FILE]     Include file to be used for migrateKeyFiles
  -E [EXCLUDE_FILE]     Exclude file to be used for migrateKeyFiles
  -S [EXCLUDE_FILE]     Staging file to be used for migrateKeyFiles
```

Migrating Key Files

In this section, you will migrate the key files from SR 8.0/7.x to SR 9.0. The migration script for the key files will put the key files migration RSA key (kfm_rsa) in place and also execute an initial migration of the key files. The specified files or directories will be mapped into a new directory, /disk1/keyfiles_staging, on the SR 9.0 EC.

Important:

- Cisco recommends that the default migrate key files command be executed ***without the -I or -E option*** to prevent any issues that may impact the execution of the migrateUsers or migrateDBKF scripts. After the SR 9.0 migration is complete, the operator can then copy over any custom keyfiles/scripts/directories from the SR 8.0/7.x system.
- The -I and -E options should only be used by advanced users who have tested migrations with the include/exclude file options.
- If you choose to use the ***-I*** option, make sure that you add the absolute path of each user-defined key file to the end of the **KeyFiles.include** file located in the /opt/cisco/backup_restore/KeyFiles_templates directory. The KeyFiles.include file must contain all default entries plus any additional user-defined entries. This file contains the default entries and should be copied and modified accordingly.

Complete the following procedure to migrate the key files to SR 9.0.

1 Are you migrating from SR 8.0 to SR 9.0?
   - If **yes**, go to the next step.
   - If **no** and you are migrating from SR 7.x to SR 9.0, go to step 4.

2 As **admin** user on the ***SR 8.0 EC***, enter the following command to list the contents of the **/dvs/dvsFiles/SnmpeventLogs** directory.

```
[admin@ecnextx8 ~]$ sudo ls -ltr /dvs/dvsFiles/SnmpeventLogs
```

3 Delete any old logs.

4 As **admin** user on the ***SR 9.0 EC***, enter the following command to change to the **/opt/cisco/backup_restore** directory.

```
[admin@ecnextx9 ~]$ cd /opt/cisco/backup_restore
```

5 Enter the following command to execute the migrateKeyFiles script.

Note: Substitute the IP address for the SR 8.0/7.x EC for the [previous_SR_IP] entry in the command. Do not include the brackets.

Migrate default key files command:

```
sudo ./migrateKeyFiles -v -l admin –r [previous_SR_IP]
```

Migrate default key files example:

```
[admin@ecnextx9 backup_restore]$ sudo ./migrateKeyFiles -v -l
admin –r 10.90.46.17
```

6 When prompted, enter **yes** to continue and then press **Enter**.

7 When prompted for the admin password, enter it and press **Enter**.

8 When prompted for the admin password again, re-enter it and press **Enter**. The keyfiles migration starts and they are migrated to the /disk1/keyfiles_staging directory on the SR 9.0 EC.

9 When the script completes, review the **/var/log/migrateKeyFilesLog** file for any errors.

10 Enter the following command to go to the **/dvs/backups** directory.

```
[admin@ecnextx9 backups_restore]$ cd /dvs/backups
```

11 Enter the following command to see if the **dncsdb.migrate** and the **appdb.migrate** directories are present in the **/dvs/backups** directory.

```
[admin@ecnextx9 backups]$ ls -ltr | grep migrate
```

Example output:

```
drwxr-xr-x. 3 root root  4096 Jul 27 11:00 dncsdb.migrate
drwxr-xr-x. 3 root root  4096 Jul 27 11:01 appdb.migrate
```

12 Are the dncsdb.migrate and appdb.migrate directories present?

If **no**, you have completed this procedure. Go to the next section.

If **yes**, go to the next step.

13 Enter the following two commands to move the directories.

```
[admin@ecnextx9 backups]$ sudo mv dncsdb.migrate
dncsdb.migrate.old
[admin@ecnextx9 backups]$ sudo mv appdb.migrate
appdb.migrate.old
```

14 Repeat step 11 to verify that the directories were moved successfully.

Example output:

```
drwxr-xr-x. 3 root root  4096 Jul 27 11:00 dncsdb.migrate.old
drwxr-xr-x. 3 root root  4096 Jul 27 11:01 appdb.migrate.old
```

Migrating Users

In this section, you will migrate the users and their user directories from either the SR 8.0/7.x EC to the SR 9.0 EC. This migration script, migrateUsers, uses the kfm_rsa key created when you executed the migrateKeyFiles script in the previous section.

This script also moves the digest file into place and removes any users who were not selected for migration. The digest is staged in /disk1/keyfiles_staging.

When migrating users to EC 9.0, you can choose to migrate all user-defined users at once or you can choose to be prompted to migrate users one at a time.

Complete the following procedure to migrate users to the SR 9.0 EC.

1. If necessary, change back to the **/opt/cisco/backup_restore** directory.
2. Do you want to migrate all user-defined users at once?
   - If **yes**, go to the next step.
   - If **no** and you want to be prompted to migrate each user-defined user, go to step 5.
3. Enter the following command to migrate all users.

   Note: Substitute the IP address for either the SR 8.0/7.x EC for the [previous_SR_IP] entry in the command. Do not include the brackets.

   Migrate All Users command:

   ```
   sudo ./migrateUsers --source [previous_SR_IP] --all_users
   ```

   Migrate All Users example:

   ```
   [admin@ecnextx9 backup_restore]$ sudo ./migrateUsers --source
   10.90.46.17 --all_users
   ```

   Result: Each user's home directory is present in **/home** on the SR 9.0 EC
4. Go to the next section in this chapter.
5. Enter the following command to be prompted to migrate each user to the SR 9.0 EC.

   Note: Substitute the IP address for the SR 8.0/7.x EC for the [previous_SR_IP] entry in the command. Do not include the brackets.

   Migrate Users command:

   ```
   sudo ./migrateUsers --source [previous_SR_IP]
   ```

   Migrate Users example:

   ```
   [admin@ecnextx9 backup_restore]$ sudo ./migrateUsers --source
   10.90.46.17
   ```

6 When prompted to migrate a user, enter **y** or **n**, as appropriate. The default is **n**.

Important:

- ***Do not*** migrate any system-related users (for example, root, admin, daemon, bin, sys, adm, lp, uucp, nuucp, smmsp, listen, gdm, webservd, postgres and svctag).
- Only migrate users that were created by the system operator and are recognized as user-created accounts.

Result: Once you have responded to all user prompts, each user's home directory is present in **/home** on the SR 9.0 EC.

Migrating the Database and Key Files

Important: Cisco recommends completing this procedure during a maintenance window due to the following:

- The migrateDBKF script will stop all EC processes on the SR 8.0/7.x system.
- All billing transactions and updates to the active SR 8.0/7.x system will be suspended.

In this section, you will migrate the database from SR 8.0/7.x to SR 9.0. This migration script, migrateDBKF, automates a remote database unload of the database(s) and then runs migrateKeyFiles to bring the database(s) over to the local machine. Any new files related to key files are also migrated.

When the migration completes, the migrateDBKF script loads the database(s).

Important: Processes will be stopped on the *primary* EC when running this script. Therefore, it is recommended to execute this procedure in a maintenance window as services will be impacted.

1 Complete the following steps on the ***SR 8.0/7.x*** system.

a As **root** user, enter the following command on the *primary* SR 8.0/7.x EC to ensure that the RepDB database sync is up to date.

Note: The last two lines in the output should be similar to the output in the example below.

Command for SR 8.0 system:

```
[root@ecnextx8 ~]# /opt/cisco/repdb/checkRepDb
```

Command for SR 7.x system:

```
# /opt/SAIrepdb/checkRepDb
```

b Is the database sync up to date?

– If **yes**, go to the next step.

– If **no**, contact Cisco Services.

c Stop all billing transactions and updates to the *primary* EC.

d Enter the following command to disable RepDB on the *primary* EC.

SR 8.0:

```
[root@ecnext8 ~]# /opt/cisco/repdb -d
```

SR 7.x:

```
# /opt/SAIrepdb/RepDb -d
```

e Enter the following command to source the environment variables.

```
[root@ecnext8 ~]# . /dvs/dncs/bin/dncsSetup
```

f Enter the following command to verify that RepDB is disabled.

SR 8.0 system:

```
[root@ecnext8 ~]# onstat -g dri
```

SR 7.x system:

```
# onstat -g dri
```

g Repeat step 1d through 1f on the *secondary* EC.

2 Complete the following steps on the ***SR 9.0*** system.

a Type the following command to migrate the database and any new keyfiles.

Important: Substitute the IP address for SR 8.0/7.x for the [SR8.0/7.x_IP] entry in the command. Do not include the brackets.

Migrate database and key files command:

```
sudo ./migrateDBKF --source [SR8.0/7.x_IP] --db dncs
```

Migrate database and key files example:

```
[admin@ecnextx9 backup_restore]$ sudo ./migrateDBKF
--source 10.90.46.17 --db dncs
```

b When prompted to proceed with the migration, enter **y** and press **Enter**.

Note: This could take up to an hour depending on the size of the database.

3 Does your system use a Cisco Application Server?

Note: The migration should be complete.

- If **yes**, go to the next step.
- If **no**, go to step 7.

4 As **dncs** user on the SR 9.0 system, enter the following commands to ensure that all Application Server processes are not running.

```
[dncs@ecnextx9 ~]$ appStop
[dncs@ecnextx9 ~]$ appKill
```

5 As **root** user, enter the following command to source the environment variables.

```
[root@ecnextx9 ~]# . /dvs/dncs/bin/dncsSetup
```

6 Enter the following command to change the appdb database logging mode to buffered logging.

```
[rootecnextx9 ~]# ontape -s -B appdb
```

7 Complete the following steps on the ***SR 8.0/7.x*** system.

a As **root** user, type one of the following commands to shutdown the *secondary* SR 8.0/7.x EC.

SR 8.0 system:

```
[root@ecnextx8 ~]# shutdown -h now
```

SR 7.x EC system:

```
# shutdown -y -g0 -i0
```

b Repeat step 7a on the *primary* SR 8.0/7.x EC.

8 Go to the next chapter, ***Update the Network Post-Application Installation or Post-Migration*** (on page 77).

6

Update the Network Post-Application Installation or Post-Migration

This chapter includes procedures to update the network configuration and the network adapters, post-application installation and post-migration (if a migration was performed).

In This Chapter

Edit Network Configuration Files

Depending on your network setup, go to one of the following sections to update the network configuration files defined for the SR 9.0 EC.

- ***Editing Configuration Files for Systems Using Unique dncseth and dncsatm Interfaces*** (on page 78)
- ***Editing Configuration Files for Systems Using a Collapsed Interface for dncseth and dncsatm*** (on page 81)

Editing Configuration Files for Systems Using Unique dncseth and dncsatm Interfaces

Complete the following procedure to update the network configuration files defined for the SR 9.0 EC.

1. Enter the following command to go to the **/etc/sysconfig/network-scripts** directory.

   ```
   [admin@ecnextx9 ~]$ cd /etc/sysconfig/network-scripts
   ```

2. Open the **ifcfg-ens192** file in a text editor.

   ```
   [admin@ecnextx9 network-scripts]$ sudo vi ifcfg-ens192
   ```

3. Delete the **GATEWAY** line.
4. Change the **DEFROUTE** value from yes to **no**.
5. Save and close the file.

   Important: Do ***not*** restart the network until you are directed to do so later in this procedure.

6. Open the **ifcfg-ens224** file in a text editor.

   ```
   [admin@ecnextx9 network-scripts]$ sudo vi ifcfg-ens224
   ```

7. Add the following entries to the file:

   Command syntax:

   ```
   GATEWAY=[Gateway for ens224 network]
   DEFROUTE=yes
   ```

   Example:

   ```
   GATEWAY=204.3.1.97
   DEFROUTE=yes
   ```

8 Change the **NM_CONTROLLED** value from yes to **no**.

Example of ifcfg-ens224 file:

```
DEVICE=ens224
BOOTPROTO=none
ONBOOT=yes
IPADDR=204.3.1.97
NETMASK=255.255.255.240
GATEWAY=204.3.1.110
DEFROUTE=yes
IPV6INIT=yes
MTU=1500
NM_CONTROLLED=no
```

9 Save and close the file.

10 Enter the following command to create a routing file for the **ens192** interface.

```
[admin@ecnextx9 network-scripts]$ sudo vi route-ens192
```

11 Add the appropriate routes for your network.

Example file:

```
10.90.0.0/16 via 10.90.44.2 dev ens192
10.82.0.0/16 via 10.90.44.2 dev ens192
10.84.0.0/16 via 10.90.44.2 dev ens192
10.86.0.0/16 via 10.90.44.2 dev ens192
64.100.0.0/16 via 10.90.44.2 dev ens192
64.102.0.0/16 via 10.90.44.2 dev ens192
10.24.0.0/16 via 10.90.44.2 dev ens192
10.78.0.0/16 via 10.90.44.2 dev ens192
10.153.0.0/16 via 10.90.44.2 dev ens192
10.78.192.0/21 via 10.90.44.2 dev ens192
10.143.32.0/23 via 10.90.44.2 dev ens192
172.18.0.0/23 via 10.90.44.2 dev ens192
72.163.47.0/24 via 10..90.44.2 dev ens192
172.36.131.0/24 via 10.90.44.2 dev ens192
```

12 Save and close the file.

13 Is the SR 9.0 EC configured with a ***temporary*** IP address for the corporate network (ens192)?

- If **no** and this was a migration that includes a new IP address, go to step 20.
- If **yes**, go to the next step.

14 Enter the following command to update the **IPADDR** entry to the IP address of the system it was migrated from in the **ens192** configuration file.

```
[admin@ecnextx9 network-scripts]$ sudo vi ifcfg-ens192
```

15 Go to the **IPADDR** entry and update the IP address.

16 Save and close the file.

17 Enter the following command to open the **/etc/hosts** file.

```
[admin@ecnextx9 network-scripts]$ sudo vi /etc/hosts
```

18 Update the IP address for the **dncseth** entry.

19 Save and close the file.

20 Enter the following command to copy an existing configuration file to a configuration file for RepDB.

Notes:

- For this example, we will copy ifcfg-ens224 (headend interface) to ifcfg-ens161 (RepDB interface).
- The ifcfg files are user-defined networks so the naming of your configuration files may be different.

```
[admin@ecnextx9 network-scripts]$ sudo cp ifcfg-ens224
ifcfg-ens161
```

21 Open the **ifcfg-ens161** file in a text editor.

22 From the **DEVICE=** entry, modify the value to match the user-defined network for RepDB.

Example:

```
DEVICE=ens161
```

23 Update the **IPADDR** and **NETMASK** entries to the IP address and netmask for the RepDB network.

24 Delete the **GATEWAY** and **DEFROUTE** lines.

Example RepDB configuration file:

```
DEVICE=ens161
BOOTPROTO=none
ONBOOT=yes
IPADDR=204.3.3.97
NETMASK=255.255.255.240
IPV6INIT=yes
MTU=1500
NM_CONTROLLED=no
```

25 Save and close the **ifcfg-ens161** file.

26 Create any other configuration files as needed.

27 Open any other **ifcfg** configuration files and change the **NM_CONTROLLED** value from yes to **no**.

28 Enter the following command to reboot the EC.

```
[admin@ecnextx9 ~]$ sudo reboot now
```

29 Go to ***Reconnect the Network Adapters*** (on page 83).

Editing Configuration Files for Systems Using a Collapsed Interface for dncseth and dncsatm

Complete the following procedure to update the network configuration files defined for the SR 9.0 EC.

1 Enter the following command to go to the **/etc/sysconfig/network-scripts** directory.

```
[admin@ecnextx9 ~]$ cd /etc/sysconfig/network-scripts
```

2 Open the **ifcfg-ens192** file in a text editor.

```
[admin@ecnextx9 network-scripts]$ sudo vi ifcfg-ens192
```

3 Update the following entries:

Note: Substitute values specific to your network for the terms shown in brackets. Do not include the brackets.

- `DEFROUTE=yes`
- `GATEWAY=[Gateway_IP_address]`
- `NM_CONTROLLED=no`

Example:

```
BOOTPROTO=none
DEVICE=ens192
ONBOOT=yes
TYPE=Ethernet
USERCTL=no
PROXY_METHOD=none
BROWSER_ONLY=no
IPADDR=204.3.1.97
PREFIX=255.255.255.240
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=no
RES_OPTIONS="rotate timeout:1 attempts:1"
NAME="System ens192"
GATEWAY=204.3.1.110
PEERDNS=no
NM_CONTROLLED=no
```

4 Save and close the file.

Important: Do ***not*** restart the network until you are directed to do so later in this procedure.

5 Enter the following command to move the **ifcfg-ens224** file to a new file so it is not recognized as an interface to bring up during a system boot.

Example:

```
[admin@ecnextx9 network-scripts]$ sudo mv ifcfg-ens224
ifcfg-ens224.bak
```

6 Enter the following command to open the **/etc/hosts** file in a text editor.

```
[admin@ecnextx9 network-scripts]$ sudo vi /etc/hosts
```

7 Copy the aliases from the line with the temporary IP address and add them to the end of the **dncsatm** line (for example, 204.3.1.97).

8 Comment out the line with the temporary IP address (for example, 10.90.46.16).

Example:

```
127.0.0.1       localhost       localhost.localdomain localhost4 localhost4.localdomain4 appservatm appserv
_host ppv_manager_host vc_server_host config_manager_host
::1     localhost       localhost.localdomain localhost6 localhost6.localdomain6
#10.90.46.16     ecnext9.vcs.prod       ecnextx9        public-ipv4.local public-ipv4 dncseth
127.0.0.2       dncsws  loopback2 dncswebsvc
192.168.1.1     dncsted-x
192.168.1.2     dncsted
204.3.1.97      dncsatm dncs_host ecnext9.vcs.prod   ecnextx9   public-ipv4.local public-ipv4 dncseth
#
# RepDB
204.3.3.97      HOSTA
204.3.3.98      HOSTB
```

9 Save and close the file.

10 Enter the following command to copy an existing configuration file to a configuration file for RepDB.

Notes:

- For this example, we will copy ifcfg-ens256 (TED interface) to ifcfg-ens161 (RepDB interface).
- The ifcfg files are user-defined networks so the naming of your configuration files may be different.

```
[admin@ecnextx9 network-scripts]$ sudo cp ifcfg-ens256
ifcfg-ens161
```

11 Open the **ifcfg-ens161** file in a text editor and update the following fields.

Note: Substitute values specific to your network for the terms shown in brackets. Do not include the brackets.

- `DEVICE=[network]`
- `IPADDR=[RepDB_IP_Address]`
- `NETMASK=[Network mask]`
- `NM_CONTROLLED=no`

Example:

```
DEVICE=ens161
BOOTPROTO=none
ONBOOT=yes
IPADDR=204.3.3.97
NETMASK=255.255.255.240
IPV6INIT=yes
MTU=1500
NM_CONTROLLED=no
```

12 Save and close the file.

13 Create any other configuration files, as needed.

14 Open any other **ifcfg** files and change the **NM_CONTROLLED** value from yes to **no**.

15 Enter the following command to reboot the EC.

```
[admin@ecnextx9 ~]$ sudo reboot now
```

16 Go to the next section.

Reconnect the Network Adapters

Refer to the appropriate section to reconnect the network adapters for your SR 9.0 VM.

- *Reconnecting Network Adapters for Systems with Unique dncseth and dncsatm Interfaces* (on page 83)
- *Reconnecting Network Adapters for Systems with a Collapsed Network for dncseth and dncsatm* (on page 84)

Reconnecting Network Adapters for Systems with Unique dncseth and dncsatm Interfaces

Important: This procedure only pertains to a system migration. If this is a Greenfield installation, you can skip this section as all of the network adapters should be connected.

Complete the following procedure to reconnect the network adapters on the SR 9.0 VM.

Note: You can complete this procedure while the SR 9.0 is rebooting.

1. From the vCenter Web UI, right-click the SR 9.0 VM and select **Edit Settings**. The Edit Settings window appears.
2. From the Virtual Hardware area, click the dropdown arrow next to **Network adapter 2** and select **Connected**.

   Note: Make sure the **Connect at Power On** option is selected as well.
3. Repeat step 2 for all other network adapters.
4. Click **OK**.
5. From a terminal window, log back into the system as **admin** user.
6. Enter the following command to verify that the default routes are correct.

   ```
   [admin@ecnextx9 ~]$ netstat -nrv
   ```
7. Enter the following command to ensure that all network interfaces are up and that the appropriate IP addresses are plumbed. The first line of the output for each interface you connected should indicate **RUNNING**.

   ```
   [admin@ecnextx9 ~]$ ifconfig -a
   ```
8. Go to *SR 9.0 Post Upgrade Procedures* (on page 85).

Reconnecting Network Adapters for Systems with a Collapsed Network for dncseth and dncsatm

Complete the following procedure to reconnect the network adapters on the SR 9.0 VM.

1. From the vCenter Web UI, right-click the SR 9.0 VM and select **Edit Settings**. The Edit Settings window appears.
2. From the Virtual Hardware area, click the dropdown arrow next to **Network adapter 2** and ***unselect*** the **Connected** and **Connect at Power On** boxes.
3. Click the dropdown arrow next to all other adapters and select **Connected** and **Connect At Power On**.
4. Click **OK**.
5. From a terminal window, log back into the system as **admin** user using the ens192 IP address.
6. Enter the following command to verify that the appropriate network interfaces are up and running. The first line of the output for each interface you connected should indicate **RUNNING**.

   ```
   [admin@ecnextx9  ~]$ ifconfig -a
   ```

7. Enter the following command to verify that the default routes are correct.

   ```
   [admin@ecnextx9  ~]$ netstat -nrv
   ```

7

SR 9.0 Post Upgrade Procedures

Introduction

Note: The procedures in this chapter should be performed after completing a new install or a migration.

Complete the procedures in this chapter to verify that the system is fully functional.

Important: If any of the tests in this chapter fail, troubleshoot the system to the best of your ability. If you are unable to resolve the failure, contact Cisco Services.

In This Chapter

Adding User-defined Entries to the /etc/hosts File

Important: If you migrated from a system other than SR 7.x or if this is a Greenfield installation, skip this procedure and go to ***Creating User Accounts*** (on page 88).

If you migrated from SR 7.x to SR 9.0, complete the following procedure.

1. As **root** user on the SR 9.0 EC, enter the following command to view the hosts file that was migrated from the SR 7.x system.

   ```
   [root@ecnextx9  ~]# cat /disk1/keyfiles_staging/etc/hosts
   ```

2. Copy the output of the file to a text file.
3. Enter the following command to open the **/etc/hosts** file.

   ```
   [root@ecnextx9  ~]# vi /etc/hosts
   ```

4. Compare the output from step 1 to the /etc/hosts file and add any user-defined entries from the /disk1/keyfiles_staging/etc/hosts file to the /etc/hosts file.
5. Save and close the **/etc/hosts** file.

Creating User Accounts

This section describes the types of user accounts that you can create on the EC, while also including the steps to create an Administrator user account.

User Account Types

The following user accounts can be created on the EC.

- **Regular User**
  - Can log into the operating system
  - Cannot read or write EC application files
  - Cannot execute EC application executable files
  - Cannot switch to the dncs user
- **Operator**
  - Can log into the operating system
  - Can read but cannot write EC application files
  - Cannot execute EC application executable files
  - Cannot switch to the dncs user
- **Administrator**
  - Can log into the operating system
  - Can read but not write EC application files
  - Cannot execute EC application executable files
  - Can switch to the dncs user — once switched to the dncs user:
    - Can read and write EC application files
    - Can execute EC application executable files

Creating an Administrative User Account

Important: It is highly recommended that you create an Administrator user account to access the dncs user account. It is best practice ***not*** to use the admin or root user account to access the dncs account.

Complete the following steps to create an Administrator account called "ecadmin". This user account, along with any other Administrative user accounts you create, will be used to sudo to the dncs account, which includes the ability to stop and start system processes.

1. As **admin** user, type the following command to create the **ecadmin** user account on the EC. The USER ADMINISTRATION MENU appears.

   ```
   [admin@ecnextx9 ~]$ sudo /dvs/admin/useradmin
   ```

2. Enter **a** to add a new user and press **Enter**.
3. Type **y** to confirm that you want to add a user and press **Enter**.
4. Select one of the following user types:
   - Add Regular User
   - Add Operator
   - Add Administrator
5. Type **3** to define this user as an Administrative user and press **Enter**.
6. Enter a username called **ecadmin** and press **Enter**.
7. Type **y** to confirm the action and press **Enter** to continue. You are prompted for the password.
8. Enter a password for the user and press **Enter**.

   Note: The password must contain upper and lower case letters, a special character, and a number.
9. Re-type the password and press **Enter**. You are then prompted to enter a password to access the Web UI.
10. Enter a password for this user to access the Web UI.

    Note: You can set this password to anything you want. We suggest that you set it to the same password as your user login password.

11 Re-enter the password for the Web UI and press **Enter**. You are returned to the User menu.

12 Continue adding users for your system, as needed.

13 When you have finished adding users, type **q** to exit the menu.

14 Type **q** again to exit the USER ADMINISTRATION MENU.

15 Are you using LDAP or NIS?

- If **no**, and you are storing passwords locally, go to the next step.
- If **yes**, go to step 18.

16 Enter the following command to reset the password for the **ecadmin** user.

```
[admin@ecnextx9 ~]$ sudo passwd ecadmin
```

17 When prompted, enter the password, and then when prompted again, re-enter the password. A confirmation will display.

Note: You can enter the same password that you used when creating the ecadmin user in the USER ADMINISTRATION MENU.

```
Changing password for user ecadmin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

18 Open a new terminal window to the EC and login as **ecadmin**.

19 Type the following command to verify that you can change to the **dncs** user.

```
[ecadmin@ecnextx9 ~]$ sudo su - dncs
```

20 When prompted, enter the password for the **ecadmin** user.

```
[ecadmin@vodwater ~]$ sudo su - dncs

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for ecadmin:
Working directory is /dvs/dtacs
Database is dtacsdb
```

Note: You should now have two terminal windows open; one as admin user and one as ecadmin user (used to change to dncs).

Set the manage_dncsLog Script Log Retention Variables

In this procedure, you will review and, if necessary, set variables in the manage_dncsLog script. These variables determine the number of days the DBDS core files and logs are kept. DBDS core files and logs can be very large and, under extreme conditions, can be created very rapidly.

Note: If this is an EC migration, you must complete this procedure as the manage_dncsLog script variables are not currently migrated.

The variables are:

- `DAYS_SAVELOGS_KEPT=10`
- `DAYS_COREFILES_KEPT=10`
- `DAYS_CORELOGDIRS_KEPT=10`

As listed above, the default value for each variable is 10 days. DBDS process logs are only saved when the logLvl +ZIP is enabled.

Notes:

- The logLvl command sets logging levels. The +ZIP switch enables the save-log option.
- Cisco recommends that logLvl +ZIP only be enabled when you are attempting to capture logs for processes that are exhibiting a problem. Once sufficient logs have been captured, this should be disabled (-ZIP).

These variables are set to minimize the possibility that core files and logs fill the file system and cause system outages. If you determine that the DBDS logs and/or core files should be kept for a longer or shorter period, follow these instructions to set the variables.

1. As **dncs** user, open the **/dvs/dncs/etc/manage_dncsLog** file in a text editor.
   ```
   [dncs@ecnextx9 ~]$ vi /dvs/dncs/etc/manage_dncsLog
   ```
2. Locate the **DAYS_SAVELOGS_KEPT** variable and change the value to the appropriate number of days.
3. Locate the **DAYS_CORELOGDIRS_KEPT** variable and change the value to the appropriate number of days.
4. Locate the **DAYS_COREFILES_KEPT** variable and change the value to the appropriate number of days.
5. Save and close the file.

Update the osmAutoMux.cfg File

Important: If your system is not using the osmAutoMux file, you can skip this procedure.

The osmAutoMux.cfg configuration file must include a headend map entry (HEMAP). If this entry is not present in the osmAutomux.cfg file, the code version table (CVT) will not be generated for remote BFS QAMs.

The following line must be added to the osmAutoMux.cfg file:

```
HEMAP|1|200
```

Note: 1 is the local headend ID and 200 is the sample headend ID.

Follow these steps to add the HEMAP entry to the osmAutoMux.cfg file.

1. As **dncs** user, enter the following command to change to the **/dvs/dvsFiles/OSM** directory.

   ```
   [dncs@ecnextx9 ~]$ cd /dvs/dvsFiles/OSM
   ```

2. Edit the **osmAutoMux.cfg** file in a text editor.

   ```
   [dncs@ecnextx9 OSM]$ vi /dvs/dvsFiles/OSM/osmAutoMux.cfg
   ```

3. Add the following entry to the end of the file.

   ```
   HEMAP|1|200
   ```

4. Save and close the file.

Modify the dncs User .profile File

In this section, review and adjust the .profile file for the following items:

- Variables that are required for Emergency Alert Messages (EAM).
- If your site is not SSP2.3 Compliant, you need to add the following entry to the EC .profile file as **dncs** user.

Note: If you have completed the procedures to this point, you should be logged in as **dncs** user.

1. As **dncs** user, type `cd` to go to the **/home/dncs** directory.
2. Enter the following command to verify the DNCS/EC management IP address includes the **dncseth** alias.

   ```
   [dncs@ecnextx9 ~]$ grep -i dncseth /etc/hosts
   ```

   Example output:

   ```
   10.90.46.17   ecnextx9.vcs.prod  ecnextx9 public-ipv4.local
                 public-ipv4 dncseth
   ```

3. Does the entry for the management IP address include the `dncseth` alias?
   - If **yes**, go to step 5.
   - If **no**, open the **/etc/hosts** file and add **dncseth** to the end of the entry.
4. Save and close the file.
5. Enter the following command to check for the LOCAL_EAS_IP in the **.profile** file.

   ```
   [dncs@ecnextx9 ~]$ grep -i local_eas /home/dncs/.profile
   ```

   Example output:

   ```
   LOCAL_EAS_IP=10.90.46.17 ; export LOCAL_EAS_IP
   ```

6. Does the output identify the LOCAL_EAS_IP has being set to either **dncseth** or to the IP address of the management/dncseth network?
   - If **yes**, go to step 11.
   - If **no**, go to the next step.
7. Open the **.profile** file in a text editor.
8. Is the export LOCAL_EAS_IP entry present?
   - If **yes**, update the entry to **dncseth**.
   - If **no**, add the following entry.

     ```
     export LOCAL_EAS_IP=dncseth
     ```

9. Save and close the file.
10. Type `. ./.profile` so the system uses the updated .profile file.

    Note: Be sure to type a space between the first two periods.

11 Is your site SSP2.3 compliant?

- If **yes**, you have completed this procedure.
- If **no**, open the .profile file in a text editor.

```
[dncs@ecnextx9 ~]$ vi .profile
```

12 Go to the end of the file and add the following content.

```
# VOD variable for systems that are not SSP2.3-compliant
DNCS_DRM_INCLUDE_HE_RSR_VOD=1
export DNCS_DRM_INCLUDE_HE_RSR_VOD
```

Note: If you are not sure what this means, or how to do this, contact Cisco Services.

13 Save and close the file.

Add the DrmCheckVodZeroScrIp Environment Variable in the .profile File

Important: This section applies to systems that include a VOD server that is running in a single element environment with direct connections to the MPEG source.

Complete the following procedure to add the DrmCheckVodZeroScrIp environment variable with a value of 1 to the dncs user .profile file.

Note: If you have completed the procedures to this point, you should be logged in as **dncs** user and in the **/home/dncs** directory.

1 Open the **.profile** file in a text editor.

```
[dncs@ecnextx9 ~]$ vi .profile
```

2 Move to the end of the file and add the following entries:

```
# VOD Server
 export DrmCheckVodZeroScrIp=1
```

3 Save and close the **.profile** file.

4 Type `. ./.profile` so the system uses the updated .profile file.

Note: Be sure to type a space between the first two periods.

Modify the .profile File for DSG

Important: If your system was not configured for DSG BFS, you can skip this procedure.

In this procedure, you will update your system to use DSG BFS.

Note: If you have completed the procedures to this point, you should be logged in as **dncs** user and in the **/home/dncs** directory.

1. Enter the following command to see if the **dncs_bfsRemote=dncsdsg** entry exists.

   ```
   [dncs@ecnextx9 ~]$ grep dncs_bfsRemote .profile
   ```

2. Did **export dncs_bfsRemote=dncsdsg** display in the output?

   - If **yes**, you have completed this procedure.
   - If **no**, enter the following command to open the **.profile** file in a text editor.

     ```
     [dncs@ecnextx9 ~]$ vi .profile
     ```

3. Add the following entry.

   ```
   export dncs_bfsRemote=dncsdsg
   ```

4. Save and close the file.
5. Type **exit** to log out of the dncs session. You are returned to the ecadmin session.
6. Enter the following command to change back to **dncs** user.

   ```
   [ecadmin@ecnextx9 ~]$ sudo su - dncs
   ```

7. Enter the following command to verify the **bfsRemote** setting. The output should be **dncsdsg**.

   ```
   [dncs@ecnextx9 ~]$ echo $dncs_bfsRemote
   ```

   Example output:

   ```
   dncsdsg
   ```

Delete Solaris-specific Entries

Important: This section applies only to systems that were migrated to SR <SR< from SR 7.x. If your system was migrated from SR 8.0 or built as a Greenfield installation, go to the next section.

Complete the following steps to remove any Solaris-specific entries from the .profule file.

Note: If you have completed the procedures to this point, you should be logged in as **dncs** user and in the **/home/dncs** directory.

1 Open the **.profile** file in a text editor.

```
[dncs@ecnextx9 ~]$ vi .profile
```

2 Browse through the file to locate any Solaris-specific entries.

Example entry in a .profile file:

```
DNCS_VERSION=`pkginfo -l SAIdncs |grep VERSION |awk '{print
$2}'`
echo ""
```

3 Comment out each line that pertains to Solaris.

Example:

```
#DNCS_VERSION=`pkginfo -l SAIdncs |grep VERSION |awk '{print
$2}'`
#echo ""
```

4 Save and close the file.

5 Type `. ./.profile` so the system uses the updated .profile file.

Note: Be sure to type a space between the first two periods.

Update the site_info Database Table for a Hostname Change

Important:

- If this is a new install you can skip this procedure.
- If this is a migration from SR 8.0/7.x to SR 9.0 in which the hostname of each system is the same, you can skip this procedure.

Complete this procedure *only* if your SR 9.0 system was a migration in which the hostname was changed to a new hostname. The new hostname would have been defined the ec.envfile in ***Installing EC 9.0*** (on page 55).

Note: For this procedure, we will assume the SR 8.0/7.x hostname is "dncs" and the hostname that was added to the ec.envfile is "ecnextx9".

1 As **dncs** user, enter the following command to verify the current hostname and the dncsatm IP address for the SR 9.0 system.

```
[dncs@ecnextx9 ~]$ hostname; grep dncsatm /etc/hosts
```

Example output:

```
ecnextx9
204.3.1.97      dncsatm dncs_host
```

2 Enter the following command to access the **dncs** database. A database prompt appears.

```
[dncs@ecnextx9 ~]$ dbaccess dncsdb -
```

3 Enter the following command to view the output of the **site_info** table.

```
> select * from site_info;
```

Example output:

```
site_id             1
site_name           DNCS
bfs_sess_mac_addr   00:00:00:00:00:00
site_ip_address     10.253.3.1
site_mac_address    00:00:00:00:00:00
site_hostname       dncs
site_status         1
oob_flow_ipaddr
gda
gda_port            0
```

4 Does the **site_hostname** entry match the hostname displayed in the output from step 1?

- If **no**, go to the next step.
- If **yes**, go to step 7.

5 Enter the following command and press **Enter** to update the **site_hostname** entry. A "1 row(s) updated" message displays and then you are returned to the database prompt.

Command syntax:

```
update site_info set site_hostname="[new_hostname]" where
site_id=[site_id value];
```

Example:

```
> update site_info set site_hostname="ecnextx9" where
site_id=1;
```

6 Enter the following command to verify that the **site_hostname** entry was successfully updated in the site_info table.

```
> select * from site_info;
```

7 Does the **site_ip_address** entry match the dncsatm IP address in the output from step 1?

- If **no**, go to the next step.
- If **yes**, go to step 10.

8 Enter the following command and press **Enter** to update the **site_ip_address** entry. A "1 row(s) updated" message displays and then you are returned to the database prompt.

Command syntax:

```
update site_info set site_ip_address="[new_dncsatm_IP]" where
site_id=[site_id value];
```

Example:

```
> update site_info set site_ip_address="204.3.1.97" where
site_id=1;
```

9 Enter the following command to verify that **site_ip_address** entry was successfully updated in the site_info table.

```
> select * from site_info;
```

10 If the entries are correct, press **Ctrl+C** to exit the database.

Verifying the EC Certificate Configuration

Complete the following procedure to verify the configuration of the EC certificate/key pair.

Note: Once all NextX nodes on your system are configured for certificates, refer to the **Verify Inter-Node Encrypted Communication** procedure in Appendix B of the ***Admin Node 2.0 Installation Guide***. This procedure allows you to execute encrypted communication checks for all nodes, including the ECs.

1 As **admin** user in the ***Admin Node*** terminal window, enter the following command to check the certificate configuration for the EC. A validation of the certificate file occurs.

Command syntax:

```
sudo /opt/cisco/ca/checkConfig -s [hostname].env
```

Example:

```
[admin@adminnodenextx90 ~]$ sudo /opt/cisco/ca/checkConfig -s
ecnextx9.env
```

2 Review the log in the **/var/log** directory.

Note: The log will be in the following format **checkConfig[date].log** (for example, /var/log/checkConfig20180503.log).

3 If the following errors exist and you are ***NOT*** regionalizing your system to an ECS, ignore the errors.

Example error output:

```
ERROR if regionalized (10.90.46.17) consul is not running
10.90.46.17 has oammgrctrl enabled at MULTIUSER
10.90.46.17 has oammgrctrl running
10.90.46.17 has tomcat enabled at MULTIUSER
10.90.46.17 has tomcat running
10.90.46.17 has httpd enabled at MULTIUSER
10.90.46.17 has httpd running
10.90.46.17 has httpd-dncsws enabled at MULTIUSER
10.90.46.17 has httpd-dncsws running
ERROR (10.90.46.17), not found but expected for node type:
/etc/consul/config.json
```

4 Did any other errors display?

- If **no**, go to the next step.
- If **yes**, contact Cisco Services.

5 Are you regionalizing the EC to an ECS?

- If **yes**, refer to **Appendix B** in the ***ECS 3.0 Installation and Upgrade Guide*** to regionalize it to the ECS. Once the EC is regionalized, go to the next step.
- If **no** and you do not wish to regionalize the EC to an ECS, go to the next section.

6 As **admin** user on the ***EC***, enter the following command to start the consul service.

```
[admin@ecnextx9 ~]$ sudo systemctl restart consul
```

7 Enter the following command to view the status of the **consul** service.

```
[admin@ecnextx9 consul]$ systemctl status consul
```

8 Enter the following command to enable the **consul** service to start on boot.

```
[admin@ecnextx9 ~]$ sudo systemctl enable consul
```

9 Enter the following command to verify that the **consul** service is enabled to start on boot.

```
[admin@ecnextx9 ~]$ systemctl list-unit-files | grep -i consul
```

Example output:

```
consul.service                enabled
```

10 Enter the following command to verify that the EC is now in the current list of members that the Consul knows about.

```
[admin@ecnextx9 ~]$ sudo consul members
```

Example output:

```
Node       Address              Status  Type    Build  Protocol  DC   Segment
consul1tp  10.90.181.189:8301  alive   server  1.0.1  2         dc1  <all>
consul2tp  10.90.181.190:8301  alive   server  1.0.1  2         dc1  <all>
consul3tp  10.90.181.191:8301  alive   server  1.0.1  2         dc1  <all>
ecnextx9   10.90.46.17:8301    alive   client  1.0.1  2         dc1  <default>
vcs1tp     10.90.181.192:8301  alive   client  1.0.1  2         dc1  <default>
```

Add IPG_TVDATA_NEW to appservSetup

Important: Only execute this procedure if you use TVDATA for IPG.

Was the IPG_TVDATA_NEW variable found in the appservSetup file during pre-upgrade checks?

- If **yes**, as **dncs** user add the variable to the **/home/dncs/.profile** file exactly as it was in the old system.

  Note: This variable should have been saved and recorded in ***Checking for the IPG_TVDATA_NEW Variable in appservSetup*** (on page 22).

- If **no**, continue with the next procedure.

Setting Up SFTP Support

Important: Only complete the procedures in this section if SFTP support is required at your site.

This section describes how to add an SFTP user for SFTP support. It also includes procedures to restrict SFTP to a single home directory.

Creating a User for SFTP Support

Complete the following procedure to create an SFTP user.

1. As **admin** user, enter the following command to create an SFTP user. The USER ADMINISTRATION MENU displays.

   ```
   [admin@ecnextx9 ~]$ sudo /dvs/admin/useradmin
   ```

2. Type **a** and press **Enter**.
3. When prompted to add a new user, type **y** and press **Enter**.
4. Type **1** and press **Enter** to add a regular user.
5. At the **New Username** prompt, type a name for this user (for example, sftpuser1).
6. When prompted to continue to add this user, type **y** and press **Enter**.
7. At the **New password** prompt, enter a new password (for example, sftpuser1) and press **Enter**.
8. At the **Retype a new password** prompt, re-enter the password and press **Enter**.
9. Type **q** to exit from adding any other users.
10. Type **q** to exit the USER ADMINISTRATION MENU. You are returned to an admin prompt.
11. Enter the following command to reset the password for the SFTP user.

    Command syntax:

    ```
    sudo passwd [SFTP-username]
    ```

    Example:

    ```
    [admin@ecnextx9 ~]$ sudo passwd sftpuser1
    ```

12. When prompted, enter the same or a new password for the SFTP user.
13. When prompted to re-enter the password, re-enter it.

    Important: By default, the password for the SFTP user will expire in 91 days. Your system administrator must decide the password expiration policies for the SFTP user.

Creating a Directory for SFTP File Transfers

Complete the following steps to create a directory that restricts SFTP access to a single home directory. The directory you create and all directories above it *must* be owned by root and have write permissions only for root.

Note: This directory must be created under /dvs.

1 Enter the following command to create a directory in **/dvs**.

Command syntax:

```
sudo mkdir /dvs/[SFTP-home-directory]
```

Example:

```
[admin@ecnextx9 ~]$ sudo mkdir /dvs/sftpuser1
```

2 Enter the following command to set the ownership of the new SFTP home directory to **root:root**.

Command syntax:

```
sudo chown root:root /dvs/[SFTP-home-directory]
```

Example:

```
[admin@ecnextx9 ~]$ sudo chown root:root /dvs/sftpuser1
```

3 Enter the following command to update the permissions of the SFTP home directory to **0755**.

Command syntax:

```
sudo chmod 0755 /dvs/[SFTP-home-directory]
```

Example:

```
[admin@ecnextx9 ~]$ sudo chmod 0755 /dvs/sftpuser1
```

4 Enter the following commands to create an upload directory under the new SFTP home directory and then change its ownership to the SFTP user with a directory permission of **0700**.

Command syntax:

```
sudo mkdir /dvs/[SFTP-username]/[upload-directory]
sudo chown [SFTP-username]:[SFTP-username]
/dvs/[SFTP-username]/[upload-directory]
sudo chmod 0700 /dvs/[SFTP-home-directory]
```

Example:

```
[admin@ecnextx9 ~]$ sudo mkdir /dvs/sftpuser1/uploads
[admin@ecnextx9 ~]$ sudo chown sftpuser1:sftpuser1
/dvs/sftpuser1/uploads
[admin@ecnextx9 ~]$ sudo chmod 0700 /dvs/sftpuser1/uploads
```

Restricting SFTP Access to a Single Directory

Complete the following steps to restrict SFTP access to a single directory.

1. Open the **/etc/ssh/sshd_config** file in a text editor.

   Important: Make sure you open and edit the **sshd_config** file and ***not*** the ssh_config file.

   ```
   [admin@ecnextx9 ~]$ sudo vi /etc/ssh/sshd_config
   ```

2. Go to the end of the file and add the following content:

   Command syntax:

   ```
   Match User [SFTP-username]
   ForceCommand internal-sftp
   PasswordAuthentication yes
   ChrootDirectory /dvs/[SFTP-home-directory]
   PermitTunnel no
   AllowAgentForwarding no
   AllowTcpForwarding no
   X11Forwarding no
   ```

   Example:

   ```
   Match User sftpuser1
   ForceCommand internal-sftp
   PasswordAuthentication yes
   ChrootDirectory /dvs/sftpuser1
   PermitTunnel no
   AllowAgentForwarding no
   AllowTcpForwarding no
   X11Forwarding no
   ```

3. Save and close the file.
4. Enter the following command to restart the **sshd** service.

   ```
   [admin@ecnextx9 ~]$ sudo systemctl restart sshd
   ```

Verifying the SFTP Configuration

Complete the following steps to verify the SFTP configuration.

1. Enter the following command to verify that you ***cannot*** connect to the sftpuser via SSH.

   Command syntax:

   ```
   sudo ssh [SFTP-username]@localhost
   ```

   Example:

   ```
   [admin@ecnextx9 ~]$ sudo ssh sftpuser1@localhost
   ```

2 When prompted, enter the password for the SFTP user. The following response should display and you should be denied the sftp connection.

```
This service allows sftp connections only.
Connection to localhost closed.
```

3 Enter the following command to verify that you ***can*** complete an SFTP request as the SFTP user.

Command syntax:

```
sudo sftp [SFTP-username]@[EC_IP_address]
```

Example:

```
[admin@ecnextx9 ~]$ sudo sftp sftpuser1@10.90.46.17
```

4 When prompted to confirm the sftp session, type **yes** and press **Enter**.

5 When prompted for the password of the SFTP user, enter the password and press **Enter**. You are connected to the local host and a sftp prompt displays.

6 At the **sftp>** prompt, type **dir**. Your SFTP upload directory should display. You should be able to read and write into the directory.

Command:

```
sftp> dir
```

Example output:

```
uploads
```

7 Enter the following command to go to the upload directory you created.

Important: You must be in the upload directory to transfer a file via SFTP.

Command syntax:

```
cd [upload_directory]
```

Example:

```
sftp> cd uploads
```

8 Attempt to execute a file transfer to and from the directory.

Note: In this example, we will transfer a file called **testfile** to the upload directory. The testfile file is in the /home/admin directory on another system.

```
sftp> put /home/admin/testfile
```

Example output:

```
Uploading /home/admin/testfile to /uploads/testfile
/home/admin/testfile          100%  246    13.1KB/s   00:00
```

9 Enter `ls` and press **Enter** to verify that the file is present in the **upload** directory.

10 Type the following command to exit the session.

```
sftp> quit
```

Remove Old BFS Entries

In this procedure, you will remove old BFS entries in the /dvs/dvsFiles/BFS_REMOTE directory.

1 As **dncs** user, type the following command and press **Enter** to check for old entries in the **/dvs/dvsFiles/BFS_REMOTE** directory:

```
[dncs@ecnextx9 ~]$ ls /dvs/dvsFiles/BFS_REMOTE
```

2 Did the output from step 1 reveal any files or directories?

- If **yes**, type the following command and press **Enter** to remove these files or directories:

  ```
  [dncs@ecnextx9 BFS_REMOTE]$ rm -rf
  /dvs/dvsFiles/BFS_REMOTE/RF
  ```

- If **no**, you have completed this procedure.

Stop and Disable Unneeded Processes

After the upgrade completes and the processes are started, all processes will be running (green). If your system includes dncs processes that were not running or enabled before the upgrade, they should be stopped and/or disabled after the upgrade.

Example: The example used throughout this procedure involves stopping and disabling the saManager process.

1 As **dncs** user, type the following command and press **Enter**. The System Control Menu appears.

```
[dncs@ecnextx9 ~]$ dncsControl
```

```
| System state: run/run   since 2017-03-06T21:43:50Z       03/10/17 15:46:39
|                           System Control Menu
--------------------------------------------------------------------------------
| -> Main Menu
--------------------------------------------------------------------------------
         1. Startup / Shutdown System
         2. Startup / Shutdown Single Group or Process
--------------------------------------------------------------------------------
         3. Define / Update Applications
         4. Define / Update Groups
         5. Define / Update Processes
         6. Update System
--------------------------------------------------------------------------------
         x. Exit Menu.
--------------------------------------------------------------------------------
Enter a menu option number, or 'X' to exit.
Enter Menu Option>
```

2 Navigate to the appropriate menus to disable unneeded processes.

3 When all unneeded processes are disabled, following the on-screen instructions to exit the dncsControl script.

Add External Database Listener for Third Party Application Servers

Important:

- This procedure is required if the site being upgraded uses a third-party application server.
- System processes should not be running. If they are, refer to ***Stop System Processes and Kill Active Sessions*** (on page 237) to stop them now. Then return to this procedure.

1 As **root** user, enter the following command to source the environment.

```
[root@ecnextx9 ~]# . /dvs/dncs/bin/dncsSetup
```

2 Enter the following command to open the **sqlhosts** file in a text editor.

```
[root@ecnextx9 ~]# vi /opt/cisco/informix/server/etc/sqlhosts
```

3 Go to the end of the file and add the following entry.

```
dncsatmDbServer     onsoctcp   dncsatm   sqlexec
```

4 Save and close the file.

5 Enter the following command to open the **onconfig** file in a text editor.

```
[root@ecnextx9 ~]# vi /opt/cisco/informix/server/etc/onconfig
```

6 Go to the DBSERVERALIASES entry and add **dncsatmDbServer** to the end of the line.

Example entry:

```
DBSERVERALIASES demo_on,localhost_tcp, dncsatmDbServer
```

7 Type the following command to restart the database listeners.

Command syntax:

```
onmode -P start [Listener]
```

Example:

```
[root@ecnextx9 ~] onmode -P start dncsatmDbServer
```

8 Repeat step 7 for each listener you may have in your system.

9 Type the following command and press **Enter** to ensure that the Informix listener(s) are running on the dncsatm interface or whatever external interface was previously configured, as well as on the loopback interface:

```
[root@ecnextx9 ~]$ netstat -an |grep 9088
```

Example output: Output should be similar to the following example:

```
tcp      0   0 172.16.3.131:9088     0.0.0.0:*     LISTEN
tcp      0   0 127.0.0.1:9088        0.0.0.0:*     LISTEN
```

Post Install Tasks When Using RCAS

Important:

- If your system is not using a Remote Conditional Access System (RCAS), you can skip this procedure and go to the next section.
- If you have not already configured the database listener, go to the previous section, ***Add External Database Listener for Third Party Application Servers*** (on page 108), to do so now.

Complete the following procedure if your system uses RCAS.

1. Open the **/etc/hosts.equiv** in a text editor and add the following entry.

   Syntax:

   ```
   [RCAS hostname]     dncs
   ```

   Example entry:

   ```
   rcas.he.15          dncs
   ```

2. Save and close the file.
3. As **root** user on the ***RCAS*** server, enter the following command to edit the ***sqlhosts*** server.

   ```
   [root@ecnextx9 ~]# vi /export/home/informix/etc/sqlhosts
   ```

4. Go to the end of the file and add the following line.

   ```
   dncsatmDbServer     ontlitcp    dncsatm    sqlexec
   ```

5. Save and close the file.
6. Enter the following command to open the **/etc/services** file in a text editor.

   ```
   [root@ecnextx9 ~]# vi /etc/services
   ```

7. Modify the **informixOnline** and **sqlexec** lines as shown below.

   ```
   informixOnline    3010/tcp
   sqlexec           9088/tcp
   ```

8. Save and close the **/etc/services** file.
9. As **dncs** user on the ***RCAS*** server, enter the following command to execute a RCAS database sync.

   ```
   [dncs@ecnextx9 ~]$ ./dvs/rcas/bin/rcasSetup;
   /dvs/rcas/bin/rcasdbsync -S
   ```

   Example output:

   ```
   ……
   -- (19762) rcasdbsync ENDED on Thu Jun 28 13:49:23 EDT 2018
   -- (19762) Finished sync of rcasdb_1 with data from the
   dncsdb@"dncsatmDbServer" ...
   -- (19762) Sending Dbsync End Event - Succeeded ...
   ```

10 Enter the following command to verify that the database sync was successful

```
[dncs@ecnextx9 ~]$ ./checksync
```

Example output:

```
./checksync Version 6.0
Thu Jun 28 13:56:50 EDT 2018
Thu Jun 28 17:56:50 GMT 2018

-- Active Database ................ : rcasdb_1
-- Sync Status is ................. : DB_READY_TO_SYNC
-- Last time synced GMT ........... : 2018-06-28 17:49:23
-- Database to sync or to be synced : rcasdb_2
-- Remote DNCS database ........... : dncsdb@"dncsatmDbServer"

Thu Jun 28 13:56:50 EDT 2018
Thu Jun 28 17:56:50 GMT 2018

================================================================================
(19762) rcasdbsync RUN ON Thu Jun 28 13:48:42 EDT 2018 >>> Status
================================================================================

-- (19762) rcasdbsync ENDED on Thu Jun 28 13:49:23 EDT 2018
-- (19762) Finished sync of rcasdb_1 with data from the dncsdb@"dncsatmDbServer" ...
-- (19762) Sending Dbsync End Event - Succeeded ...
```

Configure FTP

Configuring FTP Users and Start the vsftpd Service

Important: Complete this procedure only if the FTP service is required on your system.

The vfstpd daemon (very secure FTP daemon) is the default FTP server used in CentOS.

For security reasons, the vsftpd service does not run at initial install/bootup. The following procedure must be performed must be performed to configure FTP users, provide FTP access to the users and to start the vfstp service.

1. As **admin** user, enter the following command to open the **/etc/vsftpd/user_list** file in a text editor.

   ```
   [admin@ecnextx9 ~] $ sudo vi /etc/vsftpd/user_list
   ```

2. Add an entry for the **easftp** and **dncsftp** users.
3. Save and close the file.

Setting Multiple FTP Connections from a Single IP Address

Important: In some cases, the MAS server opens over 400 connections from the same IP address at one time. This procedure is ***required*** if this occurs at your site.

The default number of FTP connections from a single IP address is 50. Complete the following procedure if you need to increase the number of allowable FTP connections.

Note: If you do not need more than 50 FTP connections from one IP address, go to the next section to start the **vsftpd** service.

1. As **admin** user, enter the following command to open the vsftpd configuration file in a text editor.

   ```
   [admin@ecnextx9 ~] $ sudo vi /etc/vsftpd/vsftpd.conf
   ```

2. Go to the end of the file and add the following content to allow an unlimited number of connections per IP address.

   ```
   ## added because the MAS opens 400+ ftp connections at one time
   max_per_ip=0
   ```

3. Save and close the file.
4. Go to the next section to restart the **vsftpd** service.

Starting the vsftpd Service

Complete the following procedure if you configured FTP users and/or modified the **vsftpd.conf** file.

1. Enter the following command to start the **vsftpd** service.

   ```
   [admin@ecnextx9 ~]$ sudo systemctl start vsftpd
   ```

2. Enter the following command to verify that the service has started.

   ```
   [admin@ecnextx9 ~]$ systemctl status vsftpd
   ```

3. Enter the following command to set the **vsftpd** service to start automatically at bootup.

   ```
   [admin@ecnextx9 ~]$ sudo systemctl enable vsftpd
   ```

Configuring snmpd Traps on the EC Node

Important: This section should *only* be completed if the EC is or will be regionalized to an ECS.

Complete the following steps to update the snmpd configuration file to configure alarm forwarding to the VCS Console for the following services:

- dncsInitd
- appInitd
- tomcatmon
- httpd
- httpd-dncsws
- oammgr
- consul

1 As **admin** user, enter the following command to update the **snmpd.conf** file in a text editor.

```
[admin@ecnextx9 ~]$ sudo vi /etc/snmp/snmpd.conf
```

2 Go to the end of the file and add the following content.

Note: Ensure that you do not copy and paste any carriage returns as these will cause issues with the snmpd.conf file

```
# Monitor consul process and send traps
view systemview included .1.3.6.1.4.1.1429 #cisco
view systemview included .1.3.6.1.4.1.2021 #ucd
rwcommunity cisco
rocommunity Public
proc dncsInitd 1 1
proc appInitd 1 1
proc tomcatmon 1 1
proc httpd
proc httpd-dncsws
proc oammgr 1 1
proc consul 1 1
monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.1 -o
.1.3.6.1.4.1.2021.2.1.101.1 "EC application has stopped." -o
.1.3.6.1.4.1.2021.2.1.100.1 .1.3.6.1.4.1.2021.2.1.100.1 != 0
monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.1 -o
.1.3.6.1.4.1.2021.2.1.101.1 "EC application is running." -o
.1.3.6.1.4.1.2021.2.1.100.1 .1.3.6.1.4.1.2021.2.1.100.1 == 0
```

```
monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.2 -o
.1.3.6.1.4.1.2021.2.1.101.2 "AppServer has stopped." -o
.1.3.6.1.4.1.2021.2.1.100.2 .1.3.6.1.4.1.2021.2.1.100.2 != 0

monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.2 -o
.1.3.6.1.4.1.2021.2.1.101.2 "AppServer is running." -o
.1.3.6.1.4.1.2021.2.1.100.2 .1.3.6.1.4.1.2021.2.1.100.2 == 0

monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.3 -o
.1.3.6.1.4.1.2021.2.1.101.3 "EC Tomcat service has stopped." -
o .1.3.6.1.4.1.2021.2.1.100.3 .1.3.6.1.4.1.2021.2.1.100.3 != 0

monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.3 -o
.1.3.6.1.4.1.2021.2.1.101.3 "EC Tomcat service is running." -o
.1.3.6.1.4.1.2021.2.1.100.3 .1.3.6.1.4.1.2021.2.1.100.3 == 0

monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.4 -o
.1.3.6.1.4.1.2021.2.1.101.4 "EC HTTP service has stopped." -o
.1.3.6.1.4.1.2021.2.1.100.4 .1.3.6.1.4.1.2021.2.1.100.4 != 0

monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.4 -o
.1.3.6.1.4.1.2021.2.1.101.4 "EC HTTP service is running." -o
.1.3.6.1.4.1.2021.2.1.100.4 .1.3.6.1.4.1.2021.2.1.100.4 == 0

monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.5 -o
.1.3.6.1.4.1.2021.2.1.101.5 "EC HTTP-DNCSWS service has
stopped." -o .1.3.6.1.4.1.2021.2.1.100.5
.1.3.6.1.4.1.2021.2.1.100.5 != 0

monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.5 -o
.1.3.6.1.4.1.2021.2.1.101.5 "EC HTTP-DNCSWS service is
running." -o .1.3.6.1.4.1.2021.2.1.100.5
.1.3.6.1.4.1.2021.2.1.100.5 == 0

monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.6 -o
.1.3.6.1.4.1.2021.2.1.101.6 "OAM service has stopped." -o
.1.3.6.1.4.1.2021.2.1.100.6 .1.3.6.1.4.1.2021.2.1.100.6 != 0

monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.6 -o
.1.3.6.1.4.1.2021.2.1.101.6 "OAM service is running." -o
.1.3.6.1.4.1.2021.2.1.100.6 .1.3.6.1.4.1.2021.2.1.100.6 == 0

monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.7 -o
.1.3.6.1.4.1.2021.2.1.101.7 "Consul process has stopped." -o
.1.3.6.1.4.1.2021.2.1.100.7 .1.3.6.1.4.1.2021.2.1.100.7 != 0

monitor -r 5 -u admin -i -o .1.3.6.1.4.1.2021.2.1.2.7 -o
.1.3.6.1.4.1.2021.2.1.101.7 "Consul process is running." -o
.1.3.6.1.4.1.2021.2.1.100.7 .1.3.6.1.4.1.2021.2.1.100.7 == 0

rwuser admin

iquerySecName admin

agentSecName admin
```

3 Is your system regionalized to an ECS?

- If **yes**, go to the next step.
- If **no**, add the following line to the end of the file. Then go to the next step.

```
trapsess -v 2c -c public localhost:162
```

4 Save and close the file.

5 Enter the following command to restart the snmpd process.

```
[admin@ecnextx9 ~]$ sudo systemctl restart snmpd
```

Clean Up the .bashrc File

Important: If you received a warning concerning the .bashrc file after running the preUpgradeChecks script on an SR 7.x system, you ***must*** execute this procedure on the SR 9.0 system. This must be completed ***BEFORE*** starting system processes.

1. As **admin** user, enter the following command to open the **.bashrc** file in a text editor.

   ```
   [admin@ecnextx9 ~]$ sudo vi /home/dncs/.bashrc
   ```

2. Delete the content in the file.
3. Add the following content to the file:

   ```
   # Source global definitions
   if [ -f /etc/bashrc ]; then
           . /etc/bashrc
   fi
   # User specific aliases and functions
   if [ -r ~/.profile ]; then . ~/.profile;fi
   ```

4. Save and close the file.

Reinstall the Application for Network Devices (Migrated Systems Only)

Important: Only complete this procedure if the SR 9.0 system was migrated from SR 8.0/7.x. This must be completed ***before*** resetting the modulators.

Because your EC system was migrated to SR 9.0, the application and configuration files for network elements (for example, GQAMs, MQAMs, QPSKs) will not download the new code deployed with the SR 9.0 installation.

Complete the following steps to download and install the application package for each network device in your system.

1 As **root** user, enter the following command to change to the **/var/lib/tftpboot** directory.

```
[root@ecnextx9 ~]# cd /var/lib/tftpboot
```

2 Enter the following command to list the configuration files for network elements.

```
[root@ecnextx9 tftpboot]# ls -ltr *.config
```

3 Move *each* .config file to **.config.bak**.

Example:

```
[root@ecnextx9 tftpboot]# mv mqam.config mqam.config.bak
```

4 Enter the following command to reinstall the application for a network element. An **Is this ok [y/d/N]** message displays.

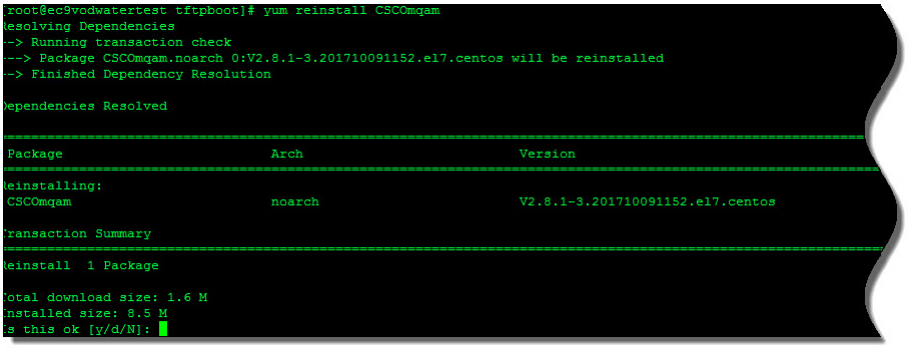
Command syntax:

```
yum reinstall [package_name]
```

Example for GQAM:

```
[root@ecnextx9 tftpboot]# yum reinstall CSCOmqam
```

Example:



5 When prompted to reinstall the package, type **y** and press **Enter**. A **Complete!** message displays.

6 Enter the following command to verify that the package installation date reflects the proper timestamp.

Command syntax:

```
rpm -qi [package_name] | grep "Install Date"
```

Example: CSCOmqam

```
[root@ecnextx9 tftpboot]# rpm -qi CSCOmqam | grep "Install
Date"
```

Example output:

```
Install Date: Mon 23 Feb 2019 03:46:36 PM EDT
```

7 Repeat steps 4 through 6 for each network element in your system.

Restart Apache and Tomcat Services

Complete the following procedure to restart Apache and Tomcat services. These services must be running to access the system Web UI.

1. As **admin** user, enter the following commands to restart the Apache and Tomcat services.

```
[admin@ecnextx9 tftpboot]$ sudo systemctl restart tomcat
[admin@ecnextx9 tftpboot]$ sudo systemctl restart httpd
[admin@ecnextx9 tftpboot]$ sudo systemctl restart httpd-dncsws
```

2. Enter the following commands to verify that the Apache and Tomcat services are running. The output should indicate that the system is active (running).

```
[admin@ecnextx9 tftpboot]$ systemctl status tomcat
[admin@ecnextx9 tftpboot]$ systemctl status httpd
[admin@ecnextx9 tftpboot]$ systemctl status httpd-dncsws
```

   Note: If a service fails to start, please contact Cisco Services.

Start the EC Processes

Important: Execute this procedure for either a new install or a migration.

1. As **dncs** user, type the following command to start dncs processes.

   ```
   [dncs@ecnextx9 ~]$ dncsStart
   ```

2. If you have installed the application server, type the following command to start the application server processes.

   ```
   [dncs@ecnextx9 ~]$ appStart
   ```

3. From a supported Web browser, use the following URL syntax to access the EC Web UI.

   URL syntax:

   ```
   https://EC IP address]
   ```

   Example:

   ```
   https://10.90.46.17
   ```

4. Login to the EC Web UI using the **ecadmin** account credentials or any other administrator account you created in ***Creating User Accounts*** (on page 88).

5. Monitor the processes as they come up. Green indicators replace red indicators as the application processes start. All processes should turn green shortly.

   Note: All process logs are located in /dvs/dncs/tmp for dncs processes and /dvs/appserv/tmp for application server processes.

6. Provision the system as needed.

   Note: Refer to the ***SR 9.0 EC Online Help*** for assistance.

Verify the Number of BFS Sessions

The number of BFS sessions after the upgrade needs to be the same as the number of BFS sessions before the upgrade. The procedures in this section guide you through the steps that are required in validating the number of BFS sessions.

Verifying the Number of Recovered BFS Sessions

1. Press the **Options** button on the front panel of the BFS QAM until the **Session Count** total appears.
2. Does the **Session Count** total equal the number of sessions you recorded in *Checking the Number of BFS Sessions* (on page 23)?
   - If **yes**, skip to step 6.
   - If **no**, telnet to the GQAM modulator where BFS sessions are built.

     Example: `telnet 192.51.100.29`

     Note: The login ID and password are both `Gqam`. If you make a typing error, follow these steps to recover.

     a. Press **Ctrl +]** to return to the telnet prompt.
     b. Type `mode ch` and press **Enter** twice. The system returns you to the GQAM.
3. Type the following command and press **Enter**. The system displays the sessions that are set up on the GQAM port.

   Command syntax:

   ```
   print_session_status <port number>
   ```

   Example:

   ```
   D9479 GQAM> print_session_status 0
   ```

   Note: Port numbers on the GQAM are 0 through 15. If your sessions are built on port 1 in the QAM Web UI, it is port 0 on the GQAM.
4. Locate Session ID **00:00:00:00:00:00:2**. Is this session **Active**?
   - If **yes**, go to step 6.
   - If **no**, go to the next step.
5. If the session is not in a **CREATE_TABMAN_WAITING** or **PAT_ASSEMBLY** state, troubleshoot this matter using your established escalation procedures. If you cannot resolve the problem, contact Cisco Services for assistance.
6. Does the **Session State** field of Session ID **00:00:00:00:00:00:2** show **PAT_ASSEMBLY**?
   - If **yes**, go to *Tear Down BFS and OSM Sessions* (on page 122).
   - If **no**, troubleshoot this matter using your established escalation procedures.

     Note: Call Cisco Services if you are unable to resolve the issue.

7 Press **Ctrl +]** to return to the telnet prompt and then type `quit` to exit the telnet session. You are returned to the root prompt.

8 As **dncs** user, type the following command and press **Enter**. The BFS session count is displayed.

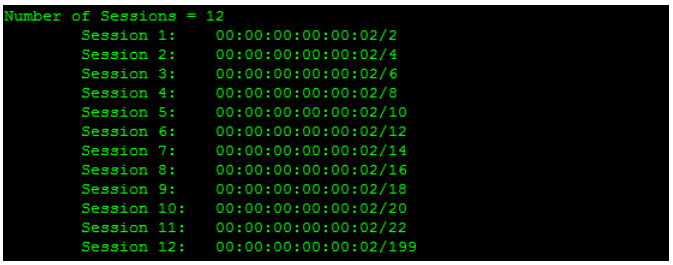
Command syntax:

```
auditQam –query [BFS QAM IP address] [port #]
```

Example:

```
[dncs@ecnextx9 ~]$ auditQam –query 209.165.202.129 1
```

Important: Make sure to use the IP address of the BFS QAM in your system when running this procedure.



Tear Down BFS and OSM Sessions

Complete this procedure ONLY if the number of recovered BFS sessions does not match the number of pre-upgrade BFS sessions. Complete these steps to tear down the BFS and OSM sessions to return the BFS session count to the expected number of sessions.

1 From the home page of the EC Web UI (displays the processes), click the button next to **bfsServer**.

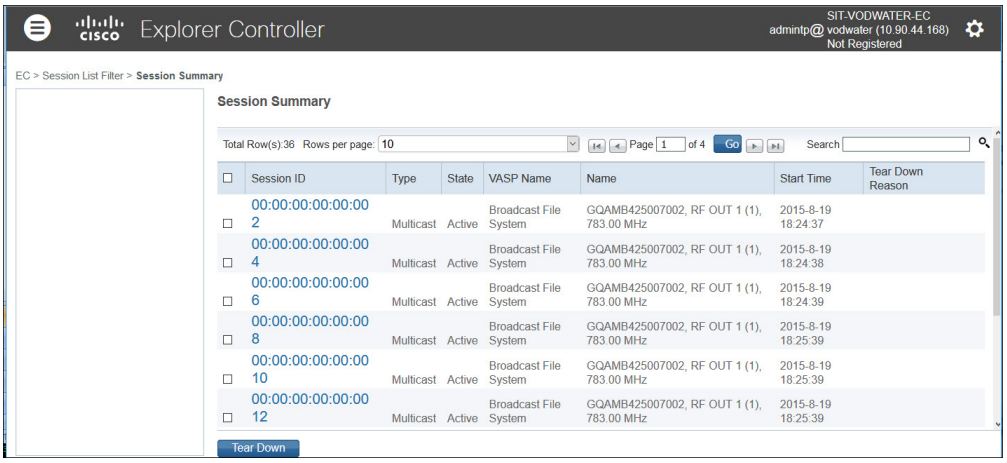
2 Click **Stop**. The bfsServer process stops and turns red.

3 Scroll down the process list and click the button next to **osm**.

4 Click **Stop**. The osm process stops and turns red.

5 Click the **Navigation** button ( ) and then select **Utilities > Session List**. The Session List Filter page opens.

6 Select the BFS QAM from the QAMs list and then click **Display**. The Session Summary page appears.



7 Does the system have more than 10 BFS sessions?

- If **yes**, change the **Rows per page** field to a value that will include all sessions.
- If **no**, continue with the next step.

8 Click the check box next to **Session ID** in the top row. This selects **ALL BFS** sessions displayed on this page.

9 Click **Tear Down** at the bottom of the page. All BFS sessions are torn down.

10 Click **EC** from the left-most portion of the window to display the home page of the EC WUI.

11 Click the **bfsServer** button and then click **Start**. The bfsServer process starts and turns green.

12 Click the **osm** button and then click **Start**. The osm process starts and turns green.

Note: Wait about 10 minutes for the BFS sessions to build.

13 Repeat Steps 5 through 6 to display the current BFS session list.

14 Are all the BFS Sessions present and active?

- If **yes**, continue with the next step.
- If **no**, contact Cisco Services for assistance.

15 Press the **Options** button on the front panel of the BFS QAM modulator until the **Session Count** total appears.

16 Does the **Session Count** total now equal the number of sessions you recorded in the ***Checking the Number of BFS Sessions*** (on page 23) procedure?

- If **yes**, continue with the next step.
- If **no**, contact Cisco Services for assistance.

17 As **dncs** user, type the following command and press **Enter**. The BFS session count is displayed.

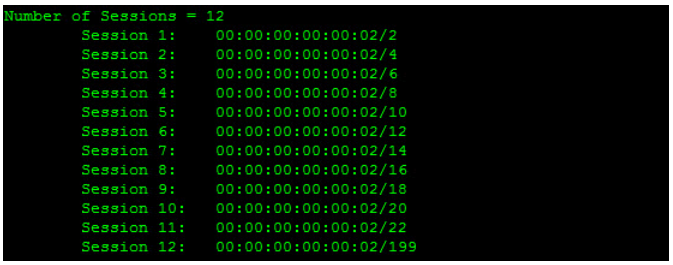
Command syntax:

```
auditQam -query [BFS QAM IP address] [port #]
```

Example:

```
[dncs@ecnextx9 ~]$ auditQam -query 209.165.202.129 1
```

Important: Be sure to use the IP address of the BFS QAM in your system when running this procedure.



18 Does the **Session Count** total equal the number of sessions you recorded in the *Checking the Number of BFS Sessions* (on page 23)?

- If **yes**, continue with the next step.
- If **no**, contact Cisco Services for assistance.

19 Telnet to the GQAM modulator where BFS sessions are built.

Example:

```
[dncs@ecnextx9 ~]$ telnet 198.51.100.29
```

Note: The login ID and password are both `Gqam`. If you make a typing error, follow these steps to recover.

a Press **Ctrl** + **]** to return to the telnet prompt.

b Type `mode ch` and press **Enter** twice.

20 Type the following command and press **Enter**. The system displays the sessions that are set up on the GQAM port.

Command syntax:

```
print_session_status <port number>
```

Example:

```
D9479 GQAM> print_session_status 0
```

Note: Port numbers on the GQAM are 0 through 15. If your sessions are built on port 1 in the QAM WUI, it is port 0 on the GQAM.

21 Locate Session ID **00:00:00:00:00:00:2**. Is this session in the **CREATE_TABMAN_WAITING** state?

- If **yes**, go to next step.
- If **no**, troubleshoot this matter using your established escalation procedures.

  Note: Call Cisco Services if you are unable to resolve the issue.

22 Does the Program State field of Session ID **00:00:00:00:00:00:2** show **PAT_ASSEMBLY**?

- If **yes**, go to the next procedure in this chapter.
- If **no**, troubleshoot this matter using your established escalation procedures.

  Note: Call Cisco Services if you are unable to resolve the issue.

Third-Party Server Post Installation Checks

Unlocking the dbreader User Account

Complete the following steps to unlock the dbreader user account.

1. As **root** user, enter the following command to view the current status for the dbreader user account.

   ```
   [root@ecnextx9 ~]# passwd -S dbreader
   ```

   Example output:

   ```
   dbreader LK 2018-07-18 7 99999 7 30 (Password locked.)
   ```

   Result: The output indicates that the dbreader account is locked.

2. Enter the following command to unlock the dbreader account. The account is unlocked.

   ```
   [root@ecnextx9 ~]# passwd -f -u dbreader
   ```

3. Repeat step 1 to view the current status of the dbreader account. The output will indicate NP which means there is no password defined for dbreader.

   Example output:

   ```
   dbreader NP 2018-07-18 7 99999 7 30 (Empty password.)
   ```

4. Enter the following command to define a password for the dbreader user.

   ```
   root@ecnextx9 ~]# passwd dbreader
   ```

5. Respond to the prompts to define the password.

6. Repeat step 1 to view the current status of the dbreader account. The output should indicates PS (Password set, SHA512 crypt.

   Example output:

   ```
   dbreader PS 2018-07-18 7 99999 7 30 (Password set, SHA512 crypt.)
   ```

Defining the Port to Access the Database

SR 9.0 requires you to update the port used to access the DB connection from 3010 to **9088**. Please make the necessary changes on your third-party server at this time.

Confirming Third Party BFS Application Cabinet Data

In this procedure, you will check to make sure that all third-party BFS application cabinet data is present following the upgrade.

Note: You need the sheet of paper that you used to record third-party BFS application cabinet data when you completed Recording Third Party BFS Application Cabinet Data.

1. From the EC Web UI, click the **Navigation** button, and then select **App Interface Modules > BFS Client**. The Site DNCS Broadcast File Server List window appears.
2. Refer to the pre-upgrade data that you recorded and determine if there are any third-party BFS application cabinets that were present before the upgrade that are now missing after the upgrade.
3. Are there any cabinets missing post upgrade?
   - If **yes**, create a cabinet for each of the missing third-party applications using the Broadcast File Server List window that is open.
     a. Click **Add Server**. The Add Server window opens.
     b. Click the **Server Name** dropdown arrow and select the appropriate server.
     c. Click the appropriate **Mode** checkbox (**1-way** or **2-way**).
     d. From the **Available Sources** area, select the appropriate source.
     e. Click **Add** to move it to the **Selected Sources** column.
     f. Click **Save**.
     g. Repeat these steps for any additional third-party BFS application cabinets that are missing.
   - If **no** (there are no missing third-party BFS application cabinets), continue with the next step.
4. Highlight each of the third-party application cabinets and click **Edit**. The Edit Server window opens for the selected cabinet.
5. Examine the **Mode** field for the selected cabinet and verify that the correct mode (**1-way** or **2-way**) is checked.
6. Verify that the correct **Selected Sources** are present for the selected cabinet.
7. Click **Cancel** to close the Edit Server window.

Reset the Modulators

The SR 9.0 installation updates your modulator code. When you reset the modulators, the modulators upgrade by downloading these versions of software from the EC. Only reset those modulators that do not already have the latest version of code.

You have the following methods available when you reset modulators:

- You can use the traditional method of resetting modulators through the EC Web UI.
- You can reset the modulators (except the QAM and QPSK modulators) through the front panel of the modulators. The QAM modulator resets through the power switch on the back panel.
- You can use the auditQam utility to reset the QAM family of modulators through the command line of the EC.

Important Notice Regarding the Reset of QAM Modulators

On occasion, for testing purposes, default configuration files for headend components are changed. For example, a site might substitute a file called gqam.config.464, instead of gqam.config, for the GQAM configuration file. If the site you have upgraded uses a custom configuration file, and if you are now ready to use the default configuration file again, you need to update the configuration file settings for your headend equipment.

The following list includes the default configuration files for the QAM-family of devices:

- QAM — /var/lib/tftpboot/qam.config
- GQAM — /var/lib/tftpboot/gqam.config
- GOQAM —/var/lib/tftpboot/goqam.config
- MQAM — /var/lib/tftpboot/mqam.config

CAUTION:

Failure to update the configuration file(s) results in the device remaining in the uniquely specified configuration. The device will not load new code. Instead, it will continue to load the code specified in the custom configuration file.

If the headend device fails to load the code you intended it to receive, check to see if either a unique file was specified in the EC Web UI or in the /var/lib/tftpboot file before contacting Cisco Services for assistance.

Which Reset Method to Use

Resetting the QAM-family of modulators from the EC Web UI or the front panel can be time consuming. If you have several modulators to reset, consider using the auditQam utility. The auditQam utility takes, as an argument, the IP address of the modulator that you want to reset. While the auditQam utility script runs, you are free to complete other upgrade-related tasks.

To reset modulators, go to one of the following sections:

- ***Resetting Modulators Through the EC WUI*** (on page 129)
- ***Resetting Modulators Through the Modulator Panel*** (on page 131)
- ***Resetting Modulators Through the auditQam Utility*** (on page 133)

Resetting Modulators Through the EC WUI

When you reset the modulators, the modulators download their new SR 9.0 code. Follow these instructions to reset the modulators through the EC WUI.

Important: Never reset more than four modulators at a time or the EC may become overloaded. The following instructions alert you to this important point at the appropriate step.

1 Follow these instructions to record the Session Count, the Program Count, and the IP address of your modulators.

Note: Skip this step for any modulator used for video-on-demand (VOD).

a Press the **Options** button on the front panel until the Session Count total appears.

b Record the Session Count on a piece of paper.

Note: Press the **RF Select** button to access each component of the MQAM and GQAM.

c Press the **Options** button on the front panel until the **Program Count** total appears.

d Record the Program Count on a piece of paper.

Note: Press the **RF Select** button to access each component of the MQAM and GQAM.

e Press the **Options** button on the front panel until the **IP address** appears.

f Record the IP address on a piece of paper.

Note: Press the RF Select button to access each component of the MQAM and GQAM.

g Repeat these steps for all of your modulators.

2. From the EC Web UI, click the **Navigation** button ( ) and then select **Network Element Provisioning > QAM**.
3. Click **QAM**.

   Result: The QAM List window opens.
4. Click **By Field** and select **All**.
5. Click **Show**. All provisioned QAM modulators on the system can now be accessed.

   Note: If the **Security Warning** dialog box opens, click **Continue**.
6. From the QAM List window, choose a modulator.

   Note: Refer to the QAM Type column to differentiate between types of modulators.
7. Click **Reset** at the bottom of the page. A confirmation message appears.
8. Click **OK** in the confirmation message.

   Result: The modulator resets.
9. Repeat steps 6 through 8 for up to three additional modulators and then go to the next step.

   Important: Never reset more than four modulators at a time as it may overload the EC.

   Note: In step 11, you will have the opportunity to reset additional modulators.
10. Wait a few minutes and as **dncs** user, enter the following command to ping modulator you just reset.

    Command syntax:

    ```
    ping [IP address of modulator]
    ```

    Example:

    ```
    [dncs@ecnextx9 ~]$ ping 192.10.2.4
    ```

    Important: Make sure to use the actual IP address for the specific modulators in your system when running this command.

    Note: It may take up to 5 minutes for each modulator to reset.
11. Do you have additional modulators to reset?
    - If **yes**, repeat steps 6 through 10 as many times as necessary until all of your modulators have been reset, and go to the next step.
    - If **no**, go to the next step.

12 Did you record the Program Count and the Session Count for each modulator not used for VOD?

- If **yes**, repeat step 1 to verify that the Program Count and Session Count totals match what you recorded before resetting the modulators, and go to the next step.

  Important: If the Program Count and Session Count totals do not match what you recorded prior to resetting the modulators, call Cisco Services for assistance.

- If **no**, go to the next step.

13 Go to *Reset QPSK Modulators* (on page 134).

Resetting Modulators Through the Modulator Panel

When you reset the modulators, the modulators download the new SR 9.0 code. Follow these instructions to reset the modulators through the modulator panel.

1 Follow these instructions to record the **Session Count**, the **Program Count**, and the **IP address** of your modulators:

  Note: Skip this step for any modulator used for video-on-demand (VOD).

  a Press the **Options** button on the front panel until the **Session Count** total appears.

  b Record the **Session Count** on a piece of paper.

  c Press the **Options** button on the front panel until the **Program Count** total appears.

  d Record the **Program Count** on a piece of paper.

  e Press the **Options** button on the front panel until the **IP address** appears.

  f Record the **IP address** on a piece of paper.

  Note: Press the **RF Select** button to access each component of the MQAM and GQAM.

  g Repeat these steps 1a through 1f for all QAM, MQAM, and/or GQAM modulators.

2 Choose one of the following options:

- To reset an MQAM or GQAM modulator, go to the next step.
- To reset a QAM modulator, go to step 4.

3 To reset an MQAM or GQAM modulator, follow these instructions:

  a Press the **Options** button on the front panel until the **Reset** option appears.

  b Follow the instructions that appear alongside the Reset option.

  c Go to step 5.

4 To reset a QAM modulator, turn off the power switch on the back of the QAM modulator, wait a few seconds, and turn it back on.

5 Repeat steps 3 and 4 for up to three additional modulators, and then go to the next step.

Important: Never reset more than four modulators at once, or you may overload the EC.

Note: In step 7, you have the opportunity to reset additional modulators.

6 Wait a few minutes and as **dncs** user, enter the following command to ping each modulator that you reset.

Command syntax:

```
ping [IP address of modulator]
```

Example:

```
[dncs@ecnextx9 ~]$ ping 192.10.2.4
```

Note: It may take up to 5 minutes for each modulator to reset.

7 Do you have additional modulators to reset?

- If **yes**, repeat steps 3 through 6 as many times as necessary until all of your modulators have been reset, and then go to the next step.
- If **no**, go to the next step.

8 Did you record the **Program Count** and the **Session Count** for each modulator not used for VOD?

- If **yes**, repeat step 1 to verify that the **Program Count** and **Session Count** totals match what you recorded before resetting the modulators, and then go to next step.

  Important: If the **Program Count** and **Session Count** totals do not match what you recorded prior to resetting the modulators, call Cisco Services, for assistance.

- If **no**, go to the next step.

9 Go to ***Reset QPSK Modulators*** (on page 134).

Resetting Modulators Through the auditQam Utility

The *reset* option of the auditQam utility allows upgrade engineers to reset a modulator from the command line of the EC, a process that is usually quicker than resetting the modulator through the EC Web UI or modulator panel. If you have only a few modulators to reset, you can just type the IP address of the modulator as an argument to the `auditQam -reset` command. If you have many modulators to reset, consider creating a script. Instructions and guidelines for both situations follow.

Resetting a Few Modulators

If you want to reset only a few modulators, complete this procedure for each modulator:

1 As **dncs** user, type the following command and press **Enter.**

Command syntax:

```
auditQam -reset [qam ip address or mqam ip address]
```

Example:

```
[dncs@ecnextx9 ~]$ auditQam -reset 209.165.202.129
```

Result: The system shuts down and reinitializes the modulator.

Note: The system also performs an audit to ensure that the session list for the modulator matches the session list from the EC.

2 Repeat step 2 for each QAM modulator on your system.

Resetting Many QAM and MQAM Modulators

You frequently do not have time to manually reset hundreds of modulators from the EC Web UI. To save time, you can create a script that runs automatically. Refer to the following example for a sample script:

```
auditQam  -reset  192.0.2.1
sleep 1
auditQam  -reset  192.0.2.2
sleep 1
auditQam  -reset  192.0.2.3
sleep 1
auditQam  -reset  192.0.2.4
```

Important: Resetting a QAM interrupts all active sessions on the QAM for up to 10 minutes. Complete this task during a maintenance period whenever possible. Do not reset more than four modulators at a time.

Reset QPSK Modulators

Important Notice Regarding the Reset of QPSK Modulators

On occasion, for testing purposes, default configuration files for headend components are changed. For example, a site might substitute a file called qpskC70.config, instead of qpsk.config, for the QPSK configuration file. If the site you have upgraded uses a custom configuration file, and if you are now ready to use the default configuration file again, you need to update the configuration file settings for your headend equipment.

The default configuration file for the QPSK modulator is **/var/lib/tftpboot/qpsk.config**.

CAUTION:

Failure to update the configuration file(s) results in the device remaining in the uniquely specified configuration. The device will not load new code. Instead, it will continue to load the code specified in the custom configuration file.

If the headend device fails to load the code you intended it to receive, check to see if either a unique file was specified in the Web UI or in the /etc/bootptab file before contacting Cisco Services for assistance.

Resetting QPSK Modulators

Complete the following steps to reset your QPSK modulators.

Notes:

- You do not have to reset the QPSK modulators if the system you are upgrading is already operating with the new version of QPSK modulator code.
- You can also reset QPSK modulators through the back panel by turning the modulator off, waiting a few seconds, and turning it back on.

1. From the EC Web UI, click the **Navigation** button ( ) and then select **Network Element Provisioning > QPSK**.
2. Use the **Filter > By Field** dropdown menu to select an option to display the appropriate QPSKs on the system. Then click **Show**.
3. Click the button next to the appropriate QPSK modulator.
4. Click **Reset** at the bottom of the Web UI window. A confirmation message appears.
5. Click **OK** to confirm the reset. The QPSK modulator resets.
6. Wait about 15 minutes and repeat steps 3 through 5 until all of your QPSK modulators have been reset.

CentOS cron and anacrontab Overview

By default, CentOS includes the following three installed cron packages:

- cronie-1.4.11-17.el7.x86_64
- crontabs-1.11-6.20121102git.el7.noarch
- cronie-anacron-1.4.11-17.el7.x86_64

Both cron and anacron are daemons that can schedule execution of recurring tasks to a certain point in time defined by the user.

The main difference between cron and anacron is that cron assumes that the system is running continuously. If your system is off and you have a job scheduled during this time, the job will not be executed.

On the other hand, anacron is designed for systems that are not running 24x7. For it to work, anacron uses time-stamped files to find out when the last time its commands were executed. Also, anacron can only run a job once a day, but cron can run as often as every minute.

For example, assume there is a power failure or scheduled maintenance on your system from 3:00AM to 5:00AM. cron.daily is set by default to run at 3:45AM. In this case, cron could not perform tasks such as logrotate. However, with anacron, this daemon takes over the task and runs the cron job after the machine is up again (i.e. at 5:00AM).

For additional info about anacron, please refer to the man pages by entering the following command as admin user: `man anacron`

cron and anacron Features

cron Features:

- Minimum granularity is in minutes (i.e. jobs can be scheduled to be run every minute).
- Can be scheduled by any normal user (not restricted for the super user).
- Expects systems to be running 24x7.

  Note: If a job is scheduled and the system is down during that time, the job is not executed.
- Desirable when a job needs executed at an exact hour and minute

anacron Features

- Minimum granularity is only daily.
- Can be used only by the super user.

  Note: Workarounds exist to enable use by normal users.
- Does not expect system to be running 24x7.

  Note: If a job is scheduled and the system is down during that time, the job will be executed when the system comes back up.
- Desirable when a job does not need executed at a precise hour and minute of the day.

Default cron Jobs

The following list identifies the default cron jobs in this release.

- /etc/cron.d/sysstat
- /etc/cron.d/0hourly
- /etc/cron.d/passwd_check
- /etc/cron.d/updatedsteffyear
- /etc/cron.d/manage_SDVLog
- /etc/cron.d/manage_pims_files
- /etc/cron.d/free_informix_memory
- /etc/cron.d/dbOptimizer
- /etc/cron.d/clearDbSessions
- /etc/cron.daily/man-db.cron
- /etc/cron.daily/logrotate
- /etc/cron.daily/CSCOapsrv_savelogs
- /etc/cron.daily/CSCOapsrv_cores
- /etc/cron.daily/appserv_updateStatistics.cron
- /etc/cron.daily/updateStatistics.cron
- /etc/cron.daily/manage_dncsLog.cron
- /etc/cron.daily/certCheck.cron
- /etc/cron.hourly/0anacron
- /etc/cron.hourly/1dncsLog

Verifying the crontab Entries Managed by cron

Verifying the cron tab Entries

After upgrading, inspect the crontab files in the **/disk1/keyfiles_staging/var/spool/cron/crontabs** directory on the EC to verify whether or not all customized cron jobs are present on the new EC.

Examining the CED.in Entry

Our engineers developed the dbOptimizer program to delete EMMs that are no longer needed by DHCTs. dbOptimizer runs as a cron job. The cron job can be found in /etc/cron.d/dbOptimizers.

Most EMMs are assigned to DHCTs during the staging process when DHCTs are prepared for deployment in the homes of subscribers. These EMMs are also stored in the database of the EC. When a DHCT has been successfully staged, those EMMs associated with the staging process are no longer needed and should be removed from the EC database. The dbOptimizer program is configured to run by default each Saturday at 4 AM as shown in the following output:

```
[admin@ecnextx9 ~]$ sudo less /etc/cron.d/dbOptimizer

#!/bin/bash

#

# This cron job runs dbOptimizer

#

MAILTO=dncs

0 4 * * 6 dncs [ -r /dvs/dncs/bin/dncsSetup ] && [ -x
/dvs/dncs/bin/dbOptimizer ] && { . /dvs/dncs/bin/dncsSetup;
/dvs/dncs/bin/dbOptimizer -d `cat /dvs/dncs/bin/CED.in`; }
>>/dvs/dncs/tmp/dbOptimizer.cron.log 2>&1
```

The /dvs/dncs/bin/CED.in file in the EC contains a value that represents a number of *days*. The dbOptimizer program is designed to delete unneeded EMMs that are older than the number of days specified in the CED.in file.

In this procedure, you will examine and change, if necessary, the number of days specified in the CED.in file.

Note: Our engineers recommend the default value of 90 days.

1 As **dncs** user on the EC, type the following command and press **Enter**. The system displays the number of days that EMMs are retained. EMMs older than this number of days are deleted by the dbOptimizer program when it runs each Saturday.

```
[dncs@ecnextx9 ~]$ cat /dvs/dncs/bin/CED.in
```

2 Are you satisfied by the number of days specified by the CED.in file?

- If **yes**, go to the next section.
- If **no**, go to the next step to edit the CED.in file.

3 Type the following command and press **Enter**. The system changes the value stored in the CED.in file.

Command syntax:

```
echo [new # of days] > /dvs/dncs/bin/CED.in
```

Example:

```
[dncs@ecnextx9 ~]$ echo 90 > /dvs/dncs/bin/CED.in
```

Adding the IPG Collector Crontab Entry

Important: Only complete this procedure if this system is a migration from SR 8.0/7.x to SR 9.0. If this is a Greenfield installation, skip this procedure and go to the next section.

1. Does your system use an IPG collector in which the collector has been successfully configured?
   - If **yes**, go to step 2.
   - If **no**, skip this procedure and go to the next section.
2. From the EC Web UI, click the **Navigation** icon () and then select **Server Applications > IPG**. The IPG Server List page opens.
3. Double click the IPG server, for example, IPG_eng (English), to display the IPG collectors to which it is associated.
4. Select an IPG collector and click **Edit**. The Edit IPG Collector window displays.
5. Click **Save**. An "IPGCollector updated successfully" message appears and you are returned to the IPG Server List window.
6. As **dncs** user in a terminal window, enter the following command to verify that the crontab entry is now present for the IPG Collector.

   ```
   [dncs@ecnextx9 ~]$ crontab -l
   ```

   Example output:

   ```
   30 06 * * * ( . /dvs/appserv/bin/appservSetup && .
   /dvs/appserv/bin/appServer.env > /dev/null 2>&1;
   /dvs/appserv/bin/ipgCollector 1 >/dvs/appserv/tmp/ipgCollector.1.cron.log
   2>&1 ) > /dev/null 2>&1
   ```

Adding Site-Specific crontab Entries

Examine old cron job entries in the /disk1/keyfiles_staging/var/spool/cron/crontabs directory. Determine if any of these entries should be retained. If necessary, complete the following procedure to add site-specific crontab entries to a desired /etc cron-specific directory (for example, /etc/cron.daily).

Important: Do not add RepDB cron jobs as these are added when enabling RepDB.

1. As **root** user, enter the following command.

   ```
   [root@ecnextx9 ~]# cd
   /disk1/keyfiles_staging/var/spool/cron/crontabs
   ```

2. Using the **cat** command, display the output of any of the cron-specific files (for example, dncs) and determine if there are site-specific cron jobs that needed added to the SR 9.0 cron directories.

3. In another terminal window as **root** user, type the following command and press **Enter**.

   ```
   [root@ecnextx9 ~# cd /etc
   ```

4. Create a cron job for any unique cron jobs from the file reviews in step 2 and save it to an appropriate **/etc** cron directory (for example, add a unique cron job to /etc/cron.daily).

   Note: Unique cron jobs can be saved in either the **/etc/cron.daily**, **/etc/cron.weekly** or **/etc/cron.monthly status** directories and should be in a script or a binary format.

5. Repeat steps 2 through 4 for any other pre-upgrade cron directories.

6. Enter the following command to verify that cron is running.

   ```
   [root@ecnextx9 etc]# systemctl status crond
   ```

   Note: If cron is not running, enter the following command to start **crond**.

   ```
   [root@ecnextx9 etc]# systemctl start crond
   ```

Verify the Upgrade

Go to Appendix B, ***System Verification Procedures*** (on page 197) to verify the upgrade.

Set the Clock on the TED (Optional)

Note: Skip this section if your system is using an nTED.

Complete this procedure for the legacy TED in your system.

1. In a **root** remote terminal window, type `date` and press **Enter**. The system date and time appear.
2. Write down the system date and time in the space provided.

   System Date: _____

   System Time: _____
3. What type of TED is installed at the site you are upgrading?
   - If it is a TED-FX, type the following command and press **Enter**:

     `telnet dncsted`
   - If it is a TED-3 or TED-4, type the following command and press **Enter**:

     `ssh dncsted`
4. Login as **root** user and press **Enter**. Then enter the password when prompted. You are logged onto the TED as root user.
5. Type `date` and press **Enter**. The TED date and time appear.
6. Compare the time results from step 1 with step 5. Do the date, time, and timezone on the EC and TED match?
   - If **yes**, go to step 9.
   - If **no**, go to the next step.
7. At the prompt, type `date [mmddhhmm]` and press **Enter**.

   Example: `date 07172017`

   Notes:
   - The format for the date command is:
     - `mm` - month
     - `dd` - day
     - `hh` - hours in 24 hour format
     - `mm` - minutes
   - The command can be modified to include the year, the seconds, or both the year and seconds.

   Examples:
   - The **date 073123162017** includes the year.
   - The **date 07132316.30** includes the seconds.
   - The **date 071323162017.30** includes the year and seconds.

8. Type `date` again and press **Enter**. Verify that the correct time now appears.
9. Type `/sbin/clock -r` and press **Enter**. The time on the hardware clock appears.
10. Type `/sbin/clock -w` and press **Enter**. This command writes the system time to the TED hardware clock.
11. Type `/sbin/clock -r` and press **Enter**. Verify the time is synchronized between the system and the TED hardware clock.
12. Type `exit` and press **Enter** to log out of the TED.

Enabling RADIUS and LDAP (Optional)

To enable RADIUS or LDAP on your system, refer to ***Configuring RADIUS and LDAP Support Configuration Guide for Explorer Controller 9.0 and DTACS 5.2***.

8

Configure and Operate the Replicated Database

The Replicated Database package, sometimes referred to as RepDB, is comprised of the following two components:

- The IBM Informix Dynamic Server Data Replication for the database.
- The rsync utility — a fast and versatile remote file-copying tool for user-defined files.

Data replication allows a copy of the database from a primary server to be maintained on a secondary server. When activated, the primary database server continuously replicates data between itself and the secondary server by sending copies of the logical-log transactions to the secondary database server.

The rsync utility allows a copy of selected files and directories from a primary server to be maintained on a secondary server. When activated, the rsync utility periodically synchronizes the primary server to the secondary server.

In This Chapter

Prerequisites for RepDB

Important: Your system environment must have a second UCS platform with VMware installed and an EC 9.0 virtual machine configuration.

- vCenter server license.
- VMware ESXi (6.0u1 or later) and vCenter infrastructure (software, license and a running vCenter machine).

  Note: VMware vSphere 6.0 Web UI is used for all RepDB procedures.
- vCenter login must have admin privileges to deploy and clone VMs.
- Network connectivity between the operational EC and the new virtual machine.
- Use the existing network ports (vSwitches) that were defined when installing or migrating the SR 9.0 EC.
  - EC 9.0 Mapping
    - NET0 – vSwitch0 – Corp/Engineering Network
    - NET1 – vSwitch1 – Headend (HE) Network
    - NET2 – vSwitch2 – TED/nTED Network
    - NET3 – vSwitch3 - RepDB

Overview of the Replicated Database Package

This section describes the Replicated Database package and lists some of the advantages and limitations associated with the package. This section also introduces the hardware platforms that are compatible with the Replicated Database, as well as the system release software requirements.

RepDB Package and Components

The RepDB package consists of the following two components:

- The IBM Informix Dynamic Server Data Replication for the database.
- The rsync utility — a fast and versatile remote file-copying tool for user-defined files.

The data replication component allows a copy of the Informix database to be maintained on another server. When the data replication component is active on a system, data is copied between a primary database server and a secondary database server. The primary database server continuously replicates data between itself and the secondary server by sending copies of the logical-log transactions to the secondary database server.

The remote file copying component allows a copy of user-defined files to be maintained on another server. When RepDB is enabled, remote file copying becomes active as a cron entry is added to the root crontab file. According to the cron entry, files and directories are periodically synchronized from the primary server to the secondary server.

Advantages of RepDB

The following are some of the advantages of enabling the Replicated Database on a system:

- Service-impacting events are reduced on the primary server by allowing third-party database query tools to access the secondary database server.
- The secondary server provides a flexible platform for developing new tools. Furthermore, if the secondary server has access to the Digital Broadband Delivery System (DBDS), it can be used by third-party tools that require both database and network access.
- The secondary server, at the operator's command, can be converted to the primary server, if needed.

Limitations of the Replicated Database

RepDB includes the following inherent limitations:

- The Replicated Database is read-only. The Replicated Database cannot be used for database backups because a database backup is considered a write process.
- There is a minor time delay between changes made to the primary database and those changes being reflected on the secondary server.
- Automatic failover — the ability to re-route users and applications to the Replicated Database with minimal interruption — is not supported. Failover requires manual intervention.
- Regular backups of the primary database server are still required. Database corruption in the primary server, if it occurs, will be copied to the secondary server while the Replicated Database is active.

Replicated Database and Failover

The Replicated Database package contains tools that maintain a synchronized file system between the primary and secondary server. It also contains tools that assist in the conversion of the secondary server to a live server, if necessary. Therefore, using this configuration, the secondary server has the capability to become the active server.

Note: For failover procedures, refer to the ***Replicated Database Operator's Guide***.

To achieve this configuration, the secondary server must meet the following conditions:

- Run the same system release software and Linux OS version as the primary server.
- Exactly match the hardware configuration of the primary server.

In addition, both the primary and secondary servers must include the following conditions:

- Both servers must be a UCS C240 M3 or UCS C240 M4 server.
- Both servers require network connectivity to one another, as well as to the network.
- In environments that do ***NOT*** include an nTED, the operator must physically connect the legacy TED to the secondary server as part of the failover process.

Cloning the Secondary VM from the Primary VM

This section provides instructions to clone a secondary VM from the primary VM. Review the following two methods to determine how you will clone the *primary* VM.

Note: Cisco recommends cloning the VM during a maintenance window (primary VM shutdown).

- **Cloning when the Primary VM is shutdown**
  - Cloning occurs during a maintenance window
  - Billing Transactions and all EC updates are suspended during the cloning process
  - Go to ***Cloning When the Primary VM is Shutdown*** (on page 151)
- **Cloning while the Primary VM is powered on and running**
  - Cloning may cause EC performance issues depending on the size of the system
  - The primary EC will be processing transactions without the interruption of interactive services
  - Go to ***Cloning When the Primary VM is Running*** (on page 153)

Cloning When the Primary VM is Shutdown

Complete the following steps to clone HOSTA while the *primary* VM is shutdown.

Note: In this example, HOSTA is the *primary* EC.

1. As **admin** user on the *primary* EC, edit the **/etc/hosts** file to include the primary and secondary RepDB entries.

   Note: You may substitute other names for HOSTA and HOSTB if you desire. However, these are the names that will be used throughout this guide.

   ```
   [admin@ecnextx9 ~]$ sudo vi /etc/hosts
   ```

2. Save and close the file.
3. Enter the following command to verify the RepDB entries.

   ```
   [admin@ecnextx9 ~]$ grep -i host /etc/hosts
   ```

   Example output:

   ```
   204.3.3.97      HOSTA
   204.3.3.98      HOSTB
   ```

4 As **dncs** user, enter the following commands to stop system processes.

```
[dncs@ecnextx9 ~]$ appStop
[dncs@ecnextx9 ~]$ appKill
[dncs@ecnextx9 ~]$ dncsStop
[dncs@ecnextx9 ~]$ dncsKill
```

5 Stop all billing transactions and updates to the *primary* EC.

6 As **admin** user, type one of the following commands to shutdown the *primary* EC.

```
[admin@ecnextx9 ~]$ sudo shutdown -h now
```

7 From the VMware vSphere Web UI, right-click the *primary* server and select **Clone > Clone to Virtual Machine**. The Clone Existing Virtual Machine window opens.

8 From the **Enter a name for the virtual machine** text box, enter a name for the *secondary* host.

9 Select the appropriate datacenter or VM folder and then click **Next**. The Select a compute resource view opens.

10 Select the compute resource (e.g., cluster, ESXi host) where the VM is to be cloned. A compatibility check occurs.

11 Once the compatibility check succeeds, click **Next**. The Select storage window opens.

12 Ensure that the "Select virtual disk format" field is set to **Same format as source**.

13 Select the correct datastore for the VM configuration files and virtual disks.

14 Click **Next**. The Select clone option window opens.

15 Select cloning options if needed and then click **Next**. The Customize vApp properties view opens.

Important: Do not make any edits to this window as the ifcfg-ens192 configuration file overwrites these values.

16 Click **Next**. Review the settings and then click **Finish**.

17 Monitor the **Recent Tasks** area to verify that the cloned VM completed successfully.

18 When the clone completes. right-click the new VM (secondary VM) and select **Edit Settings**.

19 Unselect the **Connect** and **Connect at power on** check boxes for all of the network adapters *except* RepDB.

20 Click **OK**.

21 Select and right-click the *primary* VM and select **Power > Power On**.

22 From a terminal window, login as **ecadmin** user.

23 As **dncs** user, enter the following commands to start the system processes.

```
[dncs@ecnextx9 ~]$ dncsStart
[dncs@ecnextx9 ~]$ appStart
```

24 Go to *Configure RepDB* (on page 155).

Cloning When the Primary VM is Running

Complete the following steps to clone HOSTA while the *primary* EC is running.

Note: In this example, HOSTA is the *primary* EC.

1 As **admin** user on the *primary* EC, edit the **/etc/hosts** file to include the primary and secondary RepDB entries.

Note: You may substitute other names for HOSTA and HOSTB if you desire. However, these are the names that will be used throughout this guide.

```
[admin@ecnextx9 ~]$ sudo vi /etc/hosts
```

2 Save and close the file.

3 Enter the following command to verify the RepDB entries.

```
[admin@ecnextx9 ~]$ grep -i host /etc/hosts
```

Example output:

```
204.3.3.97      HOSTA
204.3.3.98      HOSTB
```

4 From the VMware vSphere Web UI, right-click the *primary* server and select **Clone > Clone to Virtual Machine**. The Clone Existing Virtual Machine window opens.

5 From the **Enter a name for the virtual machine** text box, enter a name for the *secondary* host.

6 Select the appropriate datacenter or VM folder and then click **Next**. The Select a compute resource view opens.

7 Select the compute resource (e.g., cluster, ESXi host) where the VM is to be cloned. A compatibility check occurs.

8 Once the compatibility check succeeds, click **Next**. The Select storage window opens.

9 Ensure that the "Select virtual disk format" field is set to **Same format as source**.

10 Select the correct datastore for the VM configuration files and virtual disks.

11 Click **Next**. The Select clone option window opens.

12 Select cloning options if needed and then click **Next**. The Customize vApp properties view opens.

Important: Do not make any edits to this window as the ifcfg-ens192 configuration file overwrites these values.

13 Click **Next**. Review the settings and then click **Finish**.

14 Monitor the **Recent Tasks** area to verify that the cloned VM completed successfully.

15 When the clone completes, right-click the new VM (secondary VM) and select **Edit Settings**.

16 Unselect the **Connect** and **Connect at power on** check boxes for all of the network adapters *except* RepDB.

17 Click **OK**.

Configure RepDB

Complete the following procedures to configure the RepDB network on the primary and the secondary servers.

Configuring the Secondary Host After Cloning

1. Right-click the *secondary* VM and select **Power > Power On**.
2. Right-click the *secondary* VM again and click **Open Console**.
3. In the console window, login as **admin** user.
4. Enter the following command to verify that the interfaces are mapped correctly.

   ```
   [admin@ecnextx9 ~]$ ls -latr
   /etc/sysconfig/network-scripts/ifcfg*
   ```

5. Open the configuration file for the RepDB interface.

   Command syntax:

   ```
   sudo vi
   /etc/sysconfig/network-scripts/[RepDB_configuration_file]
   ```

   Example:

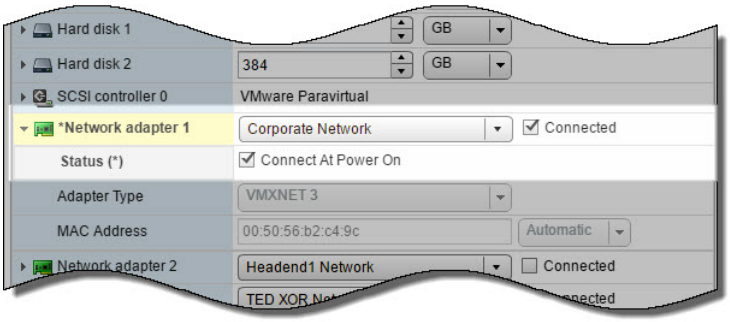
   ```
   [admin@ecnextx9 ~]$ sudo vi
   /etc/sysconfig/network-scripts/ifcfg-ens161
   ```

6. Update the **IPADDR** entry to the IP address for the *secondary* EC.
7. Save and close the file.
8. Do you want the *secondary* VM accessible remotely and/or the Admin Node to only be reachable on the corporate network (ens192)?
   - If **yes**, go to the next step.
   - If **no**, go to step 18.
9. Enter the following command to open the **ifcfg-ens192** file in a text editor.

   ```
   [admin@ecnextx9 ~]$ sudo vi
   /etc/sysconfig/network-scripts/ifcfg-eth192
   ```

10. Edit the **IPADDR** entry to the unique IP address for the *secondary* VM.
11. Save and close the file.
12. Open the **/etc/hosts** file in a text editor and update the **dncseth** entry to the IP address you configured in step 10.
13. Save and close the file.
14. From the vSphere Web UI, right-click the *secondary* VM and select **Edit Settings**.

15 From the **Network adapter 1** (corporate network) row, click the **Connected** and **Connect At Power On** boxes and then click **OK**.



16 Enter the following command to restart the network services on the *secondary* server.

```
[admin@ecnextx9 ~]$ sudo systemctl restart network
```

17 Enter the following command to verify that the interfaces are mapped properly.

```
[admin@ecnextx9 ~]$ ifconfig -a
```

18 Enter the following command to ping the *primary* server.

```
[admin@ecnextx9 ~]$ ping HOSTA
```

19 From the **primary** server, enter the following command to ping the *secondary* server.

```
[admin@ecnextx9 ~]$ ping HOSTB
```

20 Were you able to ping both hosts?

- If **yes**, go to the next section.
- If **no**, troubleshoot your network configuration or contact Cisco Services for assistance.

Setting Up SSH Login Between the EC Servers Without a Password

Complete this procedure to setup password-less SSH access between the primary and the secondary EC. This will enable RepDB features to function properly.

1 As **admin** user on the *primary* EC, enter the following command to generate SSH keys for the admin user.

Note: The keys will be saved as id-rsa-pub (public) and id-rsa (private) files in the /home/admin/.ssh directory.

```
[admin@ecnextx9 ~]$ ssh-keygen
```

2 When prompted for the location to save the key, press **Enter** to accept the default.

3 If an **Overwrite (y/n)?** message appears, enter **y** and press **Enter**.

4 When prompted for the passphrase, press **Enter** to leave this field empty.

5 When prompted to re-enter the passphrase, press **Enter**. The public and private keys are generated and saved in the **/home/admin/.ssh** directory.

6 Enter the following command to copy the keys to the *secondary* EC.

Note: The authorized_key files is saved in the **/home/admin/.ssh** directory on the remote server.

Command syntax:

```
ssh-copy-id [secondary_hostname]
```

Example:

```
[admin@ecnextx9 ~]$ ssh-copy-id HOSTB
```

7 When prompted to connect to the *secondary* VM, type **yes**.

8 When prompted for the password for the *secondary* VM, enter the password for that host.

9 Enter the following command on the *primary* host to test the password-less SSH connection to the secondary host.

```
[admin@ecnextx9 ~]$ ssh HOSTB
```

Result: You are logged into the *secondary* host without having to enter a password.

10 Enter the following command to verify that the RepDB IP address is that of the HOSTB (secondary) EC.

Command syntax:

```
ifconfig [RepDB_network_label]
```

Example: RepDB interface is ens161

```
[admin@ecnextx9 ~]$ ifconfig ens161
```

11 Type `exit` to return to the original terminal session.

12 Repeat steps 1 through 11 on the *secondary* EC.

Important: Make sure to use the *primary* host in step 6 and step 9.

Enabling RepDB

Complete the following steps to enable RepDB.

1. As **admin** user on the *primary* EC, enter the following command to enable RepDB.

   ```
   [admin@ecnextx9 ~]$ sudo /opt/cisco/repdb/configRepDb
   ```

   Note: This can take up to 30 minutes or more, depending on the size of the database.

2. When prompted for the hostname of the *primary* node, enter the hostname (for example, HOSTA) of the *primary* system's RepDB interface.

3. When prompted for the hostname of the *secondary* node, enter the hostname (for example, HOSTB) of the *secondary* system's RepDB interface.

   Result: The system returns the hostnames and IP addresses for each system, as defined by the entries in the /etc/hosts file.

   Example output:

   ```
   Please enter the hostname for the repdb interface on the active node
   Primary hostname: HOSTA

   Please enter the hostname for the repdb interface on the standby node
   Secondeary hostname: HOSTB

   Primary: HOSTA
   Primary IP:204.3.3.97
   Secondary: HOSTB
   Secondary IP:204.3.3.98

   Continue with these host settings? (y/n):
   ```

4. Verify that the entries are correct and when prompted to continue, type **y** and press **Enter**.

   Results: The RepDB environment is set up on the primary and the secondary hosts.

5. When prompted to run formatDbSpace on the *secondary* EC, type **y** and press **Enter**. The database setup begins and, if active database sessions are found, you are prompted to kill them.

6. Were you prompted to kill active database sessions?

   - If **yes**, type **y** and press **Enter**. Then go to the next step.
   - If **no**, go to the next step.

7. Observe the output and verify that Database Replication is successfully enabled on both systems and a **Replication has been SUCCESSFULLY ENABLED** message displays.

8. As **root** user, enter the following command to source the environment variables.

   ```
   [root@ecnextx9 ~]# . /dvs/dncs/bin/dncsSetup
   ```

9 Type the following command and press **Enter** on the *primary* server. The output should indicate that the database is **On-Line (Prim)** and that data replication is paired to the secondary server.

```
[root@ecnextx9 ~]# onstat -g dri
```

Example output:

```
IBM Informix Dynamic Server Version 12.10.FC8W1 -- On-Line (Prim) -- Up 1 days 02:51:18 -- 1997773
6 Kbytes

Data Replication at 0x857e1028:
  Type            State        Paired server        Last DR CKPT (id/pg)    Supports Proxy Writes
  primary         on           HOSTBDbServer                10 / 11         NA

  DRINTERVAL    5
  DRTIMEOUT     15
  DRAUTO        0
  DRLOSTFOUND   /opt/cisco/informix/server/cisco/etc/dr.lostfound
  DRIDXAUTO     0
  ENCRYPT_HDR   1
  Backlog       4
  Last Send     2018/04/19 16:46:42
  Last Receive  2018/04/19 16:46:42
  Last Ping     2018/04/19 16:46:39
  Last log page applied(log id,page): 10,530
```

10 Repeat steps 8 and 9 on the *secondary* EC. The output should indicate that the database is **Read-Only (Sec)** and is paired to the primary server.

Example output:

```
IBM Informix Dynamic Server Version 12.10.FC8W1 -- Read-Only (Sec) -- Up 00:11:03 -- 19977736 Kbyt
es

Data Replication at 0x857df028:
  Type            State        Paired server        Last DR CKPT (id/pg)    Supports Proxy Writes
  HDR Secondary   on           HOSTADbServer                10 / 11         N

  DRINTERVAL    5
  DRTIMEOUT     15
  DRAUTO        0
  DRLOSTFOUND   /opt/cisco/informix/server/cisco/etc/dr.lostfound
  DRIDXAUTO     0
  ENCRYPT_HDR   1
  Backlog       0
  Last Send     2018/04/19 16:46:48
  Last Receive  2018/04/19 16:46:48
  Last Ping     2018/04/19 16:46:41
  Last log page applied(log id,page): 10,530
```

11 Go to the next section to verify that RepDB is functioning properly.

Post RepDB Verifications

Verifying That RepDB is Running

Complete the following steps to verify that data replication from the primary server to the secondary server is functioning properly.

1 As **root** user, type the following command on the *primary* server.

```
[root@ecnextx9 ~]# /opt/cisco/repdb/checkRepDb
```

Result: The system returns the status of the secondary server, the names of the primary and secondary servers, and the number of logs the secondary server is behind.

Example output:

```
PING HOSTB (204.3.3.98) 56(84) bytes of data.
64 bytes from HOSTB (204.3.3.98): icmp_seq=1 ttl=64 time=0.302ms
64 bytes from HOSTB (204.3.3.98): icmp_seq=2 ttl=64 time=0.224ms

--- HOSTB ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.224/0.263/0.302/0.039 ms
RepDb: Primary=HOSTADbServer (HOSTA), Secondary=HOSTBDbServer (HOSTB)
RepDb: Secondary is behind 0 log(s) at THU Apr 19 16:52:36 EDT 2018
RepDb: PrimaryLog=10 (2.12% used), SecondaryLog=10 (2.11% used)
```

2 Repeat step 1 on the *secondary* server.

Verifying Remote File Copying

When the Replicated Database is enabled on the *primary* system, remote file copying is activated and key files are synced from the primary server to the secondary server.

Complete the following steps to verify that a cron job to sync key files between the remote servers is present and that the key file synchronization is functioning properly.

1 As **root** user, enter the following command to verify that the cron job is present on the *primary* host.

Note: This command synchronizes the key files twice an hour.

```
[root@ecnextx9 repdb]# crontab -l
```

Example: RepDB cron in output:

```
15,45 * * * * /opt/cisco/repdb/syncKeyFiles -l HOSTA -r HOSTB -n >
/var/log/syncKeyFiles.out 2>&1
```

2 Wait until 15 or 45 minutes past the hour (after the RepDB cron job runs) and then type the following command to verify the last modification time of the output from the syncKeyFiles crontab entry.

Notes:

- The date and time should be several minutes after the passage of the syncKeyFiles cron event.
- The syncKeyFiles.out file becomes present after the cron job runs or after you update a directory or file that is present in the KeyFiles2Sync.list.

```
[root@ecnextx9 repdb]# ls -l /var/log/syncKeyFiles.out
```

3 Review the **syncKeyFiles** log file to further check the status of the key file sync.

```
[root@ecnextx9 repdb]# less /var/log/KeyFiles2Sync.log
```

4 You can also review the **/var/log/repDbFilesyncResults** file for further information.

Note: The last three lines of this file are updated after each successful key files sync.

Editing the Key Files Sync File Lists

Complete these steps on the *primary* server to edit the list of files in the KeyFiles2Sync and the KeyFiles2Exclude files.

1 Type the following command on the *primary* server to edit the **KeyFiles2Sync.list** file in a text editor.

```
[root@ecnextx9 repdb]# vi /opt/cisco/repdb/KeyFiles2Sync.list
```

2 Add or delete any unique files, as needed.

Important:

- Do not add system-specific files, such as /etc/* or /dev/*, to this list. These files have the potential to disrupt the Replicated Database environment.
- Be certain to use absolute path names.
- When synchronizing links, do not add both the link and its target to the list. Instead, add only the link. Links are followed such that both the link and the file to which it points are synchronized.

3 Save and close the file.

9

Customer Information

If You Have Questions

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Access your company's extranet site to view or order additional technical publications. For accessing instructions, contact the representative who handles your account. Check your extranet site often as the information is updated frequently.

A

Hardware Configuration Procedures for the Cisco UCS C240

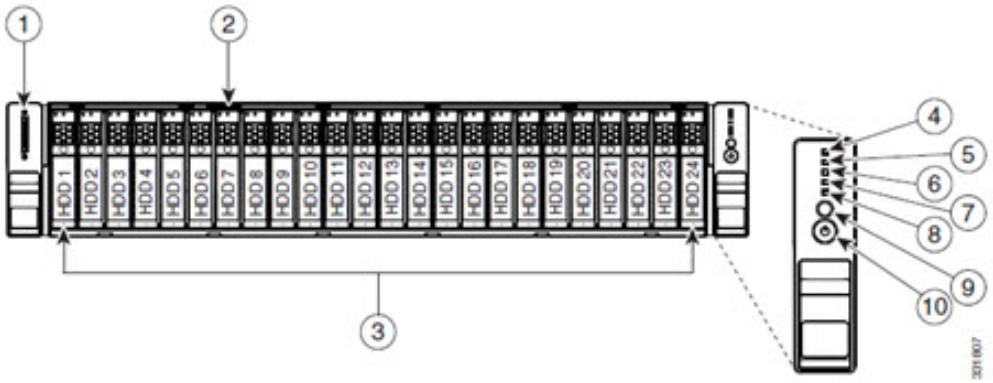
Introduction

This appendix contains procedures for configuring Cisco's UCS C240 M3 and UCS C240 M4 server for use with System Release 9.0.

In This Appendix

Hardware Diagram of the Cisco UCS C240 M3 Server

Chassis Front View

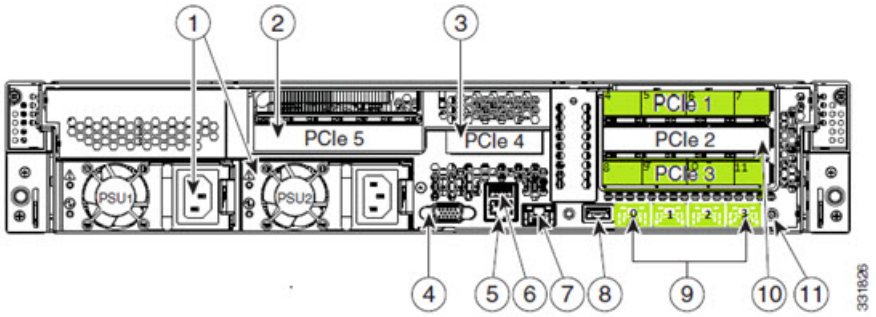


Slot	Description	Slot	Description
1	KVM connector (Used with KVM cable that provides two USB, one VGA, and one serial connector)	6	Temperature status LED
2	Asset tag (serial number)	7	Fan status LED
3	Drives (up to 24 2.5-inch hot-swappable drives)	8	System status LED
4	Network link activity LED	9	Identification button/LED
5	Power supply status LED	10	Power button/power status LED

Chassis Rear View

Important: Make sure that the network cards are installed in the slots shown in this diagram.

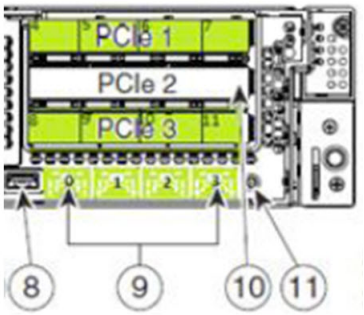
Note: Only the essential features of the rear panel are shown. A more detailed image follows.



Slot	Description	Slot	Description
1	Power supplies (up to two)	7	One RJ-45 10/100/1000 Ethernet dedicated management port
2	Standard-profile PCIe slot on riser 2: PCIe 5 - full height, 3/4-length, x16 lane width, x24 connector, GPU ready	8	USB 2.0 port
3	Low-profile PCIe slot on riser: PCIe 4 - half-height, 3/4-length, x8 lane width, x16 connector, no NCSI support	9	Quad 1-GB Ethernet ports (LAN1, LAN2, LAN3, LAN4)
4	VGA video connector	10	Standard-profile PCIe slots on riser 1 (three): ■ PCIe 1-full-height, half-length, x8 lane width, x8 connector ■ PCIe 2-full-height, half-length, x16 lane width, x24 connector (supports Cisco Virtual Interface Card (VIC) ■ PCIe 3-full-height, half-length, x8 lane width, x16 connector

Slot	Description	Slot	Description
5	Serial connector (RJ-45)	11	Rear identification button/LED
6	USB 2.0 port		

Detailed View of PCI Ports



- Top row contains ports 0, 1, 2, 3
- Middle row contains ports 4, 5, 6, 7
- Bottom row contains ports 8, 9, 10, 11

Tested Reference Configuration

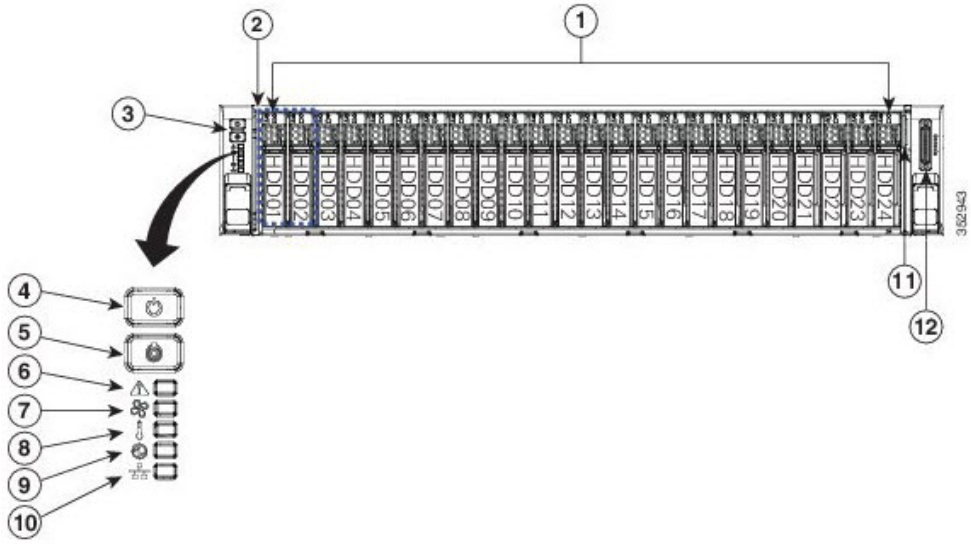
Network ports are numbered and marked as green. Cables should be run to the below designated ports.

- NIC Ports 1 and 7 — ESXi Management
- NIC Ports 8 and 4 — Headend network
- NIC Ports 9 and 5 — Corporate network
- NIC Ports 10 and 6 — RepDB network
- NIC Ports 2 and 11 — Headend 2 network (DSG)
- NIC Port 0 — TED crossover
- NIC Port 3 — Open

  Important: The DOCSIS Set-Top Gateway (DSG) network is only used if you have the licensed feature. Otherwise, these ports are unused at this time.

Hardware Diagram of the Cisco UCS C240 M4 Server

Chassis Front View

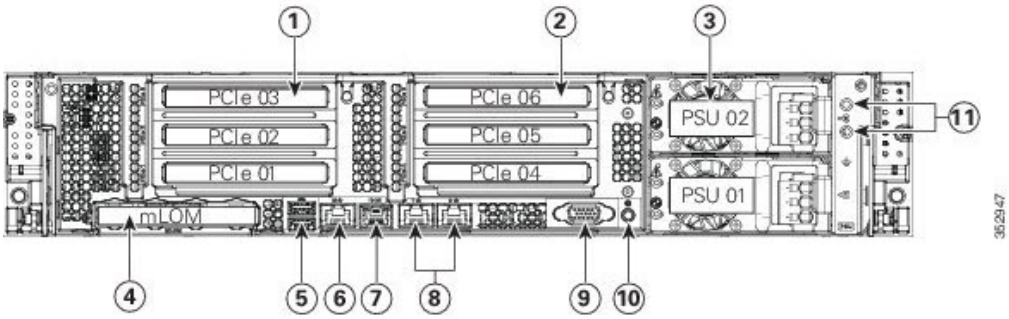


Slot	Description	Slot	Description
1	Drive bays 1-24 supports SAS/SATA drives	7	Fan status LED
2	Drive bays 1 and 2 supports NVMe PCIe SSDs and SAS/SATA drives	8	Temperature status LED
3	Operations panel buttons and LEDS Drives (up to 24 2.5-inch hot-swappable drives)	9	Power supply status LED
4	Power button/power status LED	10	Network link activity LED
5	Identification button/LED	11	Pull-out asset tag (serial number)
6	System status LED	12	KVM connector (Used with KVM cable that provides two USB, one VGA, and one serial connector)

Chassis Rear View

Important: Make sure that the network cards are installed in the slots shown in this diagram.

Note: Only the essential features of the rear panel are shown. A more detailed image follows.



Slot	Description	Slot	Description
1	PCIe riser 1 (slots 1, 2, 3*) * Slot 3 not present in all versions.	7	Serial port (RJ-45 connector)
2	PCIe riser 2 (slots 4, 5, 6)	8	Dual 1-Gb Ethernet ports (LAN1, LAN2)
3	Power supplies (DC power supply shown)	9	VGA video port (DB-15 connector)
4	Modular LAN-on-motherboard (mLOM) card slot	10	Rear Unit Identification button/LED
5	USB 3.0 ports (two)	11	Grounding-lug holes (for DC power supplies)
6	1-GB dedicated management port		

PCI Ports

- Bottom row contains ports 0, 1
- Top left row contains ports 2, 3, 4, 5
- Top right row contains ports 6, 7, 8, 9

Tested Reference Configuration

Network ports are numbered and marked as green. Cables should be run to the below designated ports.

- NIC Ports 1 and 7 — ESXi Management
- NIC Ports 8 and 4 — Headend network
- NIC Ports 9 and 5 — Corporate network
- NIC Ports 10 and 6 — RepDB network
- NIC Ports 2 and 11 — Headend 2 network (DSG)
- NIC Port 0 — TED crossover
- NIC Port 3 — Open

  Important: The DOCSIS Set-Top Gateway (DSG) network is only used if you have the licensed feature. Otherwise, these ports are unused at this time.

Hardware Requirements for a New UCS Install

The following hardware is required to install a new UCS server. This is in addition to the hardware requirements defined in Hardware Requirements.

- KVM Cable Adapter (provided with the UCS)
- Standard USB Keyboard
- Monitor with a VGA cable
- A KVM with the appropriate adapters can be used in place of the monitor and keyboard

Cisco UCS C240 Server CIMC Configuration

Important:

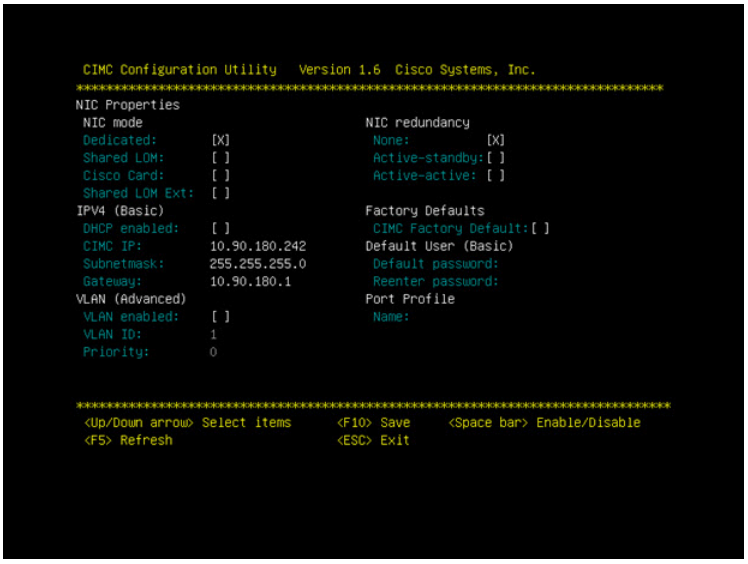
- This procedure is used for both the C240 M3 and C240 M4 servers and only needs to be performed once — when you initially install the server.
- Make sure that you use configuration data that pertains to the system that you are migrating. The screen-capture in step 5 is to be referenced as an example only.

1. Obtain the ***UCS C240 Quick Start Guide***. This guide is shipped with the server.
2. Follow the instructions in the ***UCS C240 Quick Start Guide*** through step 5.
3. Press the **Power** button to power on the UCS C240 server.
4. Press **F8** at the Cisco screen. The server boots to the CIMC Configuration Utility window.

   Important: Note the BIOS Version on the Cisco splash screen as the system is booting.
5. Use the information in the CIMC Configuration Utility window to complete the configuration.

   Note: In addition to the information in the CIMC Configuration Utility window, make sure to obtain the network IP address for the CIMC interface.

   Important: The following image is an example only. Do not use the IP address, netmask, or gateway in the image.



6. Enter a default password and re-enter it at the prompt. Store this password in a safe place for future use.
7. Press **F10** to save changes.
8. Press **Esc** to exit. The EFI shell prompt may appear.

Cisco UCS C240 Host Configuration

Important:

- This procedure only needs to be performed once — when you initially install the UCS C240 server.
- The CIMC firmware and BIOS version (noted in step 4 of ***Cisco UCS C240 Server CIMC Configuration*** (on page 173)) should be at or higher than the minimum required version found in the **Tested Reference Configuration** chart in the Preface. If it is not, contact Cisco Support for assistance in upgrading the firmware and the BIOS.

RAID Configuration

Important: This procedure only needs to be performed once — when you initially install the UCS C240 server.

Go to the appropriate section to configure RAID on your UCS hardware.

- *Configuring RAID for UCS C240 M3 Servers* (on page 175)
- *Configuring RAID for UCS C240 M4 Servers* (on page 182)

Configuring RAID for UCS C240 M3 Servers

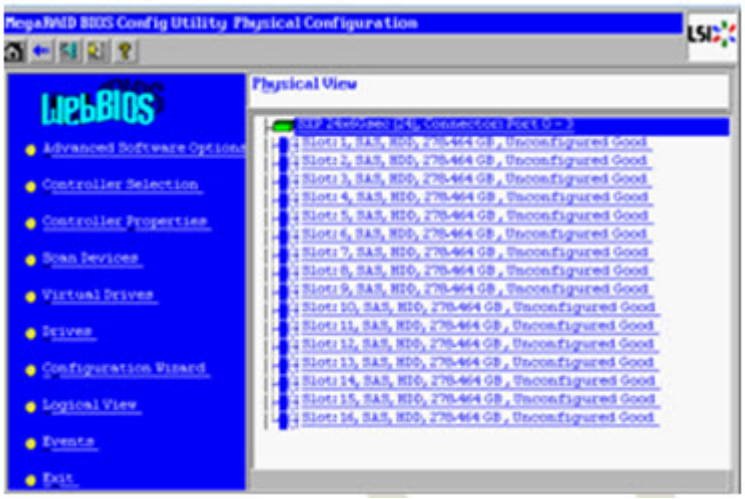
Important: This procedure only needs to be performed once — when you initially install the UCS C240 server.

The UCS hardware RAID configuration for this system release consists of a RAID 10 (14x300GB disks) for the OS disk, and two global hotspares (2X300 GB disks). This section details the steps necessary to create these volumes and hot spares.

1 Press **Ctrl-Alt-Del** to reboot the server.

2 Watch the reboot process closely. After the disks are displayed, observe the boot messages and press **Ctrl-R** when prompted to access the WebBIOS (RAID Configuration Utility). After a few minutes, a **Start** button appears.

3 Click **Start** to configure RAID. The MegaRAID BIOS Config Utility main menu appears.



4 Click the **Configuration Wizard** link in the left pane of the utility menu.

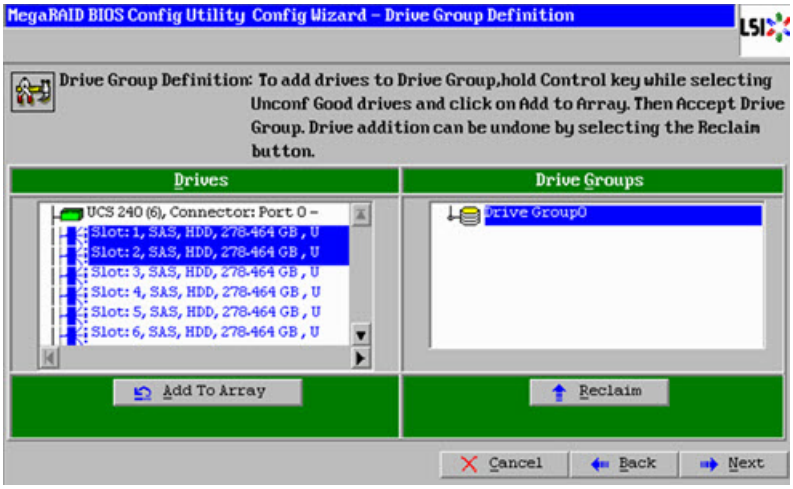
5 Click **New Configuration** and click **Next**. The utility prompts you to clear the existing configuration.

6 Click **Yes**.

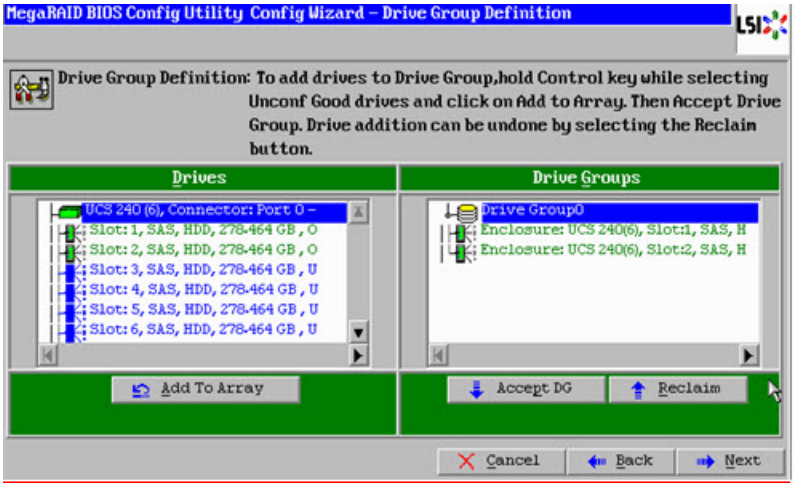
7 Click **Manual Configuration** and click **Next**. The Drive Group Definition screen appears.

Note: Within the drives panel, there is a list of all 16 hard drives. Create 7 drive groups (0-6), each consisting of 2 disks (1 and 2, 3 and 4, and so on). Drives 13 and 14 are your final drive group.

8 Select the **Slot 1** disk, and while pressing the **Ctrl** key, click the **Slot 2** disk to highlight both disks.



9 Click **Add to Array** to form **Drive Group (0)**.



10 Click **Accept DG**.

11 Repeat steps 8 through 10 for the following drive pairs:

Slots 3 and 4

Slots 5 and 6

Slots 7 and 8

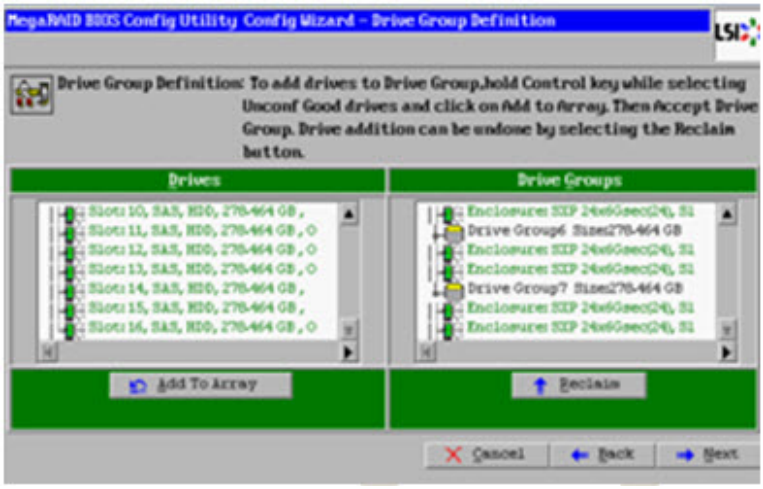
Slots 9 and 10

Slots 11 and 12

Slots 13 and 14

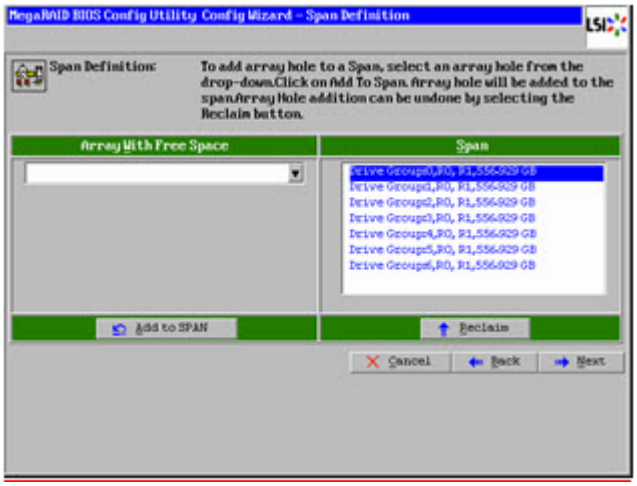
Result: The system creates a drive group for each pair.

Note: When you complete this step, you should have 7 drive groups (0 - 6).

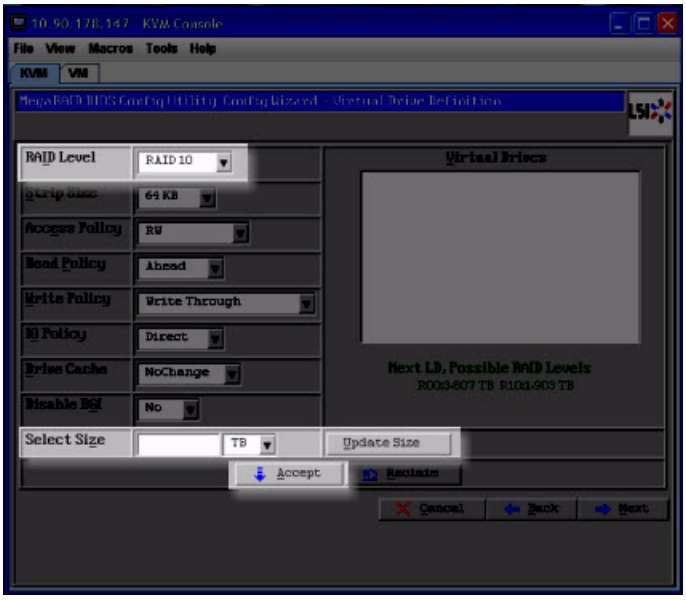


12 Click **Next** and select **Drive Group 0**.

13 Select each drive group, one by one, and click **Add to SPAN** to add all drive groups to the span list.

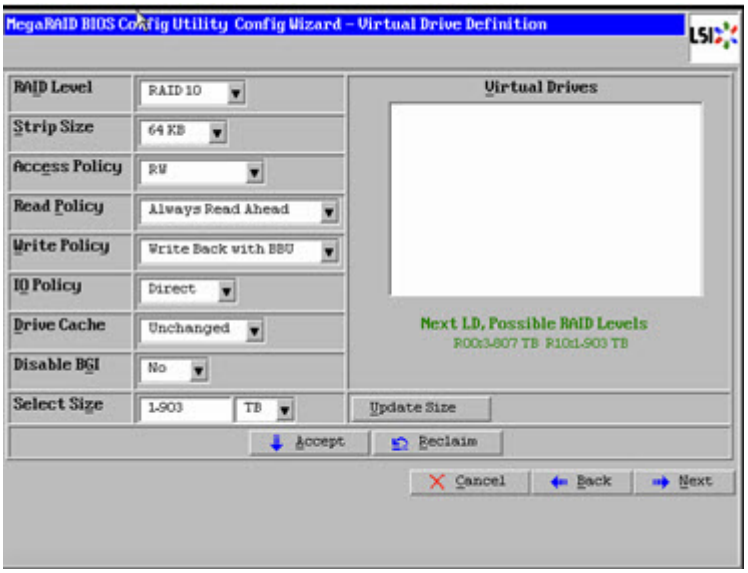


14 Click **Next**. The Virtual Drive Definition window appears.



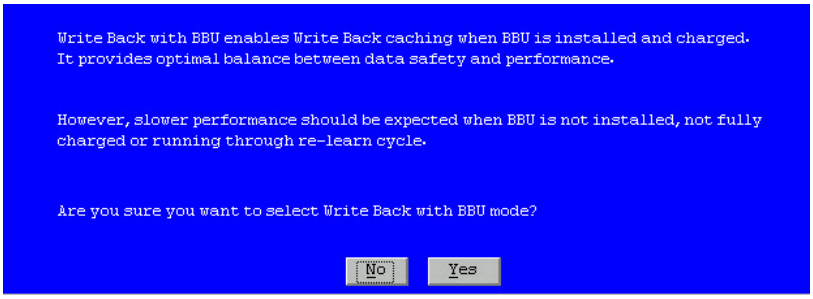
15 Select **RAID 10** from the RAID Level drop-down menu.

16 Click **Update Size**. The maximum allowed size for the selected RAID level populates the **Select Size** field.

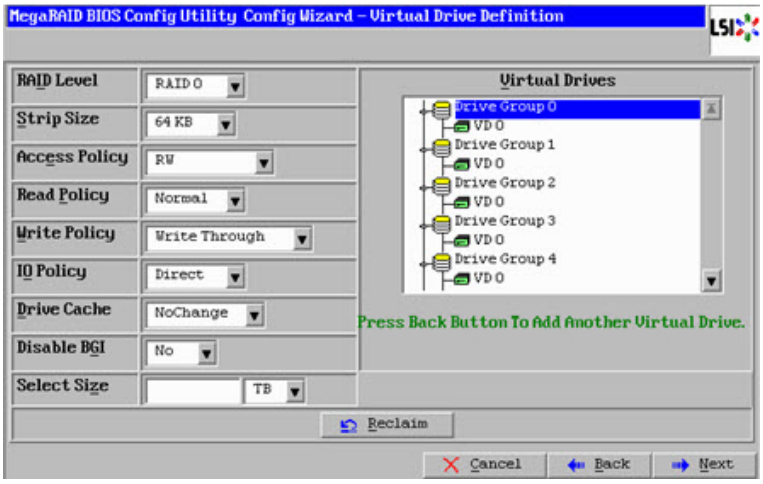


17 Record the **Select Size** here: _____

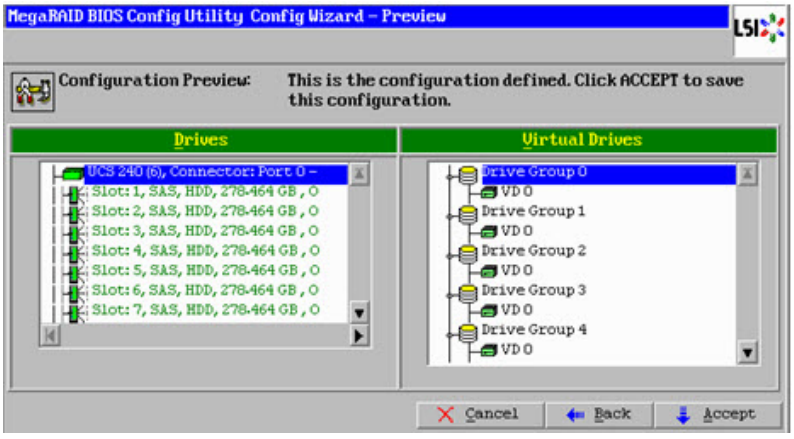
18 Click **Accept**. The Write Policy window appears.



19 Click **Yes** to confirm the default write policy. The total list of Vdisks created from Drive Groups 0-6 appears.

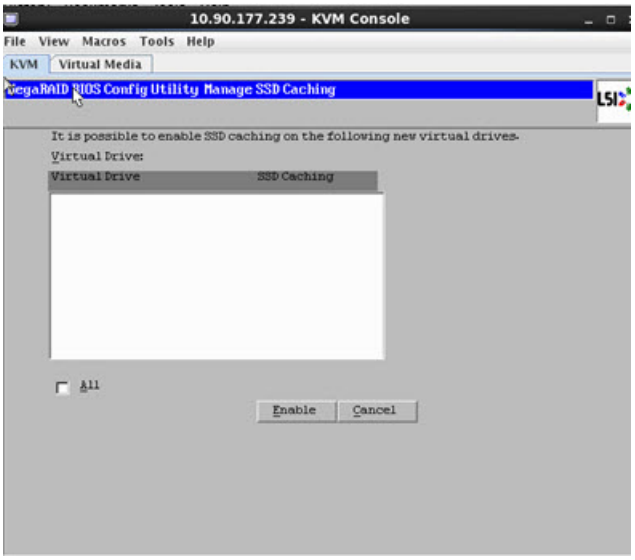


20 Click **Next**.

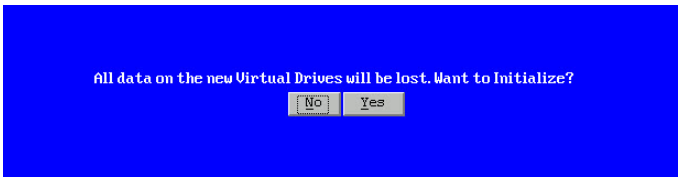


21 Examine the configuration preview to verify that the virtual drives match the previous list and click **Accept**. The system prompts to confirm saving the configuration.

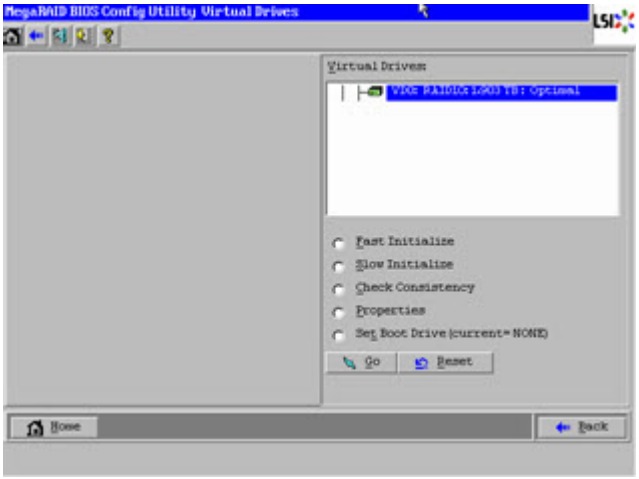
22 Click **Yes**. A warning message appears and indicates that you may lose data.



Note: After canceling the previous screen, you are prompted to initialize the new virtual drives.

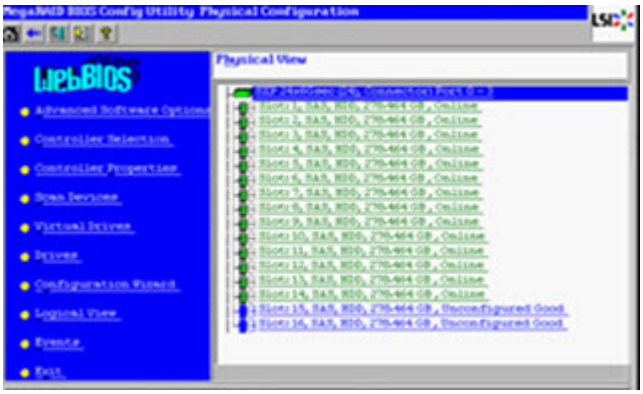


23 Click **Yes** to initialize. The Virtual Drive VD0 is displayed.



24 Click **Home**. The Raid Configuration utility main menu appears.

25 Click the **Physical View** from the left pane if it is not currently displayed.

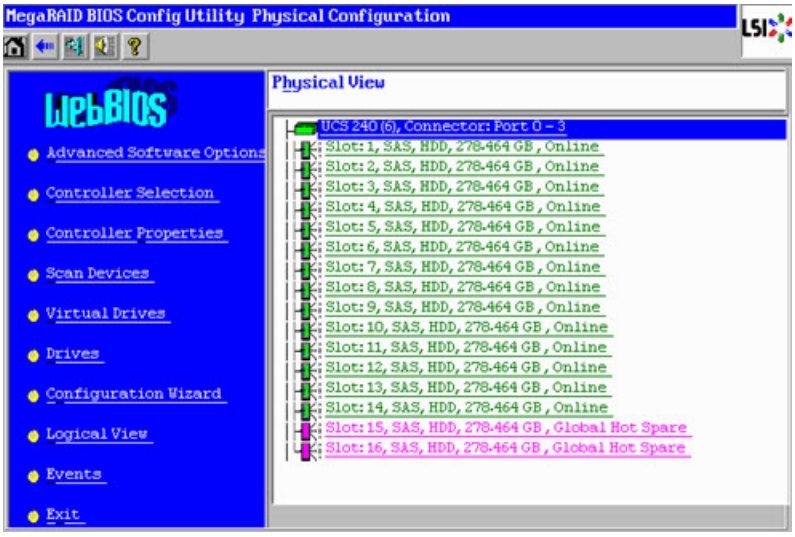


26 Click the drive on Slot 15 in the Physical View.

27 Click the option **Make Global HSP** and click **Go** to save.

28 Click **Back** and repeat steps 26 and 27 for the drive in Slot 16.

29 Click **Home** and select the **Physical View** (if it is not displayed by default).



30 Verify that the drives in Slot 15 and 16 are visible as Global Hotspares.

31 From the Main Menu, click **Exit** to exit the RAID Configuration Utility.

32 Click **Yes** to confirm exiting the utility.

Important: At this point, you may be prompted to reboot the computer. **Do NOT reboot**. It is very important that you do not reboot the computer at this time.

Configuring RAID for UCS C240 M4 Servers

Complete the following steps to configure RAID for a C240 M4 UCS server.

1 Power on the Cisco UCS C240 M4 server.

Note: If the server is already powered on, reboot the server.

2 On boot up, press **CTRL+R** to enter the Cisco 12G SAS Modular Raid Controller BIOS Configuration Utility.

3 Press **CTRL+N** and then click the **PD Mgmt** tab.

4 Use the **UP** or **DOWN** arrow keys to move between the disks.

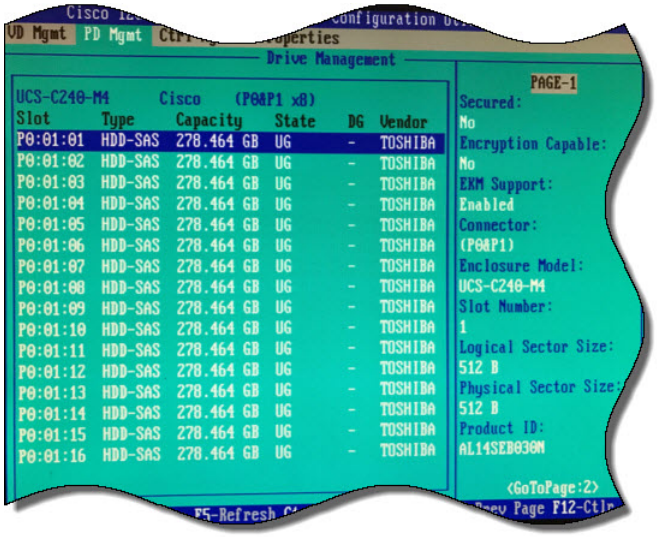
5 Complete the following steps to change the disks from Just a Bunch Of Disks (JBOD) to **Unconfigured Good (UG)**.

a Select the first disk and press **F2**.

b Select **Make unconfigured good**.

c When prompted to confirm the change, click **Yes** and press **Enter**. The state of the drive will change from JBOD to UG.

d Repeat steps 4a through 4c for the remaining drives.



6 Go back to the **VD Mgmt** tab and press **CTRL+P**.

7 Select **No Configuration Present** and press **Enter**.

8 Configure the following:

   a From the RAID Level area, select **RAID-10**.

   b From the Secure VD area, select **No**.

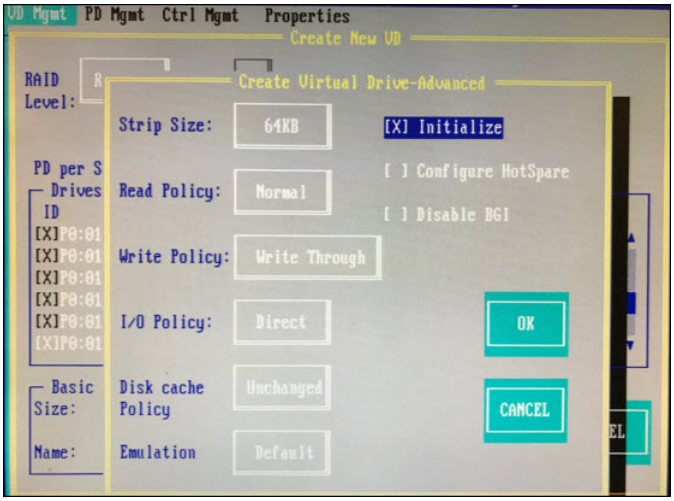
   c From PD per Span area, enter **2**.

   d From the Drives area, use the UP or DOWN arrow to highlight the appropriate drive and press **Enter**. An **X** displays next to the drive to indicate that it is selected.

   e Repeat step 8d to select the next drive that will make up this drive pair.

9 Click **Advanced** option and highlight the **Initialize** option.

10 Press **Enter**. An **X** is inserted next to Initialize to indicate that it is selected.



11 Click **Ok**.

12 Click **Ok** to close the Advanced window. The Configuration window is displayed.

13 Click **Ok** and system will now initialize the RAID-10 array. Wait for the initialization to complete.

14 Click **Ok** after the Confirmation window indicates that the initialization is complete.

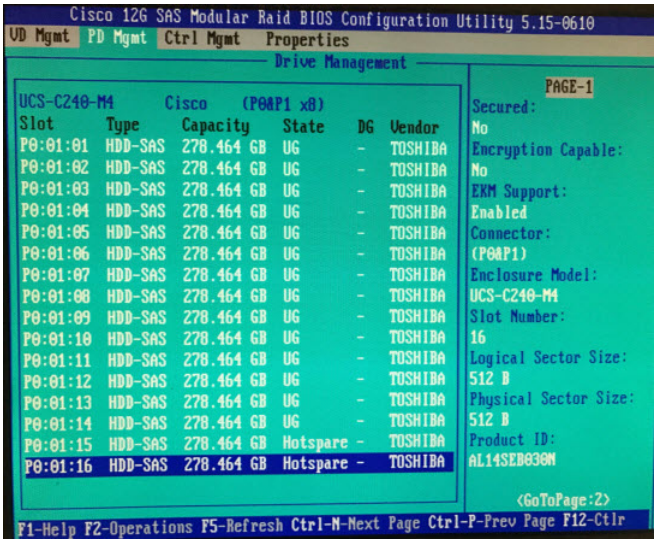
15 Click **CTRL+N** to return to the **PD Mgmt** window.

16 From the PD Mgmt window, use the **UP** or **DOWN** arrows to highlight drive **P0:01:15**.

17 Press **F2** and then select **Make Global HS**.

   Note: The state of the drive changes from **UG** to **Hotspare**.

18 Press **ESC** and then repeat steps 16 through 17 for drive **P0:01:16**.



19 Press **ESC** and click **Ok** to exit the utility.

20 Click the **Macros** tab and select **Static Macros > CTRL+ALT+DEL** to reboot the server.

Note: The server must be rebooted for the changes to go into effect.

ESXi Installation

Important: This procedure is written for both the C240 M3 and C240 M4 servers and only needs to be performed if you are executing an initial installation or moving to new hardware.

Before You Begin

Note: The Firefox browser is not officially supported for accessing the UCS C240 M3/C4 CIMC application.

1. Use a Web browser to open the CIMC application, using the IP address configured in ***Cisco UCS C240 Server CIMC Configuration*** (on page 173).
2. Log onto the server using the admin password or the password that you set in ***Cisco UCS C240 Server CIMC Configuration*** (on page 173).

Power Policy

1. Click **Power Policies**.
2. Choose **Restore Last State** from the menu.
3. Click **Save Changes**.
4. Click **Summary** on the Server tab in the CIMC.
5. Click **Launch KVM Console** from the Server Summary window.
6. Select open using java viewer in the dialog box. The KVM Console is displayed.

Installing ESXi

Important: Before beginning this procedure, make sure that you have downloaded or copied the VMware ISO image to the local hard drive that is running the CIMC application.

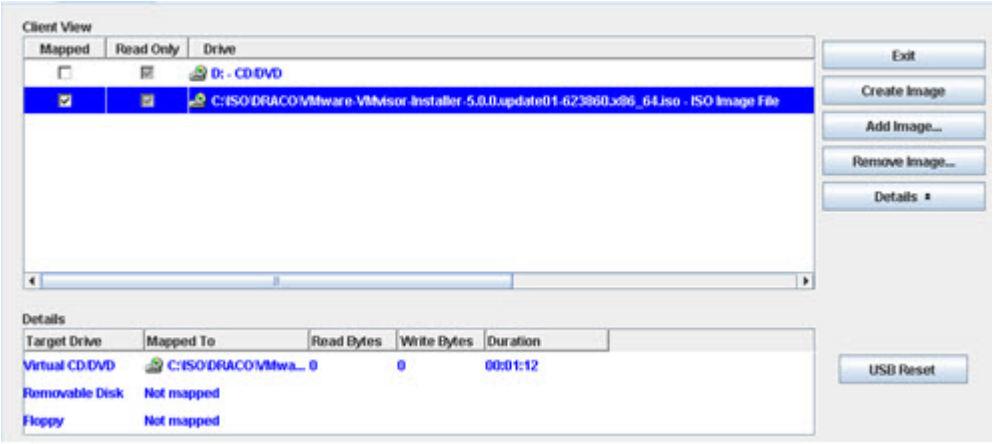
1 Follow these instructions to mount the ESXi ISO image.

   a Click the **Virtual Media** tab in the KVM Console.

   b Click **Add Image**.

   c Browse to the location of the VMware ISO image and select **Open**.

   d Click the **Mapped** box next to the added image.



   e Click the **KVM** tab in the KVM Console.

2 Select **Macros** and then the **Ctrl-Alt-Del** option from the KVM menu bar to reboot the server.

   Note: Later versions of firmware may refer to **Static Macros**.

3 Press **F2** when the Cisco screen is displayed to enter the system setup.

4 Navigate to the **Boot Options** tab.

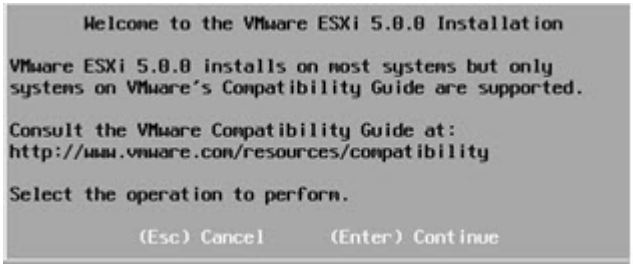
5 Make the following selections:

   - Boot Option 1 — RAID Adapter
   - Boot Option 2 — Virtual CD/DVD
   - Disable remaining boot options

6 Press **F10** to save the settings and reset system.

7 Click **Yes** to save the settings and reset the system.

8 Wait for the ESXi installer to load. After the ESXi load completes, a **Welcome** message appears.



9 When prompted, press **Enter** to continue.

10 When prompted, press **F11** to accept the license agreement.

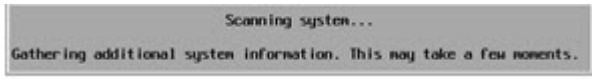
Note: This action selects the disk. Select the disk that matches the size of the Virtual Disk that was recorded in RAID Configuration, step 17.

11 Press **Enter** to continue.

12 Select the appropriate keyboard layout (for example, **US default**) and press **Enter**.

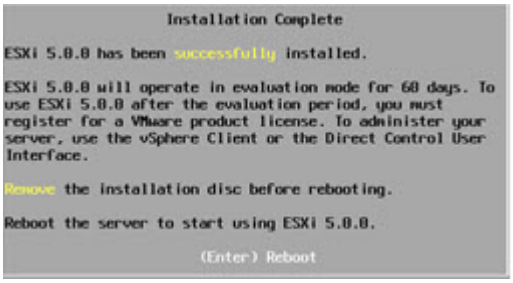
13 Enter and confirm a new **root** password for the ESXi host.

14 Press **Enter** to continue.



15 Press **F11** to confirm the installation on the selected disk. The ESXi installation begins and a progress bar appears.

16 When the installation completion screen is displayed, press **Enter** to reboot. The ISO is un-mapped and the system boots to the VMware ESXi window.



Important: Let the system boot into ESXi. If you press F2 too early (during boot-up), the BIOS configuration screen appears, which is not what you want.

17 Press **F2** to customize the system.

18 Log in as **root** user. The System Customization window appears.

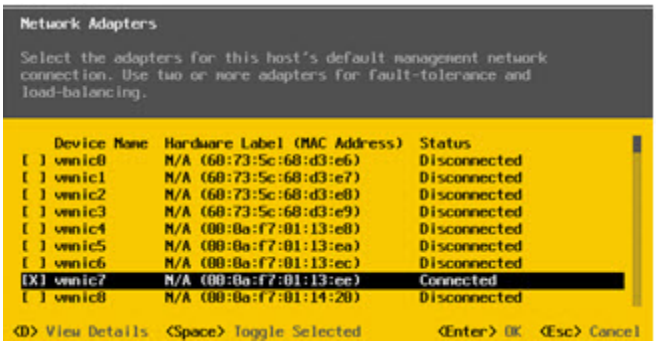
19 Navigate to **Configure Management Network** and press **Enter**.

20 Select **Network Adapters** and press **Enter**.

21 To select a vmnic, highlight the line you want and press the **Spacebar**.

Note: For the UCS 240 server, enable nic 1 and 7; disable the others. These nics are for ESXi access.

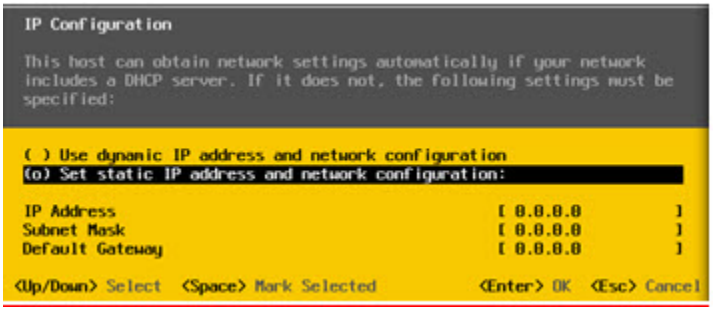
22 Verify that the devices you enabled in step 21 show a **Connected** status.



23 Press **Enter**. The system returns to the Configure Management Network window.

24 Select **IP Configuration** and press **Enter** to set/modify the IP address.

25 Use the arrow keys to highlight **Set static IP address** and press the **Spacebar**.



26 Provide the following information to configure the ESXi server:

- IP Address
- Subnet Mask
- Gateway

27 Press **Enter** to accept the changes.

28 Use the arrow keys to highlight **DNS configuration** and then press **Enter**.

29 Provide the following information.

- Primary DNS IP address
- Secondary DNS IP address (optional)
- Hostname

30 Press **Enter** to accept and return.

31 Press **Esc** to exit and press **Y** to accept the changes when prompted.

32 Select **Test Management Network** and press **Enter** to navigate to the Test Management Network dialog.

33 Press **Enter** to begin a ping test.

34 After the ping test is complete, press **Enter** to exit the test dialog.

35 See the site Network Administrator to verify addressing and cabling.

36 Scroll to **Troubleshooting Options** and press **Enter**.

37 Select **Enable SSH** and press **Enter**. The right-hand panel mode should indicate **SSH is Enabled**.

38 Press **Esc** to exit.

39 Press **Esc** to log out and disconnect the KVM.

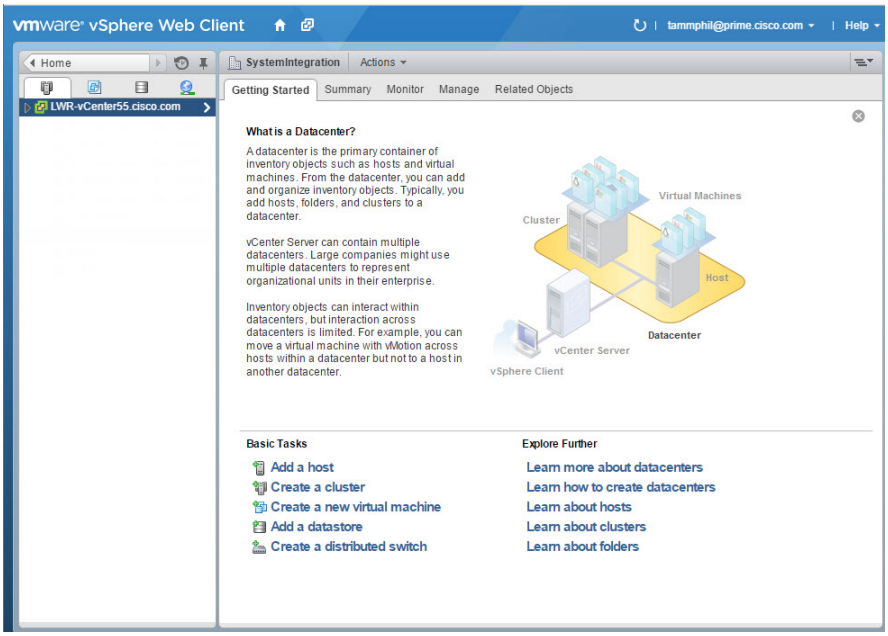
40 Click **File/Exit** to close the KVM console.

Configure the Host System

Important: This procedure is written for the C240 M3 and C240 M4 servers and only needs to be performed once — when you initially install the UCS C240 server.

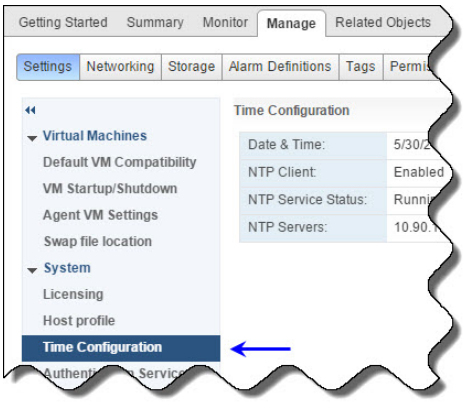
You must have a Windows, Linux, or Mac OS system with vSphere installed to complete the installation and migration of SR 9.0.

1. Provide the IP address, username, and password for the new ESXi host to the vCenter administrator. Once the administrator licenses the new host, you can able to access it through vCenter.
2. Use the VMware vSphere Web Client to connect to the vCenter server by providing the IP address, username and password for authentication.
3. Click **Hosts and Clusters**. The Host and Clusters view displays.



4. Drill down in the dropdown list to locate and select the new ESXi host.
5. Click the **Manage** tab and then click the **Settings** menu button to begin configuring resources.

6 From the **System** dropdown list on the left pane, click **Time Configuration** to modify the date and time.



7 Click **Edit**. The Edit Time Configuration window displays.

8 Complete the following steps to update the date and time.

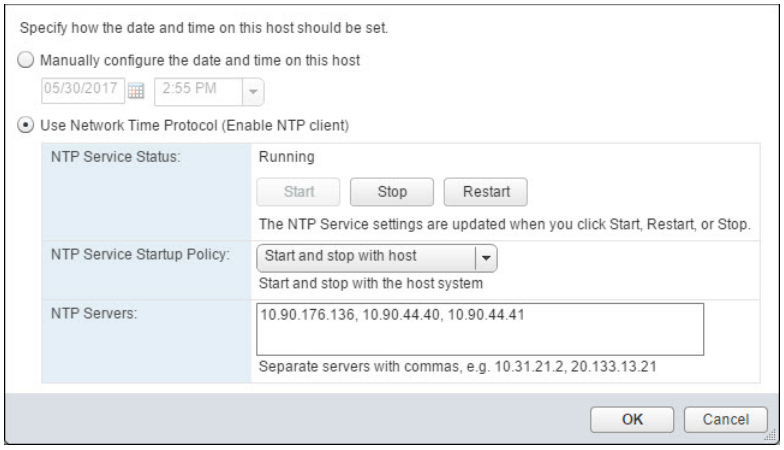
a Click **Use Network Time Protocol (Enable NTP client)**.

b From the NTP Server Startup Policy area, select **Start and stop with host**.

c From the NTP Servers area, enter the IP Addresses for your NTP servers separated by a comma.

d From the NTP Service Status area, click **Restart**.

e Verify that that NTP Service Status indicates **Running** and then click **OK**. You are returned to the Settings window.



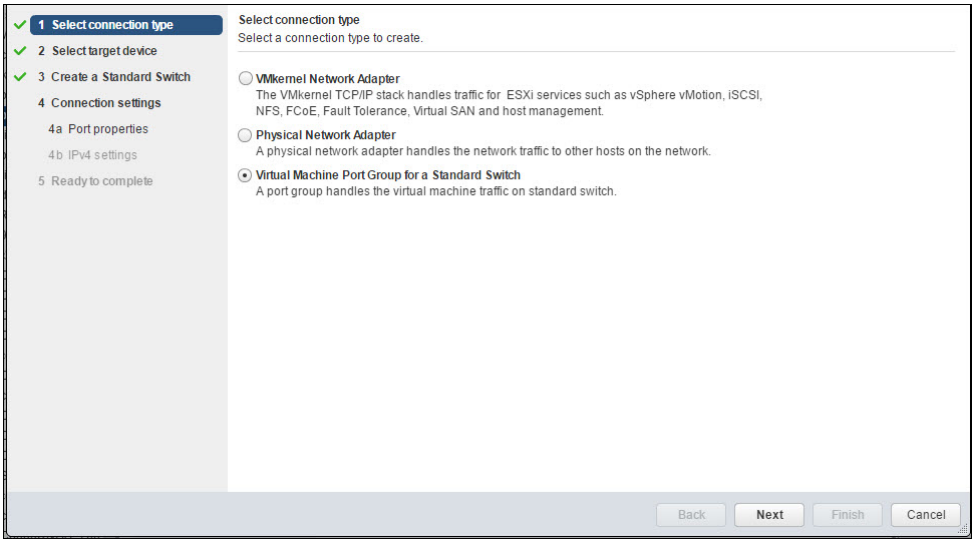
9 From the top area of the window, click the **Networking** tab and then click **Virtual Switches**.

10 From the Virtual switches area, select **vSwitch0**. The Standard switch: vSwitch0 (VM Network) area displays in the lower section of the window.

11 From the Virtual switches area, click the **Remove selected standard switch** icon (✖)

12 When prompted to remove the switch, click **Yes**.

13 From the Virtual switches area, click the **Add host networking** icon ( ) to configure the network adapters for your system. The Add Networking > Select connection type window displays.



14 Select **Virtual machine Port Group for a Standard Switch** and click **Next**. The Select target device window displays.

15 Select **New standard switch** and then click **Next**. The Create a Standard Switch window displays.

16 Click the **Add adapters** icon ( ). The Add Physical Adapters to the Switch window displays.

17 From the Network Adapters area, select the appropriate adapter for the Management network (i.e. vmnic1) and then click **OK**. You are returned to the previous screen where the new network adapter is added to the Active adapters list.

Note: Refer to the following chart to help you configure the network host system settings.

Network	UCS 240-M3	UCS 240-M4
ESXi Management	1, 7	1, 7
Headend network	4, 8	4, 8
Corporate network	5, 9	5, 9
RepDB network	10, 6	10, 6
Headend 2 network (DSG)	2, 11	2,11
TED crossover	0	0

18 Click the **Add adapters** icon again (+) and select the second network adapter for the vSwitch. Then click **OK**.

19 From the Create a Standard Switch window, click **Next** and then click **OK**. The Connection settings window displays.

20 From the **Network label** text box, change the label name to a name that is appropriate for the network adapter (for example, Management Network). Then click **Next**. The Ready to complete window displays.

Note: The vSwitch labels used in this document are suggested labels only. You can name this and the remaining vSwitches to reflect your system configuration.

21 Click the **Use static IPv4 settings** radio button and then enter the **IPv4 address** and **Subnet** mask. Click **Next**.

22 Review the settings and click **Finish**.

23 Monitor the **Recent Tasks** area to confirm that the network configuration completed successfully.

24 Repeat steps 13 through 23 to create the Headend Network on vSwitch1.

Notes:

- Use the chart in step 17 to configure the proper headend network adapters for your system.
- When entering the Network label, make sure you enter a name that identifies the network as the headend.

25 Repeat steps 13 through 23 to configure the following networks shown in the network design that was created for the customer.

The following examples are for reference only.

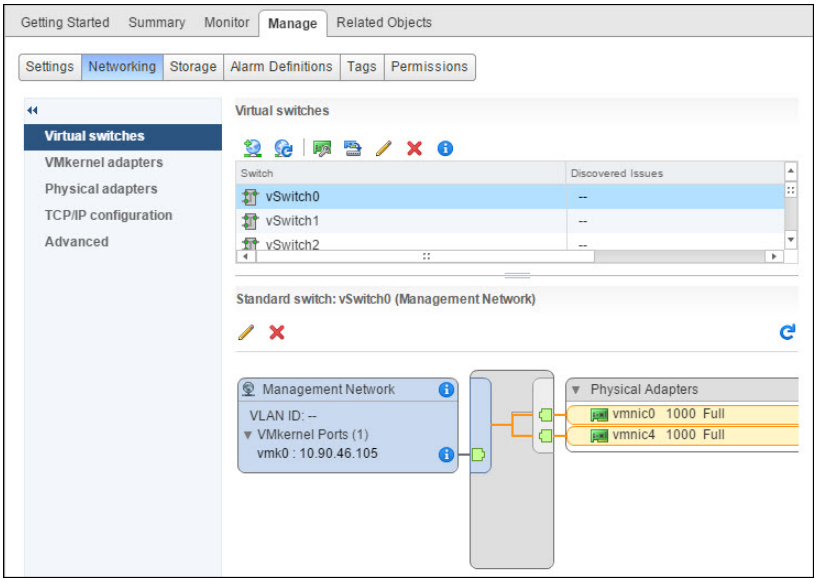
- **Corporate Network —** for corporate and back office access. This is created under **vSwitch 2.**
- **TED XOR Network —** for direct crossover connectivity with the TED. This is created under **vSwitch3.**
- **RepDB Network —** for direct connectivity to the RepDB interface when RepDB is an enabled feature. This is created under **vSwitch4**.

  Note: This network is optional and should be configured only if you are using RepDB.
- **Headend 2 Network —** this vSwitch may be used for DSG or other network requirements. This is created under **vSwitch5**.

  Note: This network is optional and should be configured only if needed.

26 To review the networking for each vSwitch, click on a vSwitch from the Virtual switches area. The Networking diagram is displayed.

Example for vSwitch0:



27 To configure the **Storage Configuration**, click the **Storage** tab.

28 From the left area of the window, click **Storage Devices**.

29 Select **datastore1** and click the **Updates the SCSI LUN display name of the selected device (**) icon.

30 In the **Name** text box, rename the device to **<hostname>_local_storage1**. Click **OK**.

Note: Cisco engineers have seen some issues when the datastore name contains blank spaces. Do not include spaces when you rename the datastore.

31 If necessary, create an NFS mapping to the location of the Linux platform image.

a Right-click the ESXi host and select **New Datastore**. The New Datastore window displays and lists the Location where the new datastore will reside.

b Click **Next**.

c Select **NFS** and click **Next**.

d In the Datastore name field, replace the name with something that describes your datastore.

e In the Server field, enter the name or IP address of the server.

f In the Folder field, enter path to the folder you want to access.

g Click the **Mount NFS as read-only** check box and then click **Next**.

h Verify the settings and click **Finish**.

B

System Verification Procedures

Introduction

Use these procedures to verify that an active communication link exists between the EC and DHCTs. The EC must be able to communicate with DHCTS to have a successful system upgrade.

In This Appendix

Verify the System Upgrade

Verifying the System Upgrade

Important: If any of the following tests fail, troubleshoot the system to the best of your ability. If you are unable to resolve the failure, contact Cisco Services for assistance.

1. As **dncs** user, type the following command and press **Enter**:

   ```
   [dncs@ecnextx9 ~]$ cd /dvs/dncs/Utilities/doctor
   ```

2. Type the following command and press **Enter**. This command runs the Doctor report.

   ```
   [dncs@ecnextx9 ~]$ doctor -vn
   ```

3. When the Doctor report completes, review it to ensure that communications exist among all DBDS elements.

4. Type the following command and press **Enter** to verify that you are using no more than 85 percent of the partition capacity of each disk:

   ```
   [dncs@ecnextx9 ~]$ df -k
   ```

   Important: If any disk partition lists a capacity greater than 85 percent, contact Cisco Services before proceeding.

5. Stage at least one new DHCT to your site's specifications. After staging the DHCT, verify the following:

   - The DHCT receives 33 or 34 EMMs.
   - The DHCT successfully receives its Entitlement Agent.

6. Complete these steps to perform a slow and fast boot on a test DHCT and Combo-Box (if available) with a working return path (2-way mode):

   a. Boot a DHCT.

      Note: Do not press the power button.

   b. Access the Power On Self Test and Boot Status Diagnostic Screen on the DHCT and verify that all parameters, except UNcfg, display **Ready**.

      Note: UNcfg displays Broadcast.

   c. Wait 5 minutes.

   d. Press the power button on the DHCT. The power to the DHCT is turned on.

   e. Access the Power On Self Test and Boot Status Diagnostic Screen on the DHCT and verify that all parameters, including UNcfg, display **Ready**.

7 Verify that you can ping the DHCT.

8 Verify that the Interactive Program Guide (IPG) displays 7 days of accurate and valid data.

9 Tune to each available channel on a DHCT to confirm that a full channel lineup is present.

Note: Record any anomalies you notice while verifying the channel lineup.

10 For all sites, verify that you can define, purchase, and view an IPPV, xOD, and VOD event.

Verify the Channel Map After the Upgrade

Verify that the channel map associated with various types of DHCTs in the headend is accurate for each specific hub. If you notice that the channel map is not accurate, complete the following steps.

Delete the sam File Server

1 Have you confirmed that there are inaccuracies in the channel map of various DHCTs?

- If **yes**, go to the next step.
- If **no**, check the channel map associated with various types of DHCTs in the headend for each specific hub.

  Note: Complete the procedures in this section only if the channel maps are not accurate.

2 From the EC Web UI, click the **Navigation** button and then select **App Interface Modules > BFS Client**. The Site DNCS Broadcast File Server List window opens.

3 Highlight the **sam** file server.

4 Click **File > Delete**. A confirmation message appears.

5 Click **Yes** and press **Enter**. The system deletes the sam file server.

Bounce the saManager Process

1 From the EC Web UI Process Status window, click the button next to the **saManager** process.

2 Click **Stop**. In a few minutes, the indicator for the saManager process changes from green to red.

Note: Do not go to the next step until the indicator has changed from green to red.

3 Click the button next to the **saManager** process again.

4 Click **Start**. In a few minutes, the indicator for the saManager process changes from red to green.

Save the Channel Map Web UIs

1. Wait the length of time of the SAM Configuration Update Timer.

   Note: You can find this value on the SAM Configuration window.

2. Examine again the channel maps for the DHCTs.
   - If the channel maps are accurate, you are finished with this procedure.
   - If the channel maps are still inaccurate, go to the next step.
3. Open the Channel Map user interface for each applicable channel map, and click **Save**.

   Note: Do not make any changes on the Web UI; simply click **Save**.
4. Wait again the length of time of the SAM Configuration Update Timer.
5. Examine each channel map again for accuracy.

Checking the EAS Configuration

After installing the SR 9.0 software, verify that your EAS equipment is working correctly by testing the system's ability to transmit EAS messages. Refer to **Conduct EAS Tests** in the ***EC 9.0 Online Help***.

C

SR 9.0 Rollback Procedures

Introduction

The SR 9.0 rollback procedures are intended for field service engineers who encounter problems while upgrading an existing digital system to SR 9.0. Prior to executing the SR 9.0 rollback procedures, contact Cisco Services.

In This Appendix

Activate the Old System Release

1. As **dncs** user, type the following commands to stop all system components.

   ```
   [dncs@ecnextx9 ~]$ appStop
   [dncs@ecnextx9 ~]$ dncsStop
   [dncs@ecnextx9 ~]$ appKill
   [dncs@ecnextx9 ~]$ dncsKill
   ```

2. As **admin** user, type the following command to shut down and power off the VM.

   ```
   [admin@ecnextx9 ~]$ sudo shutdown -h now
   ```

3. From the vSphere Web UI, right-click the VM and select **Power > Power Off**.
4. From the vSphere Web UI, right-click the EC from the previous release and select **Power > Power On**.
5. Depending on the previous system release, log onto the EC in one of the following manners.
   - **SR 8.0 system** — log in as admin user
   - **SR 7.x system** — log in an Administrative user
6. As **dncs** user, type the following commands and press **Enter** to start the EC processes:

   Note: If you are using a third-party application server, refer to the procedures for that server to start its processes.

   ```
   [dncs@ecnextx9 ~]$ dncsStart
   [dncs@ecnextx9 ~]$ appStart
   ```

7. Return to procedures at the beginning of this appendix to verify system functionality.

D

SR 9.0 Upgrade

This appendix provides the procedures to upgrade your system to a new version of SR 9.0.

In This Appendix

SR 9.0 Upgrade Prerequisites

The following prerequisites are required prior to performing a SR 9.0 upgrade.

- **Admin Node**
  - Refer to Appendix C in the ***Admin Node 2.0 Installation Guide*** for the procedure to upgrade the software repos.

    Important: The software repos ***must*** be updated before starting the EC upgrade.
- **EC System**
  - Refer to ***System Verification Procedures*** (on page 197) to verify that the active system is operating without any issues.
  - Refer to ***Post RepDB Verifications*** (on page 160) to execute a file sync and Replicated Database check.
  - Verify available disk space on the primary and secondary ESXi hosts for cloning the new VMs (for example, for a standard C240 installation, the EC requires 512 GB of disk space).
  - A temporary IP address is required if the *primary* and *secondary* VMs use the same IP address for ens192 (corporate network).
  - If your system is configured with a collapsed interface, you must add a route or an interface that can communicate with the Admin Node.

Preparing for the Upgrade

Complete the following steps on the EC to prepare the primary and secondary servers for the upgrade.

1. Stop all billing interfaces.
2. As **root** user, enter the following command to source the environment.

   ```
   [root@ecnextx9 ~]# . /dvs/dncs/bin/dncsSetup
   ```

3. Complete the following steps to disable RepDB on the *primary* and *secondary* servers.
   a. On the *primary* server, enter the following command to disable RepDB.

      ```
      [root@ecnextx9 ~]# /opt/cisco/repdb/RepDb -d
      ```

   b. When prompted to confirm the request, type **y**. Data replication is disabled.
   c. Type the following command to verify that data replication is disabled. The output should indicate that the database is **On-Line** and that Data Replication is **standard** with a state of **off**.

      ```
      [root@ecnextx9 ~]# onstat -g dri
      ```

   d. Repeat steps 3a through 3c on the *secondary* server.
4. Go to the next section.

Upgrading the Secondary VM

Cloning the Secondary VM

1. As **admin** user, enter the following command to shut down the *secondary* server.

   ```
   [admin@ecnextx9 ~]$ sudo shutdown -h now
   ```

2. From the vSphere Web UI, verify that the *secondary* VM powered off.
3. Right-click the *secondary* VM and select **Clone > Clone to Virtual Machine** to create a backup of the original VM. The Clone Existing Virtual Machine window appears.
4. In the **Enter a name for the virtual machine** text box, type a name to define the VM.

   Note: In this example, we will use ecnextx9_HOSTB_9.0-upgrade_20180814.
5. Select the datacenter where the cloned VM will be built. Then click **Next**. The Select a compute resource view opens.
6. Select the appropriate ESXi host where the VM is to be cloned. A compatibility check occurs.
7. Once the check succeeds, click **Next**. The Select storage window opens.
8. Ensure that the following settings exist and then click **Next**.
   - The "Select virtual disk format" field is set to **Same format as source**.
   - The correct datastore is selected.
9. Click **Next**. The Select clone options view opens.

   Note: You are not required to update any options in this window.
10. Click **Next**. The Customize vApp properties view opens.

    Note: Do not make any edits to this window as the **ifcfg-ens192** configuration file overwrites these values.
11. Click **Next**. Review the settings and then click **Finish**.
12. Monitor the **Recent Tasks** area to verify that the cloned VM completed successfully.
13. Do any network adapters share an IP address with the *primary* VM?
    - If **yes**, right-click the VM and select **Edit Settings**. Then ensure that the **Connected** and **Connect at Power On** boxes for each of these adapters ***are not*** selected. Click **OK** and go to the next step.
    - If **no**, go to the next step.
14. Right-click the cloned VM and select **Power > Power On**.
15. Right-click the cloned VM and select **Open Console**.
16. Login as **admin** user.

17 Will the primary and secondary hosts use the same IP address for ens192 (corporate network)?

- If **yes**, go to the next step.
- If **no**, and the ens192 IP addresses are unique, go to step 25.

18 Open the **/etc/sysconfig/network-scripts/ens192** file in a text editor.

```
[admin@ecnextx9 ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-ens192
```

19 Update the **IPADDR** entry with a temporary IP address.

Note: The temporary IP address allows access to the Admin Node and will be updated in a later procedure.

20 Save and close the file.

21 From the vSphere Web UI, right-click the VM and select **Edit Setting** and click the **Connected** and **Connect at Power On** boxes for network adapter 1.

22 Click **OK**.

23 From the Console window, type the following command to reboot the VM.

```
[admin@ecnextx9 ~]$ sudo shutdown -r now
```

24 Log back into the VM as **admin** user.

25 Enter the following commands to check the network connectivity and verify that you can ping the Admin Node.

```
[admin@ecnextx9 ~]$ ifconfig -a
[admin@ecnextx9 ~]$ ping [Admin Node IP]
```

Upgrading the Software on the New Secondary EC

1 As **dncs** user, type the following commands and press **Enter** (after each command) to kill the Initd processes.

```
[dncs@ecnextx9 ~]$ appKill
[dncs@ecnextx9 ~]$ dncsKill
```

2 As **admin** user, type the following command to see if the **CSCOec-lic** package is installed on the system.

```
[admin@ecnextx9 ~]$ rpm -qa | grep -i cscoec-lic
```

3 Is the **CSCOec-lic** package installed on the system?

- If **yes**, go to the next step.
- If **no**, go to step 5.

4 Enter the following command to remove the **cscoec-lic** package.

Command syntax:

```
rpm -e CSCOec-lic
```

Example:

```
[admin@ecnextx9 ~]$ sudo rpm -e CSCOec-lic
```

5 Type the following command to upgrade the EC software. A verification of the repos occurs and a check is done to verify which packages need upgraded.

```
[admin@ecnextx9 ~]$ sudo yum update
```

6 Once the packages are resolved and a list of the packages to upgrade is displayed, you are prompted to confirm the download of the packages.

7 Type **y** and press **Enter**. The update of the packages begins after it finishes, a **Complete!** message displays.

8 Did the yum update complete successfully?

- If **yes**, go to the next step.
- If **no**, go to step 12.

9 Enter the following command to verify the version of the **CSCOec-system-release** package. The version you upgraded to will display in the output.

```
[admin@ecnextx9 ~]$ rpm -qa | grep -i system-rel
```

10 Enter the following command to reboot the server.

```
[admin@ecnextx9 ~]$ sudo shutdown -r now
```

11 Log back into the EC as **admin** user.

12 Review the following log for any error messages.

```
[admin@ecnextx9 ~]$ sudo less /var/log/yum.log
```

13 Do any errors exist in the log?

- If **no**, go to the next section.
- If **yes**, go to the next step

14 If errors exist and you cannot determine the issue, execute one of the following options.

Important: If no errors are present, you have completed this procedure. Go to the next section in this appendix.

- Contact Cisco Services.
- Rollback the upgrade.

  Note: To rollback the upgrade, go to the next step.

15 Type the following command to shutdown the VM

```
[admin@ecnextx9 ~]$ sudo shutdown -h now
```

16 Monitor the **Recent Tasks** area to verify that the VM successfully powered off.

17 Right-click the original VM host and select **Power > Power On**.

18 Right-click the original VM and select **Power On**.

Shutting Down the Primary VM

1. As **dncs** user, enter the following commands to stop system processes on the *primary* EC.

```
[dncs@ecnextx9 ~]$ appStop
[dncs@ecnextx9 ~]$ dncsStop
[dncs@ecnextx9 ~]$ appKill
[dncs@ecnextx9 ~]$ dncsKill
```

2. As **admin** user, type the following command to shutdown the *primary* EC.

```
[admin@ecnextx9 ~]$ sudo shutdown -h now
```

3. Monitor the vSphere Web UI until the VM successfully shuts down.

Promoting the Upgraded Secondary VM to the New Primary VM

Complete the following procedure to update the ens192 IP address on the *new secondary* EC to promote it to the new, upgraded primary VM.

1. On the active *secondary* EC, enter the following command to create a backup of the **ifcfg-ens192** file.

```
[admin@ecnextx9 ~]$ sudo cp
/etc/sysconfig/network-scripts/ifcfg-ens192
/etc/sysconfig/network-scripts/orig.ifcfg-ens192
```

2. Open the **/etc/sysconfig/network-scripts/ifcfg-ens192** in a text editor and update the IP address to the required IP address for the *primary* EC.

```
[admin@ecnextx9 ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-ens192
```

3. Save and close the file.
4. Enter the following command to reboot the VM.

```
[admin@ecnextx9 ~]$ sudo shutdown -r now
```

5. While the system is rebooting, go to the vSphere Web UI, right-click this VM and select **Edit Settings**.
6. Click the **Connect** and **Connect at Power On** boxes for all network adapters.
7. Click **OK**.
8. Monitor the **Recent Tasks** area to confirm that the task completed successfully.
9. From a new terminal window, log into the VM using the IP address you defined in step 2.
10. Enter the following command to verify that the IP addresses are correct for each interface.

```
[admin@ecnextx9 ~]$ ifconfig –a
```

11 As **dncs** user, type the following commands to start system processes on the *active secondary* EC.

```
[dncs@ecnextx9 ~]$ dncsStart
[dncs@ecnextx9 ~]$ appStart
```

12 Type the following command to verify that system processes have started.

```
[dncs@ecnextx9 ~]$ pgrep -fl dvs
```

13 Log into the EC Web UI and verify that processes are coming up and eventually go green.

Note: This server is now the active *primary* EC.

14 Go to ***System Verification Procedures*** (on page 197) verify the functionality of your new *active* EC.

Note: If your EC is functioning properly, go to the next section to upgrade the original *primary* server.

Re-adding the IPG Collector cron Job

1 Does your system use an IPG Collector in which the collector has been successfully configured?

- If **yes**, go to step 2.
- If **no**, skip this procedure and go to the next section.

2 From the EC Web UI, click the **Navigation** icon () and then select **Server Applications > IPG**. The IPG Server List page opens.

3 Double-click the IPG Server, for example, IPG_eng (English) to view the IPG Collector.

4 Select the IPG collector and click **Edit**. The Edit IPG Collector page opens.

5 Click **Save**. A **Collector Updated Successfully** message appears and you are returned to the IPG Server List window.

Upgrading the Original Primary VM

Cloning the Original Primary VM

Note: This server has already been shutdown.

1. Right-click the *original primary* VM and select **Clone > Clone to Virtual Machine**. The Clone to Virtual Machine window appears.
2. In the **Enter a name for the virtual machine** text box, type a name to reflect the VM.

   Note: In this example, we will use ecnextx9_HOSTA_9.0-upgrade_20180424.
3. Select the datacenter where the cloned VM will be built. Then click **Next**. The Select a compute resource view opens.
4. Select the appropriate ESXi host where the VM is to be cloned. A compatibility check occurs.
5. Once the check succeeds, click **Next**.
6. Ensure that the following settings exist and then click **Next**.
   - The "Select virtual disk format" field is set to **Same format as source**.
   - The correct datastore is selected.
7. Click **Next**. The Select clone options view opens.

   Note: You are not required to update any options in this window.
8. Click **Next**. The Customize vApp properties view opens.

   Note: Do not make any edits to this window as the **ifcfg-ens192** configuration file overwrites these values.
9. Click **Next**. Review the settings and then click **Finish**.
10. Monitor the **Recent Tasks** area to verify that the cloned VM completed successfully.
11. From the vSphere Web UI, right-click the new, cloned VM and select **Edit Settings**.
12. Do any network adapters share an IP address with the new active VM in the system?
    - If **yes**, right-click the VM and select **Edit Settings**. Then ensure that the **Connected** and **Connect at Power On** boxes for each of these adapters ***is not*** selected. Click **OK** and go to the next step.

      Important: Ensure that the **Connected** and **Connect at Power On** boxes *are selected* for the RepDB network adapter.
    - If **no**, go to the next step.
13. Right-click the VM and select **Power > Power On**.

14 Right-click the VM again and select **Open Console**.

15 Login to the VM as **admin** user.

16 Will the primary and secondary hosts use the same IP address for ens192 (corporate network)?

- If **yes**, go to the next step.
- If **no**, and the ens192 IP addresses are unique, go to step 24.

17 Open the **/etc/sysconfig/network-scripts/ens192** file in a text editor.

```
[admin@ecnextx9 ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-ens192
```

18 Update the **IPADDR** entry with a temporary IP address.

Note: The temporary IP address allows access to the Admin Node and will be updated in a later procedure. You can use the same temporary IP address that you used in the earlier procedure.

19 Save and close the file.

20 From the vSphere Web UI, right-click the VM and select **Edit Settings**. Then click the **Connected** box for network adapter 1.

21 Click **OK**.

22 From the Console window, type the following command to reboot the VM.

```
[admin@ecnextx9 ~]$ sudo shutdown -r now
```

23 Log back into the VM as **admin** user.

24 Enter the following commands to check the network connectivity and to verify that you can ping the Admin Node.

Note: Substitute the IP address of the Admin Node for [Admin_Node_IP]. Do not include the brackets.

```
[admin@ecnextx9 ~]$ ifconfig -a
[admin@ecnextx9 ~]$ ping [Admin_Node_IP]
```

Upgrading the Software on the New VM

Note: This will become the new *secondary* EC in the system you are upgrading.

1 From the vSphere Web UI, right-click the VM and select **Open Console**.

2 As **dncs** user, enter the following commands to kill the **Initd** processes.

```
[dncs@ecnextx9 ~]$ appKill
[dncs@ecnextx9 ~]$ dncsKill
```

3 As **admin** user, type the following command to see if the **CSCOec-lic** package is installed on the system.

```
[admin@ecnextx9 ~]$ rpm -qa | grep -i cscoec-lic
```

4 Is the **CSCOec-lic** package installed on your system?

- If **yes**, go to the next step.
- If **no**, go to step 6.

5 Enter the following command to remove the **cscoec-lic** package.

Command syntax:

```
sudo rpm -e CSCOec-lic
```

Example:

```
[admin@ecnextx9 ~]$ sudo rpm -e CSCOec-lic
```

6 Type the following command to upgrade the EC software. A verification of the repos occurs and a check is done to verify which packages need upgraded.

```
[admin@ecnextx9 ~]$ sudo yum update
```

7 Once the packages are resolved and a list of the packages to upgrade is displayed, you are prompted to confirm the downloading of the packages.

8 Enter **y** and press **Enter**. The update of the packages begins and after it finishes, a **Complete!** message displays.

9 Did the yum update complete successfully?

- If **yes**, go to the next step.
- If **no**, go to step 13.

10 Enter the following command to verify the version of the **CSCOec-system-release** package. The software version is displayed in the output.

```
[admin@ecnextx9 ~]$ rpm -qa | grep -i system-rel
```

11 Enter the following command to reboot the server.

```
[admin@ecnextx9 ~]$ sudo shutdown -r now
```

12 Log back into the VM as **admin** user.

13 Review the following log for any error messages.

```
[admin@ecnextx9 ~]$ sudo less /var/log/yum.log
```

14 Are any errors present in the log?

- If **no**, go to the next section.
- If **yes**, go to the next step

15 If errors exist and you cannot determine the issue, execute one of the following options.

Important: If no errors are present, you have completed this procedure. Go to ***Configuring the VM as the New Secondary System*** (on page 216).

- Contact Cisco Services.
- Rollback the upgrade.

  Note: To rollback the upgrade, go to the next step.

16 Type the following command to shutdown the VM

```
[admin@ecnextx9 ~]$ sudo shutdown -h now
```

17 From the vSphere Web UI, right-click the VM and select **Power > Power Off**.

18 Monitor the **Recent Tasks** area to verify that the VM successfully powered off.

19 Right-click the original VM and select **Power > Power On**.

Configuring the VM as the New Secondary System

Complete the following procedure to configure this VM as the new *secondary* EC.

1 From the Console window, enter the following command to create a backup of the **ifcfg-ens192** file.

```
[admin@ecnextx9 ~]$ sudo cp
/etc/sysconfig/network-scripts/ifcfg-ens192
/etc/sysconfig/network-scripts/orig.ifcfg-ens192
```

2 Open the **/etc/sysconfig/network-scripts/ifcfg-ens192** in a text editor and update the IP address.

```
[admin@ecnextx9 ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-ens192
```

3 Save and close the file.

4 Is the ens192 IP address the same for the *primary* and the *secondary* EC?

- If **yes**, go to the next step.
- If **no** and they are unique IP addresses, go to step 13.

5 Enter the following command to reboot the VM.

```
[admin@ecnextx9 ~]$ sudo shutdown -r now
```

6 While the system is rebooting, go to the vSphere Web UI, right-click the *new secondary* VM and select **Edit Settings**.

7 Unselect the **Connect** and **Connect at Power On** boxes for ethernet adapter 1.

Note: Only the RepDB network adapter **Connect** and **Connect at Power On** boxes should be selected.

8 Click **OK**.

9 Monitor the **Recent Tasks** area to confirm that the task successfully completes.

10 Right-click the VM and select **Open Console**.

11 When prompted, log back into the VM as **admin** user.

12 Enter the following command to verify that the IP addresses are correct for each interface and that the RepDB interface it the only interface that shows **Running**.

```
[admin@ecnextx9 ~]$ ifconfig -a
```

13 Enter the following command to ping the *primary* VM.

```
[admin@ecnextx9 ~]$ ping HOSTB
```

Enabling RepDB on the Upgraded System

To enable RepDB on the upgraded system, refer to ***Enabling RepDB*** (on page 158).

E

EC SR 9.0 Patch Installs

This section describes the procedures to install a patch to the primary and secondary ECs in your NextX system.

The format for an EC patch is: **CSCOec-patch-[VERSION].[DATE].[PLATFORM].rpm**

The version for the first CSCOec-patch package is always "-2" (e.g., CSCOec-patch-9.0.4-**2**.[VERSION].[DATE].[PLATFORM].rpm). The version for any future patches is numbered sequentially (e.g., CSCOec-patch-9.0.4-**3**.[VERSION].[DATE].[PLATFORM].rpm).

In addition, each new patch is a cumulative patch, as it will include all patches previous to the current package version.

In This Appendix

Preparing for a Patch Upgrade

Complete the following steps prior to executing the patch upgrade.

1 From a Web browser, enter the following command to verify that the patch has been deployed on the Admin Node that is associated with your system.

URL syntax:

```
https://[Admin_Node_IP]/repos/nextx/9.0/
```

Example:

```
https://10.90.181.139/repos/nextx/9.0/
```

2 Is the **CSCOec-patch** RPM present?

- If **yes**, go to the next section.
- If **no**, refer to the **Updating the Application Packages Repo** section in the ***Admin Node 2.0 Installation Guide*** to update the NextX repo with the patch software.

Installing an EC Patch

A patch install to your primary and secondary servers requires you to disable and deactivate Replicated Database prior to the installation. This is because upgraded database transactions on the primary server should not flow to the secondary server until it has been patched as well.

Complete the following procedure to install a patch to your system.

1. As **admin** user, enter the following command to disable RepDB on *the* primary server.

   ```
   [dncs@ecnextx9 ~]$ sudo /opt/cisco/repdb/RepDb -d
   ```

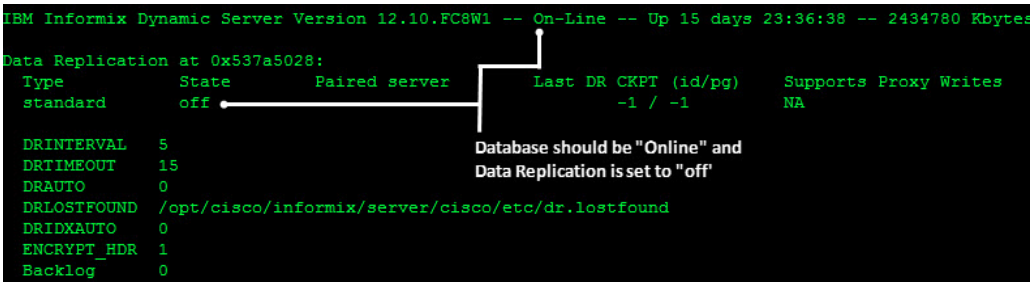
2. Enter the following command to deactivate RepDB on *the* primary server.

   ```
   [dncs@ecnextx9 ~]$ sudo /opt/cisco/repdb/RepDb -D
   ```

3. Repeat steps 1 through 2 on the *secondary* server.

4. As **root** user, enter the following command on both the *primary* and *secondary* servers to verify that RepDB is disabled.

   ```
   [root@ecnextx9 ~]# onstat -g dri
   ```



5. As **dncs** user on the *primary* server, enter the following commands to stop processes.

   ```
   [dncs@ecnextx9 ~]$ appStop
   [dncs@ecnextx9 ~]$ dncsStop
   [dncs@ecnextx9 ~]$ appKill
   [dncs@ecnextx9 ~]$ dncsKill
   ```

6. Enter the following command to verify if a **CSCOec-patch** package is currently installed on the EC?

   ```
   [dncs@ecnextx9 ~]$ rpm -qa | grep -i CSCOec-patch
   ```

7 Does a **CSCOec-patch** package exist on the system?

- If **no**, enter the following command. The script sets up the install process and verifies dependencies; and then displays an **Is this ok [y/N]** message.

  Note: If this is the first time you are installing an EC patch, enter the full package name in the installation command.

  Command syntax:

  ```
  sudo yum install CSCOec-patch-[VERSION].[DATE].[PLATFORM]
  ```

  Example:

  ```
  [admin@ecnextx9 ~]$ sudo yum install
  CSCOec-patch-9.0.4-2.201803141548.e16.x86_64
  ```

- If **yes** and you are installing a newer CSCOec-patch, enter the following command. The script sets up the install process and verifies dependencies; and then displays an **Is this ok [y/N]** message.

  Note: If a previous patch is present, enter only the patch name with an asterisk (*). The asterisk is a wildcard and installs the most current version of the EC patch that is in the NextX repo.

  ```
  [admin@ecnextx9 ~]$ sudo yum update CSCOec-patch*
  ```

8 Type **y** and press **Enter**. The installation continues and when finished, a **Complete!** message displays.

Note: The output from this particular patch install indicates that the CSCOec-patch and the CSCOecutils packages were downloaded and installed. Subsequent patch installs will contain different RPMs as required.

9 Enter the following command to verify that the **CSCOec-patch** package successfully installed, as well as any other packages.

Command syntax:

```
rpm –qa | egrep "[package_name_1] | [package_name_2]
[package_name_n]"
```

Example:

```
[admin@ecnextx9 ~]$ rpm -qa | egrep -i "CSCOec-patch|ecutils"
```

```
CSCOecutils-8.1.2-1.201801161613.el7.centos.x86_64
CSCOec-patch-9.0.4-2.201803141548.e16.x86_64
```

10 Enter the following command to query the patch package and view the release date, the version, other installed packages, and the issues corrected in the patch.

Command syntax:

```
rpm -q --changelog CSCOec-patch-[VERSION].[DATE].[PLATFORM]
```

Example:

```
[admin@ecnextx9 ~]$ rpm -q --changelog
CSCOec-patch-9.0.4-2.201803141548.e16.x86_64
```

```
* Tue Mar 14 2018 - 9.0.4-2
CSCOecutils-8.1.2-1.rpm

- CSCv16242 cvtChecker script fails to execute
- CSCvf16318 Utility script version should be correct and uniform
```

11 Enter the following command to reboot the server.

```
[admin@ecnextx9 ~]$ sudo shutdown –r now
```

12 Log back into the server and, as **dncs** user, enter the following commands to start processes.

```
[dncs@ecnextx9 ~]$ dncsStart
[dncs@ecnextx9 ~]$ appStart
```

13 Verify server functionality.

14 Is your server functioning properly?

- If **yes**, and you successfully installed the patch on the *primary* EC, go to the next step.
- If **yes** and you successfully installed the patch on the *primary* and the *secondary* EC servers, go to step 16.
- If **no**, troubleshoot the system. If you cannot remedy the issue, contact Cisco Services.

  Note: You can also choose to uninstall the patch. Refer to the next section for details.

15 Repeat steps 6 through 14 on the *secondary* system.

16 Refer to ***Enabling RepDB*** (on page 158) to re-enable replicated database on your system.

Uninstalling an EC Patch

Complete the following steps to uninstall an EC patch. This procedure also downgrades any packages that were installed/upgraded as dependencies to the patch installation.

Note: Replicated Database should still be disabled.

1. As **dncs** user on the *primary* server, enter the following commands to stop processes.

   ```
   [dncs@ecnextx9 ~]$ appStop
   [dncs@ecnextx9 ~]$ dncsStop
   [dncs@ecnextx9 ~]$ appKill
   [dncs@ecnextx9 ~]$ dncsKill
   ```

2. Enter the following command to verify the current version of the **CSCOec-patch**.

   ```
   [dncs@ecnextx9 ~]$ rpm -qa | grep -i CSCOec-patch
   ```

3. As **admin** user, enter the following command to obtain the **ID** of the CSCOec-patch installation.

   ```
   [admin@ecnextx9 ~]$ sudo yum history package-list
   CSCOec-patch\*
   ```

4. From the **ID** column, record the ID number for the CSCOec-patch installation.

   ID Number _____

5. Enter the following command to uninstall/downgrade the patch using the ID number you recorded in the previous step. An **Is this ok [y/N]** message displays.

   Command syntax:

   ```
   sudo yum history undo [ID_number]
   ```

   Example:

   ```
   [admin@ecnextx9 ~]$ sudo yum history undo 68
   ```

6. Type **y** and press **Enter**. The downgrade proceeds, and when finished, a **Complete!** message displays.

   Note: In this example, the script deletes the CSCOec-patch and downgrades the CSCOecutils package. When you execute this script for subsequent patch installs, it deletes and/or removes different RPMs as required.

7 Enter the following command to verify the current versions of the patches and any other packages that were downgraded.

Note: If this was the first time a CSCOec-patch was installed, no output is displayed for this package.

Command syntax:

```
rpm –qa | egrep "[package_name_1] | [package_name_2] [package_name_n]"
```

Example:

```
[admin@ecnextx9 ~]$ rpm -qa | egrep -i "CSCOec-patch | ecutils"
```

8 Enter the following command to reboot the server.

```
[admin@ecnextx9 ~]$ sudo shutdown –r now
```

9 Log back into the server and, as **dncs** user, enter the following command to start processes.

```
[dncs@ecnextx9 ~]$ dncsStart
[dncs@ecnextx9 ~]$ appStart
```

10 Verify EC functionality.

11 Is your EC functioning properly?

- If **yes**, go to the next step.
- If **no**, refer to the ***Backup and Restore User Guide for EC 9.0 and DTACS 5.2*** to restore your system.

12 Refer to ***Enabling RepDB*** (on page 158) to re-enable replicated database on your system.

F

Setting Up the Network Time Protocol on Servers and Clients

Introduction

The instructions in this appendix describe how to set up the Network Time Protocol (NTP) on servers and clients.

In This Appendix

Configure NTP on the Server

By default, the EC is configured to use the internal clock for timing. Follow these instructions to configure the EC to obtain timing from an external NTP server.

Note: Obtain the primary and any secondary NTP source IP addresses from the system operator.

1. As **admin** user, enter the following command to edit the **/etc/ntp.conf** file in a text editor.

   ```
   [admin@ecnextx9 ~]$ sudo vi /etc/ntp.conf
   ```

2. Go to the end of the file and enter the IPs for your NTP servers in the following format.

   Syntax:

   ```
   server [NTP IP 1] iburst
   server [NTP IP 2] iburst
   ```

   Example:

   ```
   server 10.90.44.40 iburst
   server 10.90.44.41 iburst
   ```

3. Press **Enter** twice and then enter the following:

   ```
   # Driftfile.
   driftfile /var/lib/ntp/drift
   ```

4. Save and close the **ntp.conf** file.
5. Type the following command and press **Enter**.

   ```
   [admin@ecnextx9 ~]$ systemctl status ntpd
   ```

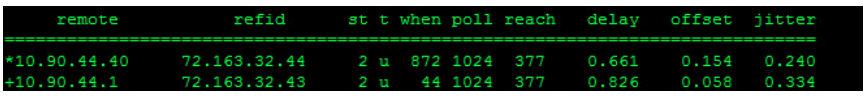
6. Did the output from step 5 show ntpd running?
   - If **yes**, continue with the next step.
   - If **no**, type the following command and press **Enter**. Then, go to the next step.

     ```
     [admin@ecnextx9 ~]$ sudo systemctl start ntpd
     ```

7. Type the following command and press **Enter** to check the status of the NTP.

   ```
   [admin@ecnextx9 ~]$ sudo ntpq -p
   ```

   Result: You should see output similar to the following:



```
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.90.44.40     72.163.32.44     2 u  872 1024  377    0.661    0.154   0.240
+10.90.44.1      72.163.32.43     2 u   44 1024  377    0.826    0.058   0.334
```

Configure NTP on the Client

Follow these instructions to configure NTP on the new client.

Note: A "client" can be any device that uses the EC server to configure its time.

1. If necessary, open a remote terminal window on the client.
2. As **admin** user, type the following command and press **Enter** to initialize the /etc/ntp.conf file as a client:

   ```
   [admin@client ~]$ sudo /dvs/platform/libexec/install_ntp -c
   ```

   Note: The default settings for the client ntp.conf file use the host "dncs_host" as the time server. If you want to change this setting, use a text editor to edit the ntp.conf file.
3. Type the following command and press **Enter** to restart the NTP service:

   ```
   [admin@client ~]$ sudo systemctl restart ntpd
   ```
4. Type the following command and press **Enter** to check the status of the NTP service:

   ```
   ntpq
   ```

   Example output: You should see output similar to the following:

   ```
   remote    refid         st t when poll reach delay offset    disp
   ==============================================================
   *ISDS     198.51.100.44  4 u   39   64    7  0.30  -9.535 1939.02
   LOCAL(0)  LOCAL(0)       5 l   41   64    7  0.00   0.000 1937.99
   ```

   Note: It takes the NTP daemon a few minutes to decide which server will be the primary server after the ntp server is restarted. An asterisk appears next to the source that is being referenced.

G

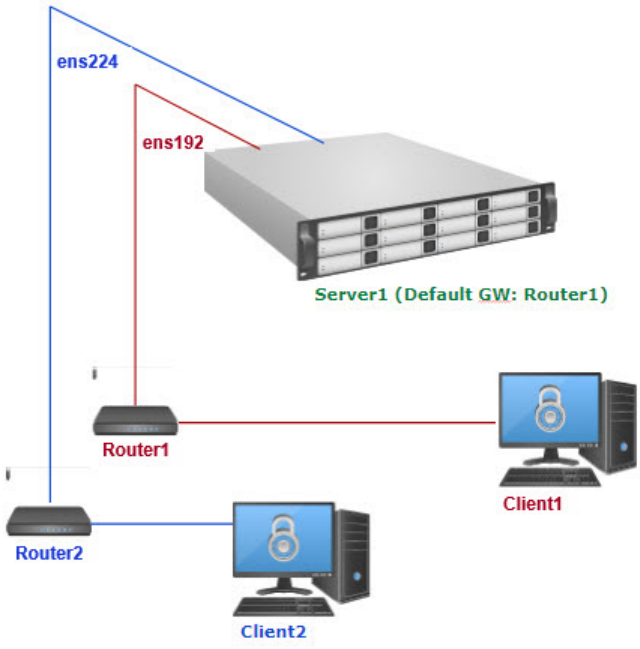
Configure Multiple Interfaces in a CentOS Environment

The instructions in this appendix describe how to configure multiple network interfaces in a CentOS environment.

In This Appendix

Background

RedHat distributions, including CentOS, do not allow multi-homed (multiple interfaces) servers to reply through a different interface from where the request came in. The following illustration demonstrates this issue:



- Client1 attempts to reach ens192.
- Server1 receives the request via ens192.
- Server1 tries to respong back using Router2 (default GW) but fails as Router2 is only accessible via a different interface from where the request originated (ens192).

Solution to this Issue

The solution to this issue relies on having two default gateways, one per interface. Refer to the next section for an example to configure two default gateways and two unique routing tables for the ens192 and ens224 network interface in your system.

Configuring Multiple Interfaces in CentOS

Complete the following procedure to configure multiple interfaces in your environment

Notes:

- Multiple default gateways work only for incoming traffic. Traffic initiated by the server still relies on its global default gateway and static routes.
- The following example includes two interfaces, ens192 and ens224, and two routing tables, one for ens192, and one for ens224.

  Example: Network Interface Configuration

  Important: Make sure to substitute the values for your system for the ens192 and ens224 interfaces, as well as for the global default gateway.

  Example routing table:

	IP Address/Mask Bits	Gateway
ens192	10.90.167.208/24	10.90.167.1
ens224	10.253.6.2/24	10.253.6.254
Global Default Gateway	N/A	10.253.6.254

1. As **admin** user, enter the following command to open the **/etc/sysconfig/network** file in a text editor.

   ```
   [admin@ecnextx9 ~]$ sudo vi /etc/sysconfig/network
   ```

2. Is the value for the **GATEWAY** field set to the global default gateway?

   - If **no**, update the value to the default global gateway. Then save and close the file.

     Example input:

     ```
     NETWORKING=yes
     NOZEROCONF=yes
     RES_OPTIONS="rotate timeout:1 attempts:1"
     GATEWAY=10.253.6.254            #Global default gateway
     ```

- If **yes**, close the file.

3 Enter the following command to configure the routes for the **ens192** interface (for example, from the previous table).

```
[admin@ecnextx9 ~]$ sudo vi
/etc/sysconfig/network-scripts/route-ens192
```

Note: In this example, the static route, 10.82.0.0.16 is used for traffic initiated from the server.

Example input:

```
10.82.0.0/16 via 10.90.167.1  #(Optional) Specific unicast
static route for table 1
10.90.167.0/24 dev ens192 table 1
default via 10.90.167.1 dev ens192 table 1
```

4 Save and close the file.

5 Enter the following command to configure the routes for the **ens224** interface.

```
[admin@ecnextx9 ~]$ sudo vi
/etc/sysconfig/network-scripts/route-ens224
```

Example input:

```
224.0.0.0/4 dev ens224  #(Optional) Specific multicast static
route for table 2
10.90.47.0/24 dev ens192  #(Optional) Specific unicast static
route for table 2
10.253.6.0/24 dev ens224 table 2
default via 10.253.6.254 dev ens224 table 2
default via 10.253.6.254 dev ens224 table 254 #Traffic
initiated from the node
```

6 Save and close the file.

7 Enter the following command to create a rules file for the **ens192** interface.

```
[admin@ecnextx9 ~]$ sudo vi
/etc/sysconfig/network-scripts/rule-ens192
```

Example input:

```
iif ens192 table 1
from 10.90.167.208 table 1
```

8 Save and close the file.

9 Enter the following command to create a rules file for the **ens224** interface.

```
[admin@ecnextx9 ~]$ sudo vi
/etc/sysconfig/network-scripts/rule-ens224
```

Example input:

```
iif ens224 table 2
from 10.253.6.2 table 2
```

10 Save and close the file.

11 Enter the following command to reboot the server.

```
[admin@ecnextx9 ~]$ sudo shutdown –r now
```

12 When the server boots up, login as **admin** user.

Testing the Setup of the Network Interfaces

Complete the following procedure to test the setup of the network interfaces.

1 As **admin** user, enter the following command to check the rules defined for your network.

```
[admin@ecnextx9 ~]$ ip rule
```

Example output:

```
0:      from all lookup local
32762:  from 10.253.6.2 lookup 2
32763:  from all iif ens224 lookup 2
32764:  from 10.90.167.208 lookup 1
32765:  from all iif ens192 lookup 1
32766:  from all lookup main
32767:  from all lookup default
```

2 Enter the following commands to verify the routing tables defined for your network.

```
[admin@ecnextx9 ~]$ ip route show table 1
```

Example output:

```
10.90.167.0/24 dev ens192 scope link
default via 10.90.167.1 dev ens192
```

```
[admin@ecnextx9 ~]$ ip route show table 2
```

Example output:

```
10.253.6.0/24 dev ens224 scope link
default via 10.253.6.254 dev ens224
```

```
[admin@ecnextx9 ~]$ ip route show table 254
```

Note: The routing table 254 is the default routing table.

Example output:

```
10.253.6.0/24 dev ens224 proto kernel scope link src 10.253.6.2
10.90.167.0/24 dev ens192 proto kernel scope link src 10.90.167.208
default via 10.253.6.254 dev ens
```

3 Were the rules and routing tables set up correctly?

- If **yes**, you have completed this procedure.
- If **no**, refer to the previous section to make sure your network is configured correctly.

H

Stop System Processes and Kill Active Sessions

This section includes procedures to stop EC system processes and to kill any active sessions.

In This Appendix

Stopping System Processes

Complete the following steps to stop system processes on the EC.

1. As **dncs** user, enter the following command to see if system processes and/or Initd is running.

   ```
   [dncs@ecnextx9 ~]$ pgrep -fl dvs
   ```

2. Are any processes running?
   - If **yes**, go to the next step.
   - If **no**, go to the next section.
3. Are you using the Cisco application server?
   - If **yes**, go to the next step.
   - If **no**, refer to the documentation for your application server to stop processes. Then go to step 5.
4. Type the following commands to stop the application server processes.

   ```
   [dncs@ecnextx9 ~]$ appStop
   [dncs@ecnextx9 ~]$ appKill
   ```

5. Type the following commands to stop the EC processes.

   ```
   [dncs@ecnextx9 ~]$ dncsStop
   [dncs@ecnextx9 ~]$ dncsKill
   ```

6. Repeat step 1 to verify that all processes and Initd are no longer running.
7. Are processes or Initd still running?
   - If **yes**, kill each process using the following command syntax.

     ```
     pkill -9 [PID]
     ```

   - If **no**, go to the next procedure.

Killing Active Sessions

1. Enter the following command to ensure that there are no active sessions.

   ```
   [dncs@ecnextx9 ~]$ showActiveSessions
   ```

2. Do any active sessions exist?

   - If **yes**, go to the next step.
   - If **no**, you have completed this procedure.

3. As **root** user, source your environment.

   ```
   [root@ecnextx9 ~]# . /dvs/dncs/bin/dncsSetup
   ```

4. Enter the following command to kill all active sessions.

   ```
   [root@ecnextx9 ~]% killActiveSessions
   ```

5. Repeat step 1 to ensure there are no longer any active sessions.

I

Increase the Size of Hard Disk 2

Use the procedure in this appendix to increase the size of Hard disk 2 in the event that your system deployment is running out of disk space under /disk1.

Important: This procedure must be performed during a maintenance window because the VM must be shutdown in order to modify the hard disk size.

In This Appendix

Increasing the Size of Hard Disk 2

1. As **dncs** user, enter the following commands to stop system processes.

```
[dncs@ecnextx9 ~]$ appStop
[dncs@ecnextx9 ~]$ dncsStop
[dncs@ecnextx9 ~]$ appKill
[dncs@ecnextx9 ~]$ dncsKill
```

2. As **root** user, source the environment variable.

```
[root@ecnextx9 ~]# . /dvs/dncs/bin/dncsSetup
```

3. Enter the following command to kill all active sessions.

```
[root@ecnextx9 ~]# killActiveSessions
```

4. Enter the following command to shutdown the VM.

```
[root@ecnextx9 ~]# shutdown -h now
```

5. From vSphere, verify that the VM is powered off.
6. From the vSphere Web UI, select the VM and click **Edit Settings**. The Edit Settings window opens.
7. From the **Hard disk 2** entry, update the size accordingly.

   Important: If there are snapshots, then the Hard Disk Provisioned Size field will be grayed out. The snapshot(s) must be removed to allow a HDD size modification.
8. Click **OK**.
9. Monitor the **Recent Tasks** area to ensure the task completed successfully.
10. Right-click the VM and select **Power > Power On**.
11. From a terminal window, log on to the EC as **admin** user.
12. As **admin** user, complete the following steps to increase the size of **/disk1** in the operating system.
    a. Enter the following command to check the new disk size.

```
[admin@ecnextx9 ~]$ sudo lsblk -nr
```

    Example output:

```
fd0 2:0 1 4K 0 disk
sda 8:0 0 64G 0 disk
sda1 8:1 0 64G 0 part /
sdb 8:16 0 400G 0 disk
sdb1 8:17 0 384G 0 part
disk1-disk1 253:0 0 384G 0 lvm /disk1
sr0 11:0 1 1024M 0 rom
```

    b. Enter the following command to extend the **/dev/sdb** partition in the partition table.

```
[admin@ecnextx9 ~]$ sudo growpart /dev/sdb 1
```

c Enter the following command to resize the physical volume of the **/dev/sdb1** partition.

```
[admin@ecnextx9 ~]$ sudo pvresize /dev/sdb1
```

d Enter the following command to add space to the logical volume for /disk1.

```
[admin@ecnextx9 ~]$ sudo lvextend –l +100%FREE
/dev/disk1/disk1
```

e Enter the following command to expand the existing XFS filesystem for /disk1.

```
[admin@ecnextx9 ~]$ sudo xfs_growfs /dev/mapper/disk1-disk1
```

f Enter the following command to verify the increase in size of /disk1.

```
[admin@ecnextx9 ~]$ df –h
```

g As **dncs** user, enter the following commands to restart system processes.

```
[dncs@ecnextx9 ~]$ dncsStart
[dncs@ecnextx9 ~]$ appStart
```

J

Reset the Password for the admin User

This appendix provides the procedure to change the password for the admin user in the event the password is lost, forgotten or expired.

In This Appendix

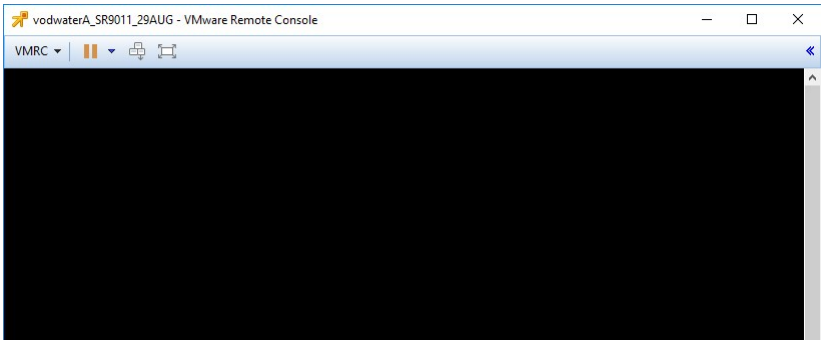
Resetting the Password for the admin User

Complete the following procedure to reset the password for the admin user.

Note: This procedure is written using the vSphere 6.0 Web UI. If you are using a different version or if you are using a vSphere client, the steps may differ.

1. From a Web browser, log into the vSphere 6.0 Web UI.
2. Select the VM in which the admin password needs reset.
3. From the right section of the window, click the **Summary** tab.
4. Click the **Launch Remote Console** link. The VMware Remote Console window opens for the VM opens in a new window.

   Important: If you have not yet downloaded the Remote Console, click the **Download Remote Console** link in the Summary window. Follow the prompts to install the remote console. Then click **Launch Remote Console**.

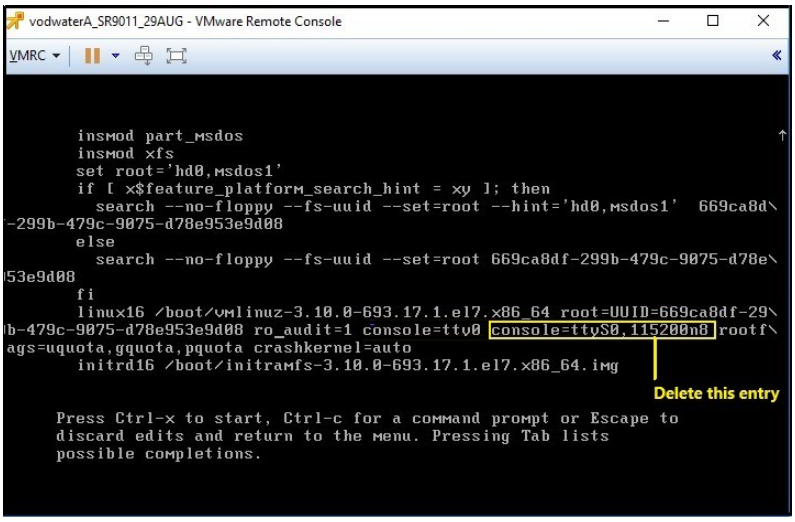


5. Select **VMRC > Ctrl+Alt+Del** to reboot the VM.
6. Use your arrow keys to select the appropriate boot entry from the Grub menu and then press **e** to edit the entry.

   Note: In most cases, the first entry is the appropriate entry; therefore, you can simply enter **e** to edit the entry.

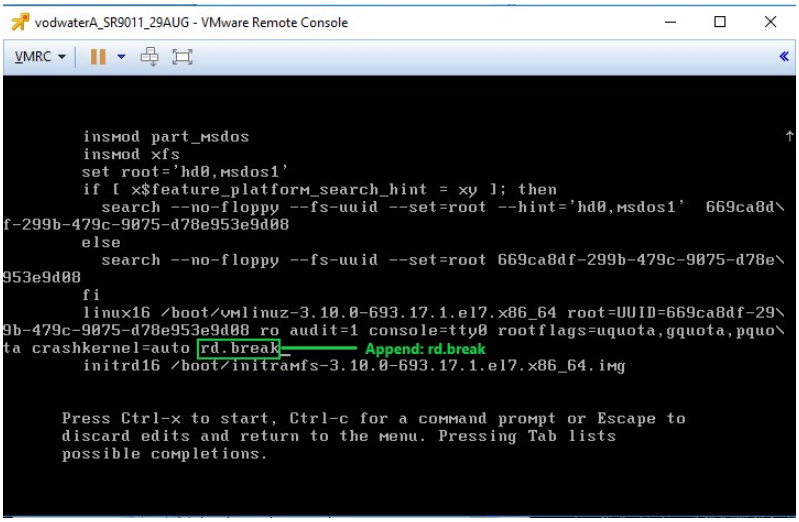
7 Use your down arrow key to move to the **linux16** line and delete the following text.

```
console=ttypsS0,115200n8
```



8 Move to the end of this line and add the following text.

```
rd.break
```



9 Press **Ctrl+x** to resume the boot process of the VM. The system boots to the bash prompt.

Note: The modifications that were made are only temporary and will not be saved.

10 At the prompt, type the following command and press **Enter** to mount the root file system with read/write access.

```
switch_root:/# mount -o remount,rw /sysroot
```

11 At the prompt, type the following command and press **Enter**.

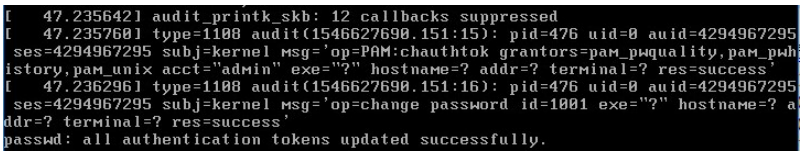
```
switch_root:/# chroot /sysroot
```

12 Enter the following command to change the password for the **admin** user.

```
sh-4.2# passwd admin
```

13 When prompted, enter the new password for the **admin** user and then press **Enter**.

14 When prompted to retype the password, re-enter the new password and then press **Enter**. The output should resemble the following:



15 At the prompt, enter the following command and press **Enter**.

```
sh-4.2# touch /.autorelabel
```

16 At the prompt, type **exit** and press **Enter**.

```
sh-4.2# exit
```

17 At the prompt, type **exit** again and press **Enter**. The boot process is resumed on the VM.

18 As **admin** user, login with your new password.

Index

E

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

http://www.cisco.com
Tel: 408 526-4000
800 553-6387
Fax: 408 527-0883

April 2019