DTACS 5.0 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 vii

Chapter 1 Planning the Install or Migration 1

Site Requirements....2
Estimated Timeline....7
Determine Which Optional Features to Enable....8

Chapter 2 Deploy the DTACS Virtual Machine 9

Deploying the VM From the Linux Platform Template....10
Reconfiguring the Virtual Hardware Settings on the VM....12
Setting the Power Policy....13

Chapter 3 Preparing the System for the Installation or Migration 15

Shutdown the Secondary SR 4.1 DTACS VM....16
Power on the New DTACS VM....17
Set Up the Network With a Static IP Configuration (Optional)....19

Chapter 4 DTACS 5.0 Installation 23

Copying the VCS Deployment Zip File to the VM....24
Installing DTACS 5.0....25
Transfer HTTPS X.509 Certificates to the DTACS Server....27

Chapter 5 Migrate DTACS 4.1 to DTACS 5.0 35

Creating an Admin User on the DTACS 4.1 Server....36
Migrating Key Files and Database to DTACS 5.0....37
Updating the DTACS Configuration....42

Chapter 6 Post Upgrade Procedures 43

Creating User Accounts 44
Updating the site_info Database Table for a Hostname Change 49
Configuring the DTACS Server for the EC 52
Configuring the EC for DTACS 54
Testing Synchronization Between the DTACS and EC Databases 56
Setting Up SFTP Support 57
Configuring DTACS BOSS Proxy (Optional) 61
Restarting Apache and Tomcat Services 62
CentOS cron and anacrontab Overview 63
Verifying the crontab Entries Managed by cron 65
Verifying User-Defined CRON Entries on the Migrated VM 66
Starting DTACS Processes 67
Testing dbsync from the DTACS Web UI 68
Enabling RADIUS and LDAP (Optional) 69
SCID Sharing Support Feature (Optional) 70

Chapter 7 Configure and Operate the Replicated Database 71

Prerequisites for RepDB 72
Overview of the Replicated Database Package 73
Setup Replicated Database 75
Configure RepDB 80
Post RepDB Verifications 90

Appendix A Hardware Configuration Procedures for the Cisco UCS C240 93

Hardware Diagram of the Cisco UCS C240 M3 Server 94
Hardware Diagram of the Cisco UCS C240 M4 Server 97
Hardware Requirements for a New UCS Install 100
Cisco UCS C240 Server CIMC Configuration 101
Cisco UCS C240 Host Configuration 102
RAID Configuration 103
ESXi Installation 113
Configure the VM Host 119

Appendix B Procedures When Using an ESXi Client 123

Deploy and Configure a VM Using an ESXi Client 124
Modifying the Device Status for an Ethernet Adapter 126
Setting Up RepDB Using an ESXi Client 127

Appendix C SR 5.0 Rollback Procedures 129

Activate the Old System Release 130

Appendix D DTACS SR 5.0 Upgrade 131

DTACS SR 5.0 Upgrade Prerequisites 132
Preparing for the Upgrade 133
Upgrading the Secondary VM 134
Cloning the Primary VM 138
Enabling RepDB on the Upgraded System 142

Appendix E DTACS 5.0 Patch Installs 143

Preparing for a Patch Install 144
Installing a DTACS Patch 145
Uninstalling a DTACS Patch 148

Appendix F Configure Multiple Interfaces in a CentOS Environment 151

Background 152
Solution to this Issue 153

Index 157

About This Guide

Introduction

This guide provides step-by-step instructions for the installation and migration of a Digital Transport Adaptor Control System (DTACS) to System Release (SR) 5.0.

The DTACS application manages and controls Digital Transport Adaptors (DTAs). DTAs are hardware components used in the Digital Broadband Delivery System (DBDS) network to convert digital channels into analog services.

The DTACS application, combined with DTAs, allow Multiple System Operators (MSOs) to support customers who use standard definition televisions to access cable services.

This guide provides step-by-step instructions for the following DTACS 5.0 installation scenarios.

- Initial installation of System Release (SR) 5.0
- Migration of 4.1 to SR 5.0
- Upgrade to a newer version of SR 5.0

SR 5.0 Features Forklift Upgrade

The upgrade to DTACS 5.0 involves migration from Sun Microsystems (Sun) SPARC servers to Cisco's Unified Computing System (UCS). The DTACS 5.0 upgrade allows engineers to upgrade the system without having to shut the system down until the activation of the new system software.

How Long to Complete the Upgrade?

The upgrade to DTACS 5.0 is to be completed within a maintenance window that usually begins at midnight. Upgrade engineers have determined that a typical site can be upgraded within one 6-hour maintenance window. The maintenance window should begin when you stop the system components as described in ***Migrating the Database and Key Files*** (on page 40).

Audience

This guide is written for field service engineers and system operators who are responsible for creating virtual machines (VMs) and installing or upgrading to SR 5.0.

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 DTACS software need the following skills:

- Advanced knowledge of Linux
  - Experience with the Linux vi editor. Several times throughout the system upgrade process, system files are edited using the Linux vi editor. The Linux vi editor is not intuitive. The instructions provided in this guide are no substitute for an advanced working knowledge of vi.
- Knowledge of VMware
- A thorough understanding of the DBDS system

Document Version

This is the first formal release of this document.

Revision History

Date	Revision	Section
20180228	Add Appendix F to provide the procedures to configure multiple network interfaces. This is required for systems using a multi-home environment on a CentOS platform.	Configure Multiple Interfaces in a CentOS Environment
	Added SFTP Support section.	***Setting Up SFTP Support*** (on page 57)
20180306	Deleted section to create a user for use with an AGI Adapter.	N/A
	Added a note to Setting Up SFTP Support that the SFTP user you create can be used with an AGI Adapter.	***Setting Up SFTP Support*** (on page 57)

Date	Revision	Section
20180321	Added section in Chapter 6 to ensure GQAM code if version 4.7.0 if enabling SCID Sharing feature support.	***SCID Sharing Support Feature (Optional)*** (on page 70)

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..... 2
- Estimated Timeline 7
- Determine Which Optional Features to Enable 8

Site Requirements

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

Hardware Requirements

The following hardware prerequisites are required to deploy virtual machines (VMs) in a DTACS 5.0 environment.

- Requires Cisco UCS hardware (C240 M3 or C240 M4) with the latest ESXi software installed.

  Important: If you are using a new UCS C240 server, refer to ***Appendix A, Hardware Configuration Procedures for the Cisco UCS C240 Server*** to configure the server. This must be completed prior to deploying the OVA. See ***UCS Hardware and Software Compatibility*** (***https://ucshcltool.cloudapps.cisco.com/public/***) for details.

- Supported DTACS Server Platform:

Platform	Hard Drives	Memory
Cisco UCS C240 M3	16 X 300 GB	128 GB minimum
Cisco UCS C240 M4	16 X 300 GB	128 GB minimum

  Notes:

  - EC and DTACS servers coexist on the same hardware.
  - The procedures in this guide deal primarily with the setup and configuration of the UCS C240 M3 server.
  - To ensure the reliable operation of the UCS and the DTACS, the UCS should be connected to a UPS-protected power source and should be shut down gracefully if there is a risk that the server will lose power. Details on the power requirements for the UCS can be found in the hardware installations guides provided with the servers.

- Cisco UCS hardware should have adequate CPU, Memory, a local disk datastore and a sufficient network for DTACS Virtual Machines (VMs):

CPUs	Memory (GB)	Hard Disks (GB)	Network Interfaces	Number of Nodes for HA
4	32	1 x 64 (root) 1 x 128 (disk)	1 x Public 1 x Headend	2

- C240 M3 Tested reference configuration:

Configuration	Specification
Server Series	C Series Standalone Server
UCS Release	1.5(3)
Server Model	C240-M3 (SFF)
OS Vendor	VMware
OS	VMware vSphere ESXi 5.5 or later
Component	RAID Adapter
Adapter	LSI 9271-8i /LSI 9271CV- 8i MegaRaid SAS HBA
Adapter Driver	**VMware 5.5**: 6.602.54.00.1vmw

- C240 M4 Tested reference configuration:

Configuration	Specification
Server Series	C Series Standalone Server
UCS Release	2.0(13i)
Server Model	C240-M4 (SFF)
OS Vendor	VMware
OS	VMware vSphere ESXi 5.5 or later
Component	RAID Adapter
Adapter	Cisco 12G SAS Modular Raid Controller
Adapter Driver	■ **VMware 6.0**: 6.605.08.00-6vmw.600.0.0.2494585 ■ **VMware 5.5 U2**: 6.606.06.00.1vmw

Note: This is the **minimum** tested reference configuration. Refer to the UCS Hardware and Software Compatibility Web page to ensure that your components satisfy these requirements. (http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html)

- **DTACS 5.0 Mapping**:
  - NET0 – vSwitch0 – Corp/Engineering Network

    Important: By default, DHCP is enabled on the eth0 NET0-vSwitch0-Corp network. If DHCP is not available, then a static IP address, netmask, and gateway, as well as DNS information is required.
  - NET1 – vSwitch1 – Headend (HE) Network
  - NET2 – vSwitch2 – RepDB Network

Note: RepDB is configured after the installation/migration to DTACS 5.0.

Software Requirements

The following software prerequisites are required for an SR 5.0 installation.

- VMware ESXi (5.5 or later) and vCenter infrastructure (software, license, and a running vCenter machine).
- Requires a vCenter Web UI login or a vSphere client to connect and perform management tasks.
  - vCenter login must have admin privileges to deploy VMs
- Admin Node installed (refer to the ***Admin Node Installation Guide*** [part number TP-00145].
- Linux Platform Template saved via vCenter Server (created from a procedure in the ***Admin Node Installation Guide***).
- Requires Admin Node access to copy the following files to your VM:
  - cisco-vcs-deployment-[VERSION].zip
  - dtacs-system-release-[VERSION].tar
  - SSL Certificates created for each unique DTACS node
  - CSCOlxplat-[VERSION].ova

    Note: The CSCOlxplat OVA is only needed if you are using vSphere client rather than the vSphere Web UI.
- You are currently running DTACS 4.1 or later (migration only).

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 DTACS.

Java must be enabled in the browser to be able to view the Performance Monitoring graph.

Turn Off Automatic Updates for Mozilla Firefox ESR Only

1. Open the Firefox browser.
2. Click the **Navigation** icon,  , and select **Options**.
3. From the left area, click **Advanced** and then click the **Update** tab.
4. In the Firefox Updates section, click either the **Check for updates but let me choose whether to install them** or the **Never check for updates** option.
5. Click **OK**.

X.509 CA Certificate and Associated Private Key Requirements

Important: During the installation and configuration of the Admin Node, you should have created a root CA, as well as all of the certificate/key pairs for each node in your NextX system. If you have not created these certificates, refer to Chapters 5 through 6 in the ***Admin Node Installation Guide*** to create them now.

Each DTACS 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.

The NextX X.509 certificates were created when you deployed and configured the Admin Node. In this guide, you will distribute the appropriate certificates from the Admin Node to their respective DTACS node.

Additional IP Address and NAS Interface Requirements

In addition to inheriting all of the IP address of the existing DTACS, the SR 5.0 DTACS will require the following additional IP addresses.

- Temporary 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 UCS/DTACS 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 vCenter Server to do so.

Estimated Timeline

Estimated Time to Complete the Upgrade

The upgrade to DTACS 5.0 features the forklift upgrade, which allows you 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.

Determine Which Optional Features to Enable

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:

- Any features that have been previously enabled or licensed as part of an earlier upgrade do not have to be re-enabled.
- If this is a new install to and features need to be enabled, contact Cisco Services.

2

Deploy the DTACS Virtual Machine

Introduction

Important: If this is a new UCS C240 server, refer to Appendix A, Hardware Configuration Procedures for the Cisco UCS C240 Server, to install and configure the server. The procedures in the appendix only need performed once. When you have completed the installation and configuration of the server, return to this chapter.

This chapter provides the procedure to deploy a DTACS VM from a Linux platform template. This template was created when the Admin Node was built. You will need the admin user password that was created 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 Admin Node IP address, the location and the password for the Linux platform template.

In This Chapter

- Deploying the VM From the Linux Platform Template 10
- Reconfiguring the Virtual Hardware Settings on the VM 12
- Setting the Power Policy 13

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, deploy the OVF template on the *secondary* DTACS.
- If you are deploying your VM from a vSphere ESXi client, refer to Appendix B, ***Procedures When Using an ESXi Client*** (on page 123).

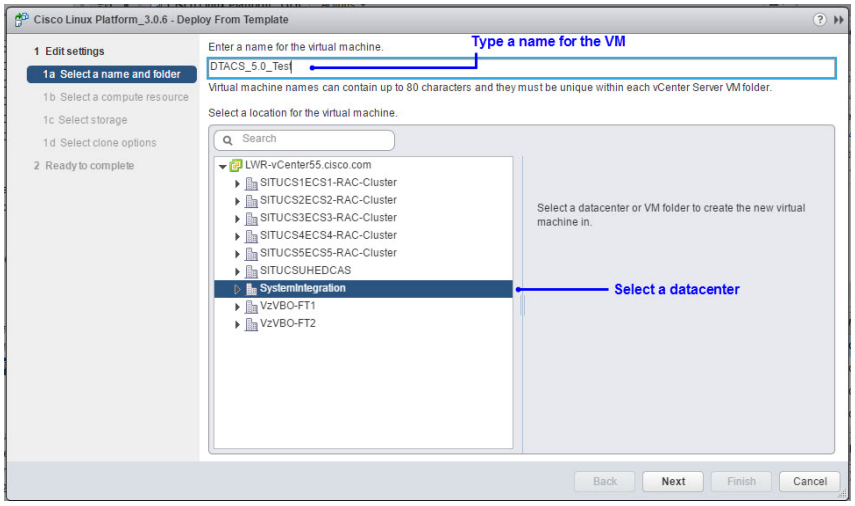
Follow these steps to deploy the OVA.

1 From vCenter Web client, click **VMs and Templates**.

2 Locate and select the CSCOlxplat template that was created from the procedures in the ***Admin Node Installation Guide***.

3 Right-click the template and select **Deploy VM from this Template**. The Deploy From Template window opens.

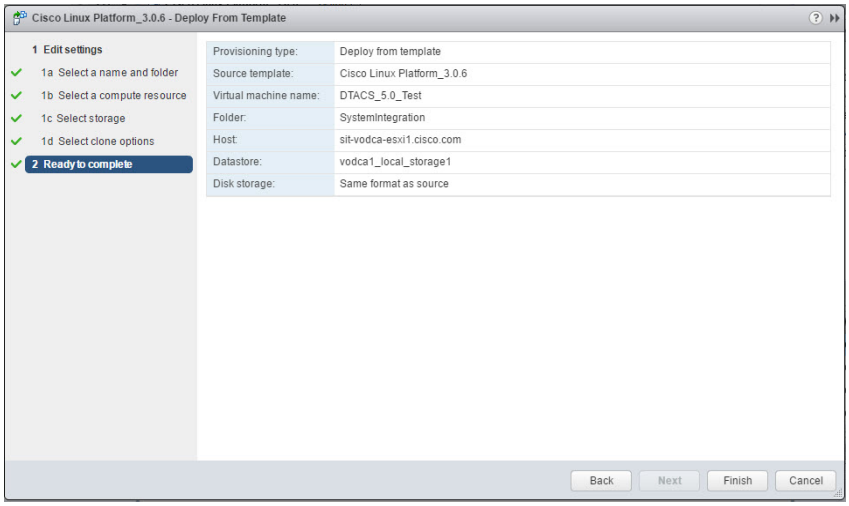
4 In the text box, enter a name for the VM you are creating and then select the datacenter or VM folder where it will be deployed. Click **Next.**



5 Select the compute resource (e.g. cluster, host) where the VM will run and click **Next**.

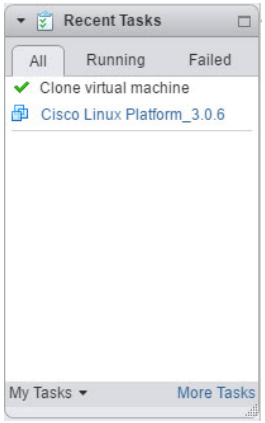
6 From the **Select virtual disk format** dropdown menu, maintain the **Same format as source** default. Then ensure that the appropriate datastore is selected.

7 Click **Next** and then click **Next** again. The Ready to Complete view displays.



8 Review the settings and click **Finish**.

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



Reconfiguring the Virtual Hardware Settings on the VM

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

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

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

2 Locate and select the new 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 **Memory** entry, modify the memory to **32 GB**.

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

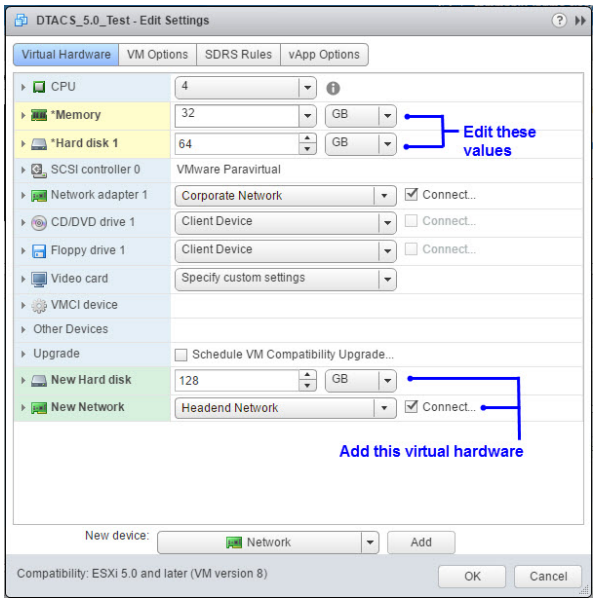
6 From the **New device** dropdown menu at the bottom of the window, select **New Hard Disk**.

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

8 Modify the disk size to **128 GB**.

9 From the **New device** dropdown menu, select **Network** and then click **Add**. A New Network entry is added to the bottom of the Virtual Hardware list.

10 From the dropdown menu, select the network label for the headend (i.e. HeadEnd Network).



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.

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.

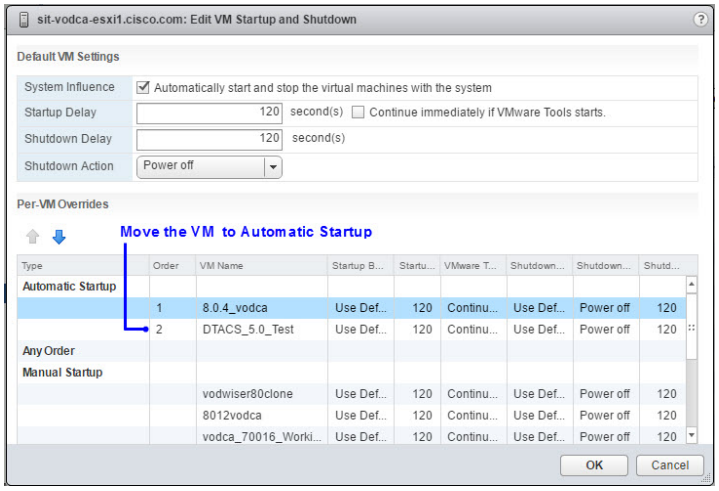
3 Click the **Settings** tab and from the Virtual Machines area, click **VM Startup/Shutdown**.

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.

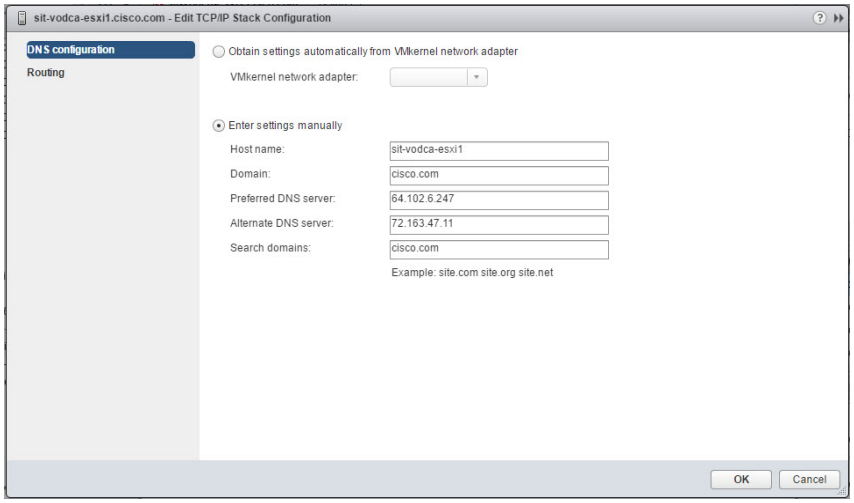


8 Click **OK**.

9 Click the **Networking** tab and then click **TCP/IP configuration**.

10 Click the **pencil** icon, , and then click **DNS configuration**.

11 Click the **Enter settings manually** radio button and then enter the IP address for the **Preferred DNS server** and the **Alternate DNS server**.



12 Click **Routing** from the left area, and if necessary, enter the default gateway in the **VMkernel gateway** text box.

13 Click **OK**.

3

Preparing the System for the Installation or Migration

This chapter contains procedures to prepare the system for the installation or migration of DTACS 5.0.

Important: Follow the procedures carefully as some procedures will not always pertain to both a new installation and a migration.

In This Chapter

- Shutdown the Secondary SR 4.1 DTACS VM 16
- Power on the New DTACS VM 17
- Set Up the Network With a Static IP Configuration (Optional) 19

Shutdown the Secondary SR 4.1 DTACS VM

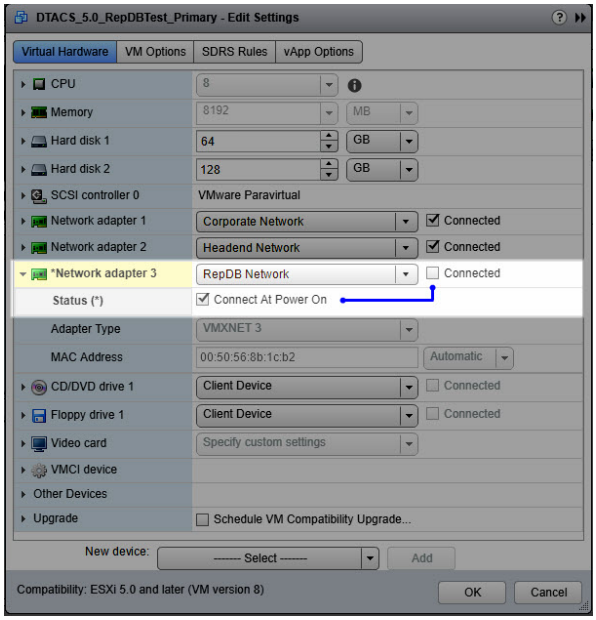
Important: Complete this procedure if you are performing a migration to SR 5.0. If this is an initial installation or you are creating a secondary VM for Replicated Database, go to ***Power on the New DTACS VM*** (on page 17).

Complete the following procedure on the *secondary* SR 4.1 DTACS.

1. Backup the key files and database to your NAS drive using one of the following methods.
   - The 4.1 ISO image
   - Backup and Restore scripts available from Cisco
   - Cloning the VM
2. Is RepDB enabled on your system?
   - If **yes**, refer to the ***Replicated Database Operator's Guide*** (part number TP-00140) to disable it. Then go to the next step.
   - If **no**, go to the next step.
3. Select and right-click the *secondary* DTACS and select **All vCenter Actions > Power > Power Off**. The secondary DTACS is shut down.

Power on the New DTACS VM

1. Select and right-click the DTACS 5.0 VM and select **Power On**.
2. Is this a new installation of SR 5.0?
   - If **no** and this is a migration, go to the next step.
   - If **yes**, go to Step 6.
3. Select and right-click the DTACS SR 5.0 VM again and select **Edit Settings**.
4. Unselect the **Connected** box for the **Network adapter 2** (Headend Network) device.



   Note: Do ***not*** unselect the **Connect At Power On** box.
5. Click **OK**. Monitor the **Recent Tasks** area until the VM is successfully reconfigured.
6. Right-click the VM again and select **Open Console**.

   Note: If you are using DHCP, you can use an SSH client to login to the VM.
7. 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]

   Important: If you are performing an DTACS migration, you will use this password to create an admin user in the ***Creating an Admin User on the DTACS 4.1 Server*** (on page 36).

8 Do you plan to configure a static IP configuration?

- If **yes**, go to ***Set Up the Network With a Static IP Configuration (Optional)*** (on page 19).
- If **no**, go to ***DTACS 5.0 Installation*** (on page 23).

Set Up the Network With a Static IP Configuration (Optional)

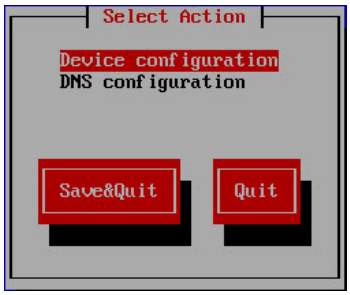
Important: This procedure is only required if you choose to set up your network with a static IP configuration. If you choose to use a DHCP configuration, you can skip this procedure and go to ***DTACS 5.0 Installation*** (on page 23).

By default, eth0 (Corporate Network) will boot up as DHCP. If you wish to change to a static IP, you must manually update ifcfg-eth0, DNS and add static routes.

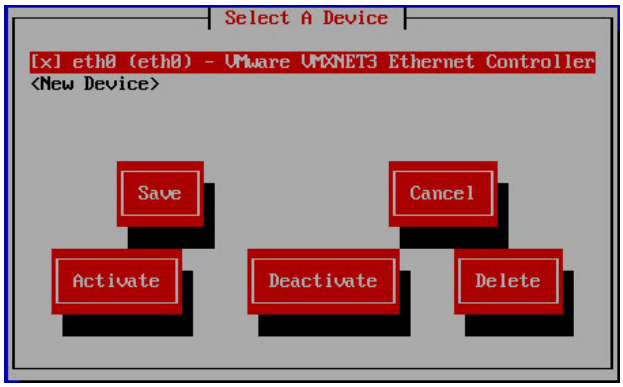
Complete the following procedure to configure a static IP network for the Cisco Linux platform.

1 From the console window, enter the following command to configure the network and DNS settings. The Select Device window displays.

```
[admin@platform ~]$ sudo system-config-network
```



2 Maintain the **Device configuration** selection and press **Enter**. The Select a Device window appears.



3 Maintain the default setting to configure eth0 and press **Enter**.

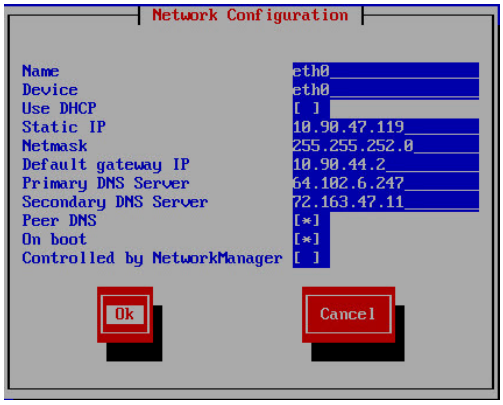
4 Press the **Tab** key until the cursor is in the **Use DHCP** field. Then press the **Spacebar** to unselect this option.

5 Tab to each of the following fields to enter the appropriate values for your system.

- **Static IP**
- **Netmask**
- **Default gateway IP**
- **Primary DNS Server**
- **Secondary DNS Server**

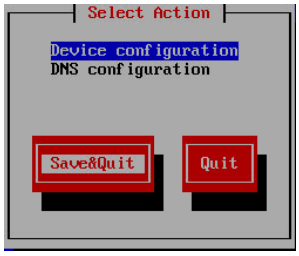
6 Verify that **Peer DNS** is selected.

7 Press the **Tab** key until the cursor is in the **Controlled by NetworkManager** field. Then press the **Spacebar** to unselect this option.



8 Press **Tab** to highlight **Ok** and press **Enter**. The Select A Device window appears.

9 Press **Tab** to highlight **Save** and press **Enter**. The Select Action window appears.



10 Click **Save&Quit**.

11 Enter the following command to edit the **ifcfg-eth0** configuration file.

```
[admin@platform ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-eth0
```

12 Go to the **IPV6INIT** field and change the value from yes to **no**.

13 Go to the **HWADDR** field and delete the entire line.

14 Save and close the file.

15 Restart the network service to update the interface configuration.

```
[admin@platform ~]$ sudo service network restart
```

16 Close the console window.

17 Using an SSH client, log into the VM using the IP address you configured for eth0.

18 Is the DTACS on the same network as the Admin Node?

- If **yes**, then go to the ***DTACS 5.0 Installation*** (on page 23).
- If **no**, add a route to the DTACS.

  Note: Only add routes that are required to access the Admin Node and/or the local machine where the Cisco VCS Deployment scripts were downloaded. Please note that any static routes added to /etc/sysconfig/network-scripts/route-eth0 will be overwritten during the deployment of packages.

  Example:

```
[admin@platform ~]$ sudo route add –net 10.90.44.0/24
gw 10.90.47.1 dev eth0
```

19 Can you can ping the Admin Node from the DTACS.

- If **yes**, go to the next section.
- If **no**, troubleshoot your network or contact your system administrator.

4

DTACS 5.0 Installation

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

This chapter provides step-by-step instructions for copying the DTACS application (zip file) to your VM and for installing the application.

In This Chapter

- Copying the VCS Deployment Zip File to the VM 24
- Installing DTACS 5.0 25
- Transfer HTTPS X.509 Certificates to the DTACS Server 27

Copying the VCS Deployment Zip File to the VM

The cisco-vcs-deployment zip file resides on the Admin Node for your site. In this procedure, you will copy this file to your VM.

Important: You will need the IP address of the Admin Node for this procedure.

1 Enter the following command to change to **root** user.

```
[admin@platform ~]$ sudo -i
[root@platform ~]#
```

Important: At this point, the only user that can log into the system is the **admin** user. When you see the instruction, "As root user", you will need to execute "sudo -i" from the admin user account to become root user.

2 Secure copy (SCP protocol) the **cisco-vcs-deployment** zip file from the Admin Node to the **/var/tmp** directory on the new VM.

Command Syntax: Assumes the zip file is in the /opt/cisco/software/admin_node directory on the Admin Node.

```
scp admin@[Admin_Node_IP]:/opt/cisco/software/admin_node/
cisco-vcs-deployment-1.0.X.zip /var/tmp
```

Example:

```
[root@platform scripts]# admin@10.90.47.106://opt/cisco/software/admin_node/cisco-vcs-d
eployment-1.0.6.zip /var/tmp
The authenticity of host '10.90.47.106 (10.90.47.106)' can't be established.
RSA key fingerprint is 2f:33:59:4f:c4:e8:89:0d:fd:99:aa:57:21:08:8c:ae.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.90.47.106' (RSA) to the list of known hosts.
admin@10.90.47.106's password:
cisco-vcs-deployment-1.0.6.zip                100%   29KB  29.4KB/s   00:00
```

3 On the new VM, change to the **/var/tmp** directory.

```
[root@platform ~]# cd /var/tmp
```

4 Unzip the file using the following command.

```
[root@platform tmp]# unzip cisco-vcs-deployment*.zip
```

5 Enter the following command to change to the **cisco-vcs-deployment-1.0.x/scripts** directory.

```
[root@platform tmp]# cd cisco-vcs-deployment*/scripts
```

6 Enter the following command to verify that the following DTACS-specific files are present.

- **deploy-dtacs.sh**
- **dtacs.envfile**

```
[root@platform scripts]# ls -ltr| grep dtacs
```

7 Stay in this directory and go to the next section.

Installing DTACS 5.0

Important: You will need the IP address or the Admin Node for this procedure.

1 Enter the following command to open the **dtacs.envfile** file in a text editor.

```
[root@platform scripts]# vi dtacs.envfile
```

2 Enter values specific to your system.

Important:

- Values are required for each line.
- Go to the end of the file and add a "hostname=" entry and then append the hostname for your DTACS.
  - If this is a migration, the hostname must match the previous system hostname. If you are not sure, type hostname on the 4.1 DTACS active system.

    Note: If this is a migration from SR 4.1 to SR 5.0 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 ***Updating the site_info Database Table for a Hostname Change*** (on page 49) procedure, post upgrade, or dtacsInit.d will not start.

Default dtacs.envfile

```
admin_node=
default_gateway=
dtacs_headend_interface=
dtacs_headend_ip=
dtacs_headend_netmask=
route_eth0_file=
```

Example dtacs.envfile

```
admin_node=10.90.44.70
default_gateway=10.90.44.2
dtacs_headend_interface=eth1
dtacs_headend_ip=204.3.1.33
dtacs_headend_netmask=255.255.255.240
route_eth0_file=/var/tmp/route-eth0
hostname=dtacs_50
```

3 Save and close the file.

4 Enter the following command to create the route-eth0 file in the **/var/tmp** directory.

Note: If this is a migration, reference the /etc/rc2.d/S85SASpecial file on the DTACS 4.1 system to obtain the appropriate routes.

```
[root@platform scripts]# vi /var/tmp/route-eth0
```

Example:

```
10.90.0.0/16 via 10.90.44.2 dev eth0
64.100.0.0/16 via 10.90.44.2 dev eth0
64.102.0.0/16 via 10.90.44.2 dev eth0
10.116.0.0/16 via 10.90.44.2 dev eth0
10.84.0.0/16 via 10.90.44.2 dev eth0
10.82.0.0/16 via 10.90.44.2 dev eth0
10.78.192.0/21 via 10.90.44.2 dev eth0
10.143.32.0/23 via 10.90.44.2 dev eth0
172.18.0.0/23 via 10.90.44.2 dev eth0
```

5 Save and close the **route-eth0** file.

6 Execute the following command to deploy the DTACS application. This will take several minutes.

```
[root@platform scripts]# ./deploy-dtacs.sh
--envfile=dtacs.envfile 2>&1 | tee /var/log/deploy-dtacs.out
```

Result: A "dtacs installation completed" message will display with no errors. The VM will then reboot.

Example:

```
+ shutdown -r now 'dtacs installation completed'

Broadcast message from admin@platform
        (/dev/pts/0) at 11:35 ...

The system is going down for reboot NOW!
```

7 In the terminal window, log back into the DTACS as **admin** user.

8 Verify that the network interfaces are up by entering the following command.

```
[root@dtacs_50 ~]# ifconfig -a
```

9 Enter the following command to verify that the RPM packages are installed.

```
[root@dtacs_50 ~]# rpm -qa | egrep -i "puppet|cscodtacs"
```

```
CSCOdtacs-help-5.0.4-1.el6.noarch
CSCOdtacs-bootp-5.0.10-1.201705041125.el6.x86_64
CSCOdtacs-core-libs-5.0.10-1.201705041125.el6.x86_64
CSCOdtacs-5.0.10-1.201705041125.el6.x86_64
puppetlabs-release-22.0-2.noarch
cisco-vcs-puppet-modules-1.0.7-1.0.noarch
CSCOdtacs-prep-5.0.10-1.201705041125.el6.x86_64
CSCOdtacs-app-5.0.10-1.201705041125.el6.x86_64
CSCOdtacs-core-5.0.10-1.201705041125.el6.x86_64
puppet-3.8.7-1.el6.noarch
CSCOdtacs-webui-5.0.10-1.201705041125.el6.x86_64
CSCOdtacs-system-release-5.0.9-1.201704120758.el6.noarch
```

Result: A list of the installed packages are displayed.

10 Do any patches to the installation exist?

- If **yes**, go to ***DTACS 5.0 Patch Installs*** (on page 143). Once the patch is installed, go to the next section in this chapter.
- If **no**, go to the next section.

Transfer HTTPS X.509 Certificates to the DTACS Server

Important: The NextX X.509 certificates were created for each DTACS node when you deployed the Admin Node. If they have not yet been created, go to the following chapters in the ***Admin Node Installation Guide*** to create them now.

- Chapter 5: Create Environment Files for NextX Nodes
- Chapter 6: Create NextX X.509 Root CA Certificates

This section includes the procedures to transfer the HTTPS X.509 certificates from the Admin Node to the DTACS node in your system.

Creating the config.json File on the DTACS

Complete the following steps to configure the config.json file on the DTACS.

1. As **admin** user on the DTACS server, enter the following command to copy the /etc/consul/client.json.template file to the **/etc/consul/config.json** file.

   ```
   [admin@dtacs_50 ~]$ sudo cp /etc/consul/client.json.template
   /etc/consul/config.json
   ```

2. Enter the following command to open the **/etc/consul/config.json** file in a text editor.

   ```
   [admin@dtacs_50 ~]$ sudo /etc/consul/config.json
   ```

3. In the "**bind_addr**" line, replace <client_ip> with the IP address of the DTACS.

   Example:

   ```
   "bind_address": "10.90.45.181"
   ```

4. Do you plan on building an Explorer Controller Suite (ECS) 3.0 system?
   - If **no**, save and close the config.json file and then ***Transferring DTACS Certificates Created From the Admin Node*** (on page 28).
   - If **yes**, do not close this file and go to the next step.

     Note: You may need to refer to the **Deploying the Consul VM** section of the *Explorer Controller Suite 3.0 Installation and Upgrade Guide* (part number TP-00133) for assistance.

5. Has a consul encrypt key been generated for your NextX system?
   - If **no**, go to the next step.
   - If **yes**, retrieve the encrypt key and go to Step 7.

6. From another terminal window, log into the Admin Node and enter the following command to generate the consul encryption key. A key is generated and displayed in the output.

   ```
   [admin@adminnode ~]$ sudo consul keygen
   ```

Example:

```
nSv70A9cEX28KLfmUgRLHA==
```

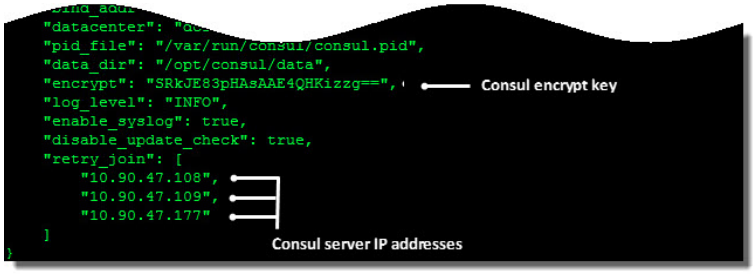
Note: Store the key in a safe location as you will need it for all nodes in your NextX system.

7 In the terminal window for the DTACS, where the config.json file is open, go to the **"encrypt"** line and replace <output from <`consul keygen`> with the encryption key.

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

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

Example:



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

Transferring DTACS Certificates Created From the Admin Node

Important: This procedure must be executed for certificates that were generated from an internal root CA or from an external CA.

Complete the following steps to transfer the appropriate certificate files to the DTACS node.

Note: You should have two terminal windows open from the previous procedure. One for the DTACS where you are logged in as root user and one for the Admin Node where you are logged in as admin.

1 On the Admin Node, enter the following command to change to the **/opt/cisco/ca** directory.

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

2 Enter the following command and press **Enter** to transfer the certificate and key pair to the DTACS.

Command Syntax:

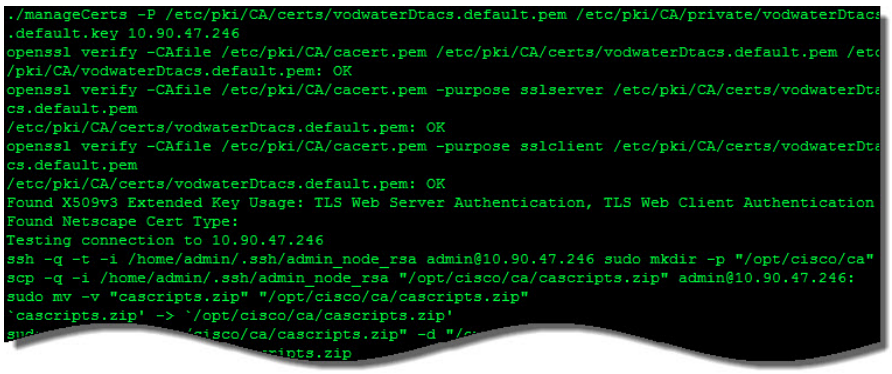
```
sudo ./manageCerts -P [absolute_path_to_cert]
[absolute_path_to_key] [DTACS_IP]
```

Example:

```
[admin@adminnode ca] sudo ./manageCerts -P
/etc/pki/CA/certs/vodwaterDtacs.domain.pem
/etc/pki/CA/private/vodwaterDtacs.domain.key 10.90.47.246
```

Notes:

- Replace [cert] with the location of the node certificate file (e.g. /etc/pki/CA/certs/[CA.pem]) on the Admin Node.
- Replace [key] with the location of the node private key file (e.g. /etc/pki/CA/private/[CA.key]) on the Admin Node.
- Replace [IP] with the IP address of the DTACS, which is the IP address defined as IP.1 in the [hostname].env file for that DTACS.



3 Were you prompted to verify the SSH RSA key fingerprint:

- If **yes**, type **yes** and press **Enter**. Then go to the next step.
- If **no**, go to the next step.

4 When prompted, enter and then re-enter the DTACS admin password.

5 When prompted, enter the keystore password and press **Enter**. Make note of this keystore password.

6 When prompted again, re-enter the keystore password and press **Enter**.

7 When prompted, enter the trust store password and press **Enter**. Make note of this trust store password.

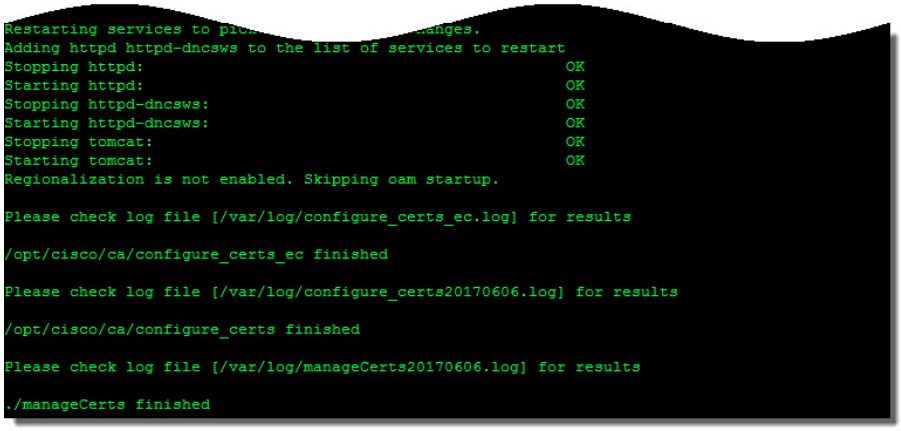
Note: Alternatively press **Enter** to use the keystore passphrase from the previous step.

8 When prompted again, re-enter the trust store password and press **Enter**.

Results:

- The keystore and truststore are generated from the signed SSL certificates on the DTACS node.
- The SSL certificate is deployed for the HTTPS service.
- Apache and tomcat services are restarted.
- A **./manageCerts finished** message displays.

Example:



9 Go to *Verifying the DTACS Certificate Configuration* (on page 30) to verify that the X.509 certificate was successfully configured.

Verifying the DTACS Certificate Configuration

Complete the following procedure to verify the certificate configuration.

Notes:

- If the DTACS system is not regionalized, then the consul service will not be running. Executing this procedure will result in an error when the consul service is not running. You can ignore this message.
- 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 Installation Guide*. This procedure allows you to execute encrypted communication checks for all nodes, including the DTACS.

1 As **admin** user on the Admin Node, enter the following command to check the certificate configuration for DTACS in which certificates have been generated. A validation of the certificate files occurs.

Command Syntax:

```
[admin@adminnode ca]$ sudo ./checkConfig -s [hostname.env]
```

Example:

```
[admin@adminnode ca]$ sudo ./checkConfig -s vodwaterDtacs.env
```

```
==========20170601.134808==========
./checkConfig -s vodwaterDtacs.env

===Checking node at IP 10.90.47.104 from vodwaterDtacs.env
Validating files in check/10.90.47.104
Checking ec or dtacs at 10.90.47.104
10.90.47.104 has consul enabled
10.90.47.104 has consul running
10.90.47.104 has tomcat enabled
10.90.47.104 has tomcat running
10.90.47.104 has httpd enabled
10.90.47.104 has httpd running
10.90.47.104 has httpd-dncsws enabled
10.90.47.104 has httpd-dncsws running
Checking consul config etc/consul/config.json
Checking CA cert etc/pki/tls/cacert.pem
Checking server client key etc/pki/tls/certs/bossclient.key
Checking CA cert etc/pki/tls/certs/cacert.pem
Checking CA chain etc/pki/tls/certs/cachain.crt
Checking Keystore etc/pki/tls/certs/genericKeystore.jks
Found aliases  Alias name: vodwater-Dtacs50
Checking Truststore etc/pki/tls/certs/genericTruststore.jks
Found aliases  Alias name: caserver
Checking server client key etc/pki/tls/certs/ldsclient.key
Checking server client key etc/pki/tls/certs/rpoclient.key
Checking server cert etc/pki/tls/certs/server.crt
Checking server key etc/pki/tls/certs/server.key
Checking server key etc/pki/tls/private/server.key
Checking security properties opt/cisco/vcs/security.properties
openssl verify -CAfile /opt/cisco/ca/check/10.90.47.104/etc/pki/tls/cacert.pem /opt/cisco/ca/c
heck/10.90.47.104/etc/pki/tls/certs/server.crt
/opt/cisco/ca/check/10.90.47.104/etc/pki/tls/certs/server.crt: OK
```

2 Did any errors display?

- If **yes**, review the **/var/log/checkConfig[date].log** file to remedy the issue. Then repeat Step 1. When the issues are corrected, you have completed this procedure.
- If **no**, go to the next step.

3 Do you plan to regionalize the DTACS to an existing ECS?

- If **yes**, go to the next step.
- If **no**, skip to step 16.

4 Is the DTACS currently regionalized?

- If **yes**, go to the next step.
- If **no**, refer to **Appendix B** in the ***ECS 3.0 Installation and Upgrade Guide*** to regionalize it to the ECS. Then go to Step 16.

5 From a terminal window for the DTACS, enter the following command to view the status of the consul service.

```
[admin@vodwaterDtacs consul]$ service consul status
```

6 Is the consul service running?

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

```
[admin@vodwaterDtacs ~]$ sudo service consul start
```

7 Enter the following command to SSH to the *primary* Consul node as **admin** user.

8 Enter the following command to stop and restart the consul service.

```
[admin@consul ~]$ sudo service consul stop
[admin@consul ~]$ sudo service consul start
```

9 Verify that the consul service started successfully.

```
[admin@consul ~]$ sudo service consul status
```

10 Enter the following command to verify that the consul service is running.

```
[admin@consul ~]$ sudo consul monitor
```

Result: Output similar to the following should display.

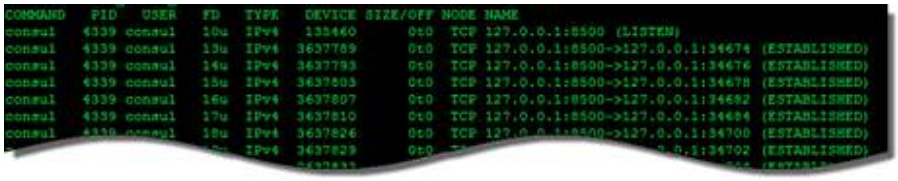
```
2017/04/11 13:15:42 [INFO] agent.rpc: Accepted client:
127.0.0.1:50448
```

Note: Press **Ctrl-C** to exit from the consul monitor.

11 Enter the following command to view a list of open processes/files on port 8500.

```
[admin@consul ~]$ sudo lsof -Pni :8500
```

Example Output:



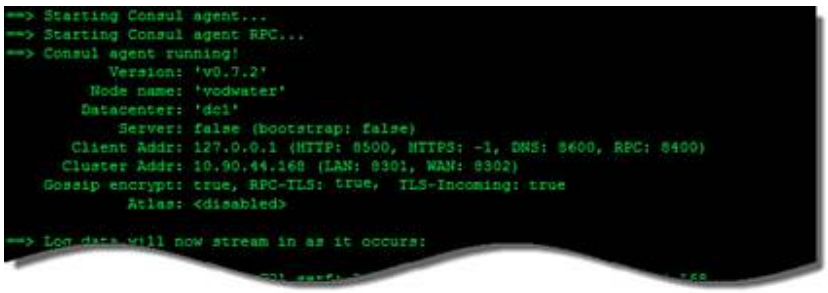
12 Enter the following command to verify that DTACS is now in the current list of members that the Consul knows about.

```
[admin@consul ~]$ sudo consul members
```

Example Output:

13 Review the **/var/log/consul/consul.log** file to verify that consul encryption has been successfully enabled.

Example Output:



14 Verify that the following values are all set to **true**.

Note: These three values appear on the same line

- Gossip encrypt
- RPC-TLS
- TLS-Incoming

15 Type **exit** to close the SSH session to the Consul node.

16 Is this a new installation?

Note: If you just configured a *secondary* host for your system, go to ***Configure and Operate the Replicated Database*** (on page 71).

- If **yes**, go to ***Post Upgrade Procedures*** (on page 43).
- If **no** and this is a migration, go to ***Migrate DTACS 4.1 to DTACS 5.0*** (on page 35). Type **exit** to close the SSH session to the Consul node and return to the DTACS session.

5

Migrate DTACS 4.1 to DTACS 5.0

Important: If you are executing a new DTACS 5.0 installation, skip this section and go to ***DTACS 5.0 Post Upgrade Procedures*** (see "***Post Upgrade Procedures***" on page 43).

This section provides the procedure to migrate a DTACS 4.1 running on a Solaris_x86-10 platform to DTACS 5.0 on a Cisco Linux platform.

In This Chapter

- Creating an Admin User on the DTACS 4.1 Server 36
- Migrating Key Files and Database to DTACS 5.0 37
- Updating the DTACS Configuration 42

Creating an Admin User on the DTACS 4.1 Server

To successfully migrate to DTACS 5.0, you must create an admin user on the DTACS 4.1 server. The admin user is used to assist in the migration activities.

Important: This section provides the steps to be completed on the existing DTACS 4.1 system.

1. From a terminal window, log into the SR 4.1 DTACS.
2. 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
   ```

3. Enter the following command to set the password for the **admin** user.

   ```
   # passwd -r files admin
   ```

4. When prompted for the new password, enter the same password defined for the admin user on the newly deployed SR 5.0 DTACS server.

   Important: The password for the admin user on the SR 4.1 and SR 5.0 DTACS systems must match.

5. When prompted, re-enter the password. A successful message appears.
6. 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_config** 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.
7. Complete these steps to verify that the admin user as sudo root access.
   a. In a new terminal window, log into the 4.1 DTACS as **admin** user.
   b. When prompted, enter the admin password.
   c. Enter **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 6.

Migrating Key Files and Database to DTACS 5.0

This section provides the procedure to migrate an existing Solaris_x86 SR 4.1 DTACS server to the new DTACS SR 5.0 Linux platform.

Important: If the SR 4.1 DTACS server is registered to Explorer Controller Suite (ECS) 2.0, you must first unregionalize and delete the registration. Refer to Appendix B in the ***Explorer Controller Suite 3.0 Installation and Upgrade Guide*** for details.

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 Enter the following command to view the description of the **migrateKeyFiles** script.

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

```
usage: migrateUsers [-h] --source [SRC_HOST]

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
```

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

```
[admin@vodwater ~]$ 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 DTACS SR 4.1 to DTACS SR 5.0. The migration script for the key files will put the key files migration RSA key (kfm_rsa) in place and 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 DTACS SR 5.0 system.

Complete the following procedure to migrate the key files.

Note: These procedures will be executed on the DTACS SR 5.0 system.

1 AS **admin** user, change to the **/opt/cisco/backup_restore** directory.

```
[admin@dtacs_50 ~]$ sudo cd /opt/cisco/backup_restore
```

2 Execute one of the following migrateKeyFiles script as shown below.

Note: Substitute the IP address for the DTACS SR 4.1 server for the <DTACS_4.x_IP> entry in the command.

Migrate Default Key Files Command

```
migrateKeyFiles -v -l admin -r <DTACS_4.x_IP>
```

Migrate Default Key Files Example

```
[admin@dtacs_50 backup_restore]$ sudo ./migrateKeyFiles -v -l
admin -r 10.90.46.120
```

Migrate Default and Specific Key Files Command

```
migrateKeyFiles -v -I <PATH/keyfiles_include> -E
<PATH/keyfiles_exclude> -l admin -r <DTACS_4.x_IP>
```

Migrate Default and Specific Key Files Example

```
[admin@dtacs_50 backup_restore]$ sudo ./migrateKeyFiles -v -I
tmp/keyfiles_include -E /tmp/keyfiles_exclude -l admin -r
10.90.46.120
```

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

4 When prompted, enter the admin password and press **Enter**.

5 Re-enter the admin password and press **Enter**. The key files are migrated to the SR 5.0 DTACS in the /disk1/keyfiles_staging directory. The keyfile migration starts.

6 When the script completes, review the output in the **/var/log/migrateKeyFilesLog**.

Migrating Users

In this section, you will migrate the users and their user directories from 4.1 to SR 5.0. 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.

Complete the following procedure to migrate users.

Note: From the previous procedure, you should still be root user and in the /opt/cisco/backup_restore directory.

1 Execute the following script to migrate users to the SR 4.1 DTACS server. You will be prompted to confirm or deny the migration of each user, line by line.

Note: Substitute the IP address for the SR 4.1 DTACS server for the <DTACS_4.x_IP> entry in the command.

Migrate Users Command

```
migrateUsers --source <DTACS_4.x_IP>
```

Migrate Users Example

```
[admin@dtacs_50 backup_restore]$ sudo ./migrateUsers --source
10.90.46.120
```

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

Result: Once you have responded to all user prompts, each user's home directory is present in **/home/<user>/migrated_home**.

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 DTACS processes on the SR 4.1 system
- All billing transactions and updates to the active SR 4.1 system will be suspended

In this section, you will migrate the database from the SR 4.1 system to the SR 5.0 system. 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 when running this script. Therefore, perform this procedure in a maintenance window as services will be impacted.

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

Important: Substitute the IP address for the SR 4.1 DTACS server for the <DTACS_4.x_IP> entry in the command.

Migrate Database and Key Files Command

```
migrateDBKF --source <DTACS_4.x_IP> --db dtacs
```

Migrate Database and Key Files Example

```
[admin@dtacs_50 backup_restore]$ sudo ./migrateDBKF --source
10.90.46.120 --db dtacs
```

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

3 When the migration completes, open the **/disk1/keyfiles_staging/export/home/dtacs/.profile** file from the SR 5.0 DTACS server.

```
# vi /disk1/keyfiles_staging/export/home/dtacs/.profile
```

4 Copy the user-configured entries that are present.

5 Close the file.

6 Open the in the **/export/home/dncs/.profile** file from the SR 5.0 DTACS server in a text editor and paste the entries you copied from Step 4.

```
[admin@dtacs_50 scripts]$ sudo vi /export/home/dncs/.profile
```

7 Save and close the file.

8 By default during the migration, the files are copied as "dbreader" user. Execute the following steps to change the ownership of the files to **dncs:dncs**.

```
[admin@dtacs_50 scripts]$ sudo chown -R dncs:dncs
/dvs/dvsFiles/
```

Note: This /dvs/dvsFiles points to the /disk1/dvs/dvsFilesdirectory on the DTACS SR4.1 server.

9 Enter the following command to change to the **/dvs/dtacs** directory on the DTACS 5.0 server.

```
[admin@dtacs_50 scripts]$ cd /dvs/dtacs
```

10 Enter the following command to change the ownership of the OCDL directory and its sub-directories to **dncs:dncs**.

```
[admin@dtacs_50 scripts]$ sudo chown -R dncs:dncs OCDL
```

11 Enter the following command to change the ownership of the pub directory and its sub-directories to **dncs:dncs**.

```
[admin@dtacs_50 scripts]$ sudo chown dncs:dncs pub
```

12 From the DTACS SR 4.1 terminal window, type the following command to shutdown the server.

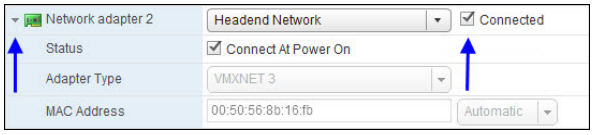
```
# shutdown -y -g0 -i0
```

13 Go to the next section in this chapter.

Updating the DTACS Configuration

1. From the vCenter Web UI, right-click the **SR 5.0 DTACS** server and select **Edit Settings**. The Edit Settings window appears.
2. From the Virtual Hardware area, click the pointer next to **Network adapter 2** and select **Connected**.

   Note: If you are using vSphere ESXi client, refer to ***Modifying the Device Status for an Ethernet Adapter*** (on page 126).



3. Click **OK**.
4. In the **SR 5.0 DTACS** terminal window, type `sudo service network restart` to restart the network service.

6

Post Upgrade Procedures

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

- Creating User Accounts 44
- Updating the site_info Database Table for a Hostname Change 49
- Configuring the DTACS Server for the EC 52
- Configuring the EC for DTACS 54
- Testing Synchronization Between the DTACS and EC Databases 56
- Setting Up SFTP Support 57
- Configuring DTACS BOSS Proxy (Optional) 61
- Restarting Apache and Tomcat Services 62
- CentOS cron and anacrontab Overview 63
- Verifying the crontab Entries Managed by cron 65
- Verifying User-Defined CRON Entries on the Migrated VM 66
- Starting DTACS Processes 67
- Testing dbsync from the DTACS Web UI 68
- Enabling RADIUS and LDAP (Optional) 69
- SCID Sharing Support Feature (Optional) 70

Creating User Accounts

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

User Account Types

The following user accounts can be created on the DTACS.

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

Accessing the root and dncs User Accounts

Important:

- Role-Based Access Control is no longer supported in DTACS 5.0. Please follow the steps below to switch between different user accounts.
- The dtacsadmin user is used in examples for all Cisco DBDS documents pertaining to DTACS 5.0.
- Commands run as root user are preceded with a **#** symbol.

  Example:

  ```
  [root@dtacs_50 ~]#
  ```

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

  Example:

  ```
  [admin@dtacs_50 ~]$
  [dtacsadmin@dtacs_50 ~]$
  [dncs@dtacs_50 ~]$
  ```

Once the DTACS application installation is complete, you can only log in with the admin or an Administrator 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:

Command Example: Executing a root command as Admin user:

```
[admin@dtacs_50 ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-eth0
```

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@dtacs_50 ~]$ sudo –i
```

Any ***Administrator*** account that you create using the useradmin script (see the next section) has privileges to log into the DTACS 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:

```
[dtacsadmin@dtacs_50 ~]$ sudo su - dncs
```

Note: Throughout all Cisco DBDS documentation, the dtacsadmin Administrator user is used as an example.

Overview:

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

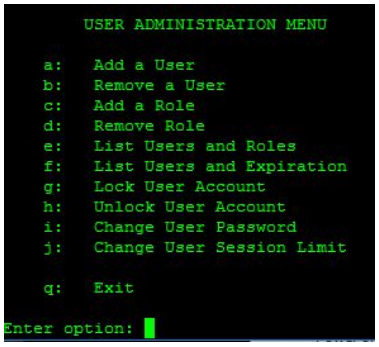
Creating an Administrative User Account

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 "dtacsadmin". 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 **dtacsadmin** user account on the DTACS. The USER ADMINISTRATION MENU appears.

```
[admin@dtacs_50 ~]$ 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 **dtacsadmin** 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 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?

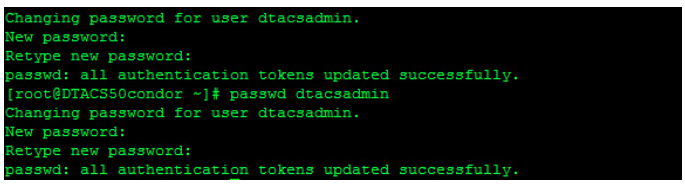
- If **no**, and you are storing passwords locally, go to the next step.
- If **yes**, go to Step 18.

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

```
[admin@dtacs_50 ~]$ sudo passwd dtacsadmin
```

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

Note: Enter the same password that you used when creating the dtacsadmin user with the USER ADMINISTRATION MENU.

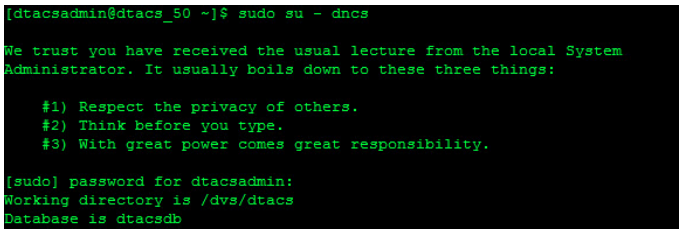


18 Open a new terminal window to the DTACS and login as **dtacsadmin**.

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

```
[dtacsadmin@dtacs_50 ~]$ sudo su - dncs
```

20 When prompted, enter the password for the dtacsadmin user.



Note: You should now have two terminal windows open; one as admin user (can sudo to root) and one as dtacsadmin user (use to sudo to dncs).

Updating the site_info Database Table for a Hostname Change

Important: If this is a new install or a migration from SR 4.1 to SR 5.0 in which the hostname of the SR 4.1 and SR 5.0 system is the same, you can skip this procedure.

Complete this procedure only if your SR 5.0 system was a migration from SR 4.1 in which the hostname was changed to a new hostname when you defined the ec.envfile in Installing DTACS 5.0.

Note: For this procedure, we will assume the SR 4.1 hostname is "dtacs" and the hostname that was added to the ec.envfile is "dtacs_50".

1 As **root** user, enter the following command to verify the current hostname for the SR 5.0 system.

Note: The output of this command should be the same as the "hostname=" value in the /var/tmp/cisco-vcs-deployment-1.0.*/scripts/ec.envfile.

```
[root@dtacs_50 ~]# hostname
```

Example Output:

```
dtacs_50
```

2 Enter the following command to source the environment.

```
[root@dtacs_50 ~]# . /dvs/dtacs/bin/dtacsSetup
```

3 Enter the following command to access the dtacs database. A database prompt appears.

```
[root@dtacs_50 ~]# dbaccess dtacsdb -
>
```

4 Enter the following command to view the output of the **site_info** table.

```
> select * from site_info;
```

Example Output:

```
site_id             1
site_name           DTACS
bfs_sess_mac_addr   00:00:00:00:00:00
site_ip_address     204.123.1.34
site_mac_address    00:00:00:00:00:00
site_hostname       dtacs
site_status         1
oob_flow_ipaddr
gda
gda_port            0

1 row(s) retrieved.
```

5 Does the **site_hostname** entry match the output from Step 1?

- If **yes**, go to Step 8.
- If **no**, go to the next step.

6 Enter the following command and press **Enter** to update the **site_hostname** entry. 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="dtacs_50" where
site_id=1;
```

```
> update site_info set site_hostname="dtacs_50" where site_id=1;

1 row(s) updated.
```

7 Repeat Step 4 to verify that the **site_hostname** was successfully updated in the site_info table.

Example Output:

```
site_id             1
site_name           DTACS
bfs_sess_mac_addr   00:00:00:00:00:00
site_ip_address     204.123.1.34
site_mac_address    00:00:00:00:00:00
site_hostname       dtacs_50 ◄——— Updated hostname
site_status         1
oob_flow_ipaddr
gda
gda_port            0

1 row(s) retrieved.
```

8 Press **Ctrl+C** to exit the database.

9 Enter the following command to verify the IP address for the **dtacsatm** entry.

```
[root@dtacs_50 ~]# less /etc/hosts | grep dtacsatm
```

Example Output:

```
204.4.12.34      dtacsatm dtacs_host dtacshost
```

10 Does the site_ip_address entry match the dtacsatm IP address from the output of Step 7?

- If **yes**, you have completed this procedure.
- If **no**, go to the next step.

11 Enter the following command to access the dtacs database. A database prompt appears.

```
[root@dtacs_50 ~]# dbaccess dtacsdb -
>
```

12 Enter the following command and press **Enter** to update the **site_ip_address** entry. You are returned to the database prompt.

Command Syntax:

```
update site_info set site_ip_address="[new_dtacsatm_IP]" where
site_id=[site_id value];
```

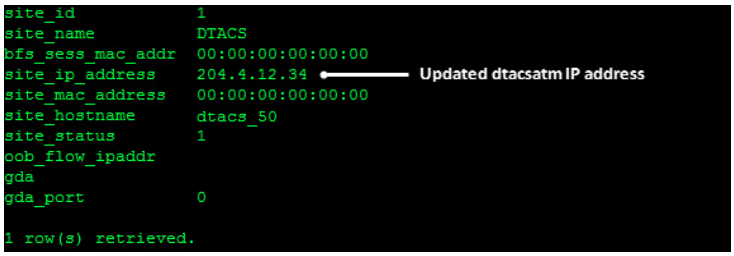
Example:

```
> update site_info set site_ip_address="204.4.12.34" where
site_id=1;
```

13 Enter the following command to verify that the **site_ip_address** entry was successfully updated in the site_info table.

```
> select * from site_info;
```

Example Output:



14 Press **Ctrl+C** to exit the database.

Configuring the DTACS Server for the EC

Important: This procedure is executed on the DTACS server.

1 As **admin** user on the DTACS VM, enter the following command to open the **/opt/cisco/informix/server/etc/sqlhosts** file in a text editor.

```
[admin@dtacs_50 ~]$ sudo vi
/opt/cisco/informix/server/etc/sqlhosts
```

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

- **If Associated EC is SR 8.0**:

```
dncsatmDbServer  onsoctcp  dncsatm  sqlexec
```

- **If Associated EC is SR 7.x**:

```
dncsatmDbServer  onsoctcp  dncsatm  informixOnline
```

3 Save and close the file.

4 Is the associated EC running SR 8.0?

- If **yes**, go to Step 8.
- If **no**, go to the next step.

5 Enter the following command to open the **/etc/services** file in a text editor.

```
[admin@dtacs_50 ~]$ sudo vi /etc/services
```

6 Add the following entry to the file.

```
informixOnline 3010/tcp
```

7 Save and close the **/etc/services** file.

8 Open the **/etc/hosts** file in a text editor and add the following entry.

Command Syntax:

```
[EC_dncsatm_IP]     dncsatm dncs_host dncshost
```

Example:

```
204.123.1.49        dncsatm dncs_host dncshost
```

9 Save and close the file.

10 As **root** user, enter the following command to source the dtacs environment.

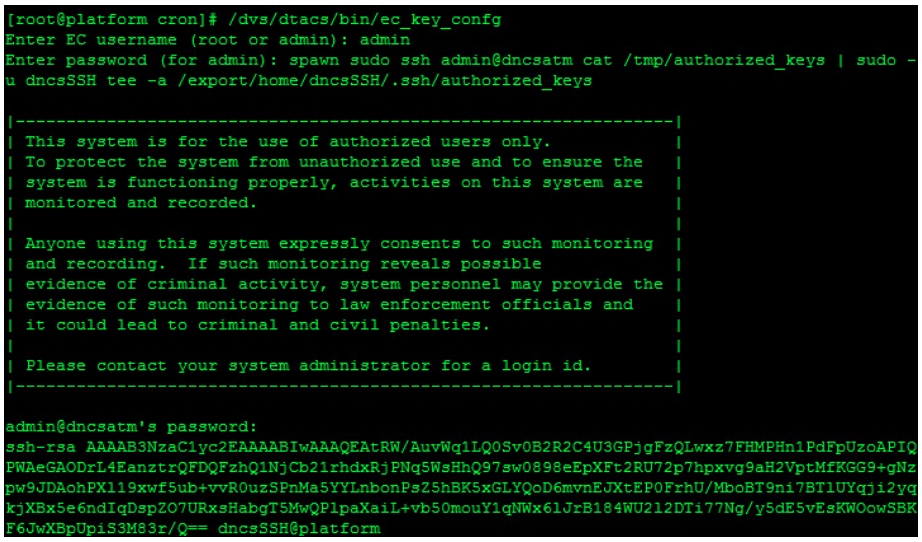
```
[root@dtacs_50 ~]# . /dvs/dtacs/bin/dtacsSetup
```

11 Enter the following command to create an SSH key authorization between the DTACS and the EC servers.

```
[root@dtacs_50 ~]# /dvs/dtacs/bin/ec_key_confg
```

12 When prompted for the username of the EC, type **admin** and press **Enter**.

13 When prompted for the password for the admin user on the EC, enter the password and press **Enter**. An SSH key is generated and saved to the /export/home/dncsSSH/.ssh/authorized_keys file on the EC server.



14 Go to the next procedure to configure the EC for DTACS.

Configuring the EC for DTACS

Important: This procedure is executed on the EC server.

1 As **root** user on the EC, enter the following command to edit the **onconfig** file.

EC SR 8.0:

```
[root@EC_80 ~]# vi /opt/cisco/informix/server/etc/onconfig
```

EC SR 7.x:

```
# /export/home/informix/etc/onconfig
```

2 Go to the **DBSERVERALIASES** entry.

3 Does the entry include a value for **dncsatmDbServer**?

- If **yes**, close the file and go to Step 6.
- If **no**, go to the next step.

4 Move to the **DBSERVERALIASES** entry and append **dncsatmDbServer**.

Example:

```
DBSERVERALIASES
demo_on,localhost_tcp,auto_tcp,dncsatmDbServer
```

5 Save and close the **onconfig** file.

6 Enter the following command to edit the **sqlhosts** file.

EC SR 8.0:

```
[root@EC_80 ~]# vi /opt/cisco/informix/server/etc/sqlhosts
```

EC SR 7.x:

```
# /export/home/informix/etc/sqlhosts
```

7 Move to the end of the file and add the following entry to the **sqlhosts** file if it does not exist.

EC SR 8.0:

```
dncsatmDbServer  onsoctcp  dncsatm  sqlexec
```

EC SR 7.x:

```
dncsatmDbServer  onsoctcp  dncsatm  informixOnline
```

8 Save and close the **sqlhosts** file.

9 Are you using EC SR 7.x?

- If **yes**, add the following entry in the **/etc/services** file and then go to the next step.

  ```
  informixOnline   3010/tcp
  ```

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

10 Enter the following command to source the environment.

```
[root@EC_80 ~]# . /dvs/dncs/bin/dncsSetup
```

11 Enter the following command to start the Informix listener for dncsatmDbServer.

```
[root@EC_80 ~]# onmode -P start dncsatmDbServer
```

12 Open the **/etc/hosts** file in a text editor and add the following entry.

Command Syntax:

```
[DTACS_dtacsatm_IP]  dtacsatm dtacshost dtacs
```

Command Example:

```
204.3.1.34  dtacsatm dtacshost dtacs
```

13 Save and close the **/etc/hosts** file.

14 Enter the following command to create the **hosts.equiv** file.

```
[root@EC_80 ~]# vi /etc/hosts.equiv
```

15 Add the following lines to the file.

Note: The first entry in each line must match the first entry for the DTACS IP in the /etc/hosts file.

Example: /etc/hosts file entry: 204.123.1.34 dtacsatm dtacs_host dtacshost

```
dtacsatm  dtacs
dtacsatm  dncs
dtacsatm  root
```

16 Save and close the file.

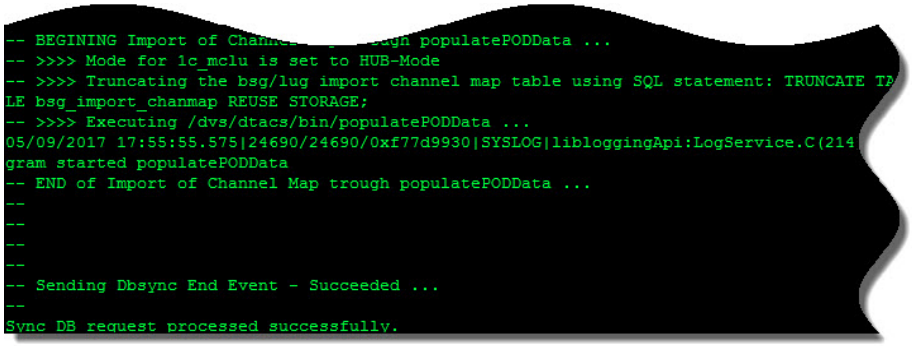
Testing Synchronization Between the DTACS and EC Databases

Complete the following steps to test synchronization between the DTACS and EC databases.

1 As **dncs** user on the DTACS, type the following command to test the database sync. A **Sync DB request processed successfully** message displays.

```
[dncs@dtacs_50 ~]$ dtacsdbsync -S
```

Example:



2 Was the database sync successful?

- If **yes**, go to the next section.
- If **no**, troubleshoot your system or contact Cisco Services.

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.

Note: The SFTP user you create can also be used to communicate with an AGI Adapter provided you have configured an AGI Adapter.

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@dtacs_50 ~]$ 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@dtacs_50 ~]$ 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@dtacs_50 ~]$ 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@dtacs_50 ~]$ 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@dtacs_50 ~]$ sudo chmod 0755 /dvs/sftpuser1
```

4 Enter the following command 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]
chown root:root /dvs/[SFTP-home-directory]
```

Example:

```
[admin@dtacs_50 ~]$ sudo mkdir /dvs/sftpuser1/uploads
[admin@dtacs_50 ~]$ sudo chown sftpuser1:sftpuser1
/dvs/sftpuser1/uploads
[admin@dtacs_50 ~]$ 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.

```
[admin@dtacs_50 ~]$ 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 Enter the following command to restart the **sshd** service.

```
[admin@dtacs_50 ~]$ 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 complete an SSH request as SFTP user.

   Command Syntax:

   ```
   sudo ssh [SFTP-username]@localhost
   ```

   Example:

   ```
   [admin@dtacs_50 ~]$ sudo ssh sftpuser1@localhost
   ```

2. Enter the following command to verify that you can successfully execute an SFTP file transfer.

   Command Syntax:

   ```
   sudo sftp[SFTP-username]@localhost
   ```

   Example:

   ```
   [admin@dtacs_50 ~]$ sudo sftp sftpuser1@localhost
   ```

3. When prompted, enter the password for the SFTP user. You are connected to local host and an sftp prompt displays.

4. At the **sftp>** prompt, type `dir`. Your SFTP upload directory should display. You should be able to read and write into the directory.

   Example:

   ```
   sftp> dir
   uploads
   sftp>
   ```

5. Attempt a file transfer to the directory.

Configuring DTACS BOSS Proxy (Optional)

Important: Skip this procedure if your system does not use a BOSS proxy.

The Billing System can be set to send BOSS transactions to the EC. The DTACS then forwards any non-DTA related transactions to the associated EC.

Complete the following procedure to configure DTACS BOSS proxy.

1 As **admin** user, type the following command and press **Enter** to change to the **/dvs/dtacs/etc** directory.

```
[admin@dtacs_50 ~]$ sudo cd /dvs/dtacs/etc
```

2 Type the following command and press **Enter** to determine whether the **bossServer.cfg** file exists.

```
[admin@dtacs_50 etc]$ ls -l bossServer.cfg*
```

3 Does the **bossServer.cfg** file exist?

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

4 Type the following command and press **Enter** to create a **bossServer.cfg** file using the sample configuration file provided.

```
[admin@dtacs_50 etc]$ sudo cp bossServer.cfg.sample
bossServer.cfg
```

5 Enter the following command to open the **bossServer.cfg** file in a text editor.

```
[admin@dtacs_50 etc]$ sudo vi bossServer.cfg
```

6 Update the **DNCS_BOSS_PROXYING** value to **1**. This enables DTACS to proxy non-DTA BOSS transactions to the EC.

Example:

```
DNCS_BOSS_PROXYING = 1
```

7 Save and close the **bossServer.cfg** file.

8 Type the following command and press **Enter** to view the ownership for the bossServer.cfg file.

```
[admin@dtacs_50 etc]$ ls -ltr bossServer.cfg
```

9 Does the system indicates the ownership as **dncs:dncs**?

- If **yes**, then the directory ownership is correct. You are finished with this procedure.
- If **no**, type the following command and press **Enter** to change the ownership to **dncs:dncs**.

```
[admin@dtacs_50 etc]$ sudo chown dncs:dncs bossServer.cfg
```

Restarting Apache and Tomcat Services

Apache and Tomcat services must be running to access the DTACS Web UI. Complete the following steps to restart these services and verify that they are running.

1 As **admin** user, enter the following commands to restart the Apache and Tomcat services.

```
[admin@dtacs_50 etc]$ sudo service tomcat restart
[admin@dtacs_50 etc]$ sudo service httpd-dncsws restart
[admin@dtacs_50 etc]$ sudo service httpd restart
```

2 Enter the following commands to check the status of each service.

```
[admin@dtacs_50 etc]$ sudo service tomcat status
[admin@dtacs_50 etc]$ sudo service httpd-dncsws status
[admin@dtacs_50 etc]$ sudo service httpd status
```

Note: If a service fails to start, please contact Cisco Services.

CentOS cron and anacrontab Overview

By default, CentOS includes the following three installed cron packages:

- cronie-[VERSION].x86_64
- cronie-anacron-[VERSION].x86_64
- crontabs-[VERSION].noarch

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 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.daily/logrotate
- /etc/cron.daily/makewhatis.cron
- /etc/cron.daily/mlocate.cron
- /etc/cron.daily/prelink
- /etc/cron.daily/readahead.cron
- /etc/cron.daily/tmpwatch
- /etc/cron.d/raid-check
- /etc/cron.d/sysstat
- /etc/cron.hourly/0anacron
- /etc/cron.monthly/readahead-monthly.cron

Verifying the crontab Entries Managed by cron

Verifying the crontab Entries

After upgrading, inspect the crontab file in the keyFiles.staging directory on the DTACS.

Important: All DTACS 4.1 cron jobs are not migrated over to cron. They are only copied to the staging directory.

Verifying User-Defined CRON Entries on the Migrated VM

Important: If this is a new DTACS installation, you can skip this procedure.

This procedure allows you to verify and update the user defined crontab entries for the dncs and root users. Complete the following procedure to verify user-defined cron entries.

1 As **root** user, enter the following command to view the staged root cron entries migrated from the DTACS SR 4.1 server.

```
[root@DTACS_50 httpd]# vi
/disk1/keyfiles_staging/var/spool/cron/crontabs/root
```

2 Copy and save any user-defined entries to a text file.

3 Close the file.

4 Enter the following command to change to the **/var/spool/cron** directory on the DTACS 5.0 system.

```
[root@DTACS_50 httpd]# cd /var/spool/cron
```

5 Type the following command to create the **root** crontab file.

```
[root@DTACS_50 cron]# crontab -e
```

6 Paste the cron entries you copied from Step 2 into this file.

7 Save and close the file.

8 Enter the following command to edit the **root** cron file on the DTACS 5.0 system.

9 Execute the following command and add user-defined jobs to the users crontab on the new DTACS 5.0 system.

```
[root@DTACS_50 cron]#
/disk1/keyfiles_staging/var/spool/cron/crontabs/[user]
```

10 Verify both of the entries.

Starting DTACS Processes

Complete the following steps to start the DTACS processes.

1 As **dncs** user, enter the following command and press **Enter** to start DTACS processes.

```
[dncs@dtacs_50 ~]$ dtacsStart
```

2 In a supported Firefox Web browser, enter the following URL.

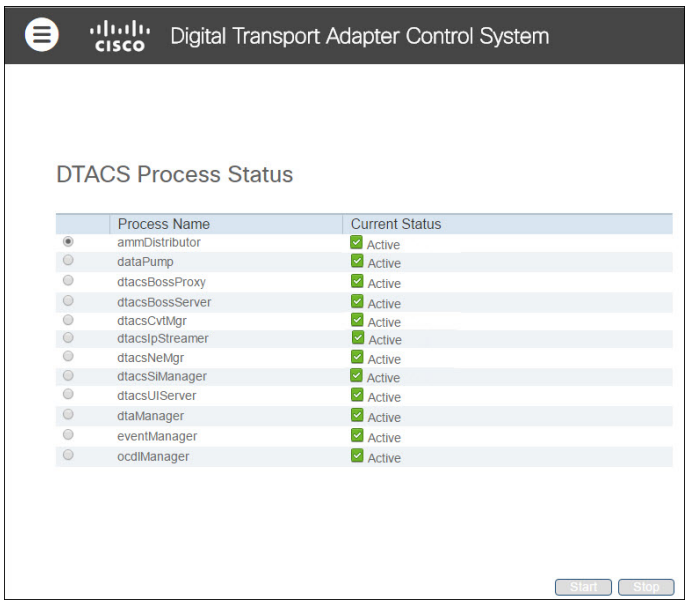
URL Syntax:

```
https://[DTACS_IP]
```

Example:

```
https://198.51.100.17
```

3 When prompted, enter the **dtacsadmin** user name and password, and then press **Enter**. The DTACS Process Status window appears.



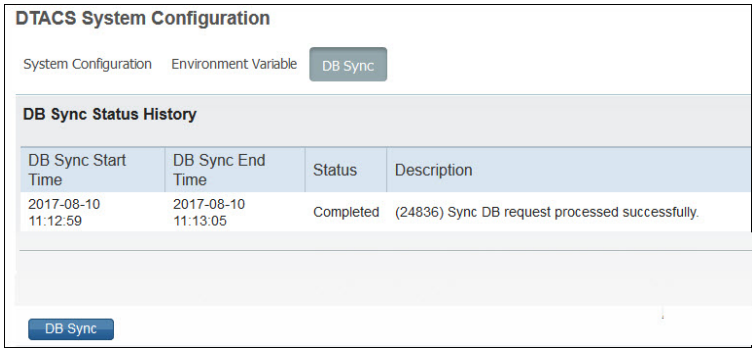
4 Monitor the processes as they come up.

- Green indicators replace red indicators as the DTACS processes start.
- All processes should turn green.

Testing dbsync from the DTACS Web UI

1. From the DTACS Web UI, click the **Navigation** icon, , and then select **System Provisioning > Sys Config**. The DTACS System Configuration window displays and includes a DB Sync List history table.
2. Click the **DB Sync** tab and then click the **DB Sync** button to initiate the DTACS database synchronization process. A **Sync Database Request Sent Successfully** message appears in the lower, right corner of the window.

   Note: The DB Sync Status history table is refreshed automatically every three seconds.
3. Check for the following synchronization status:
   - If the status is **Completed** and the entry in the DB Sync End Time column is current, the synchronization was successful.



   - If the status is **In Progress**, wait for a few seconds for the status to refresh.
   - If the status is **Failed** and if the description reveals that the synchronization is still in progress, repeat this procedure after a few seconds.

     Note: Contact Cisco Services if you are not able to synchronize the database successfully.

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 8.0 and DTACS 5.0***.

SCID Sharing Support Feature (Optional)

If you plan to enable the SCID (Simple Channel ID) Sharing feature on DTACS, the GQAM code on the associated EC ***must*** be version 4.7.0. If it is not version 4.7.0, you must download v4.7.0 to the GQAMs by resetting these devices from the EC system or from the front panel of the GQAMs.

Complete the following procedure to download the GQAM code from the EC to the GQAMs and to enable the SCID Sharing Support feature.

Important: Update the GQAM code ***prior*** to enabling the SCID Sharing Support feature.

1 Verify if v4.7.0 has been downloaded to the GQAMs on the EC system?

- If the GQAM code is v4.7.0, go to Step 3.
- If the GQAM code is ***not*** v4.7.0, go to the next step.

2 Reset the GQAMs using one of the following methods.

Note: For detailed steps to reset your GQAMs, refer to the "Reset the Modulators" section in the ***SR 8.0 Installation and Migration Guide***.

- From the EC Web UI
- From the front panel of the modulators
- From the command line using the auditQam utility

3 When the reset completes, contact Cisco Services to enable the SCID Sharing feature.

7

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..... 72
- Overview of the Replicated Database Package..... 73
- Setup Replicated Database 75
- Configure RepDB 80
- Post RepDB Verifications..... 90

Prerequisites for RepDB

Important: Your system environment must have a second UCS platform with VMware installed and a DTACS 5.0 virtual machine configuration.

- ESXi host standalone license or vCenter server license.
- VMware vSphere client, login and connection to the VMware vSphere Hypervisor ESXi 5.5 or later.
- Network connectivity between the operational DTACS server and the new virtual machine.
- Use the existing network ports (vSwitches) that were defined when installing or migrating the DTACS 5.0 server.
  - DTACS 5.0 Mapping
    - NET0 – vSwitch0 – Corp/Engineering Network

    Important: By default, DHCP is enabled on the eth0 NET0-vSwitch0-Corp network. If DHCP is not available, then static a IP address, netmask, gateway, and DNS information is required.
    - NET1 – vSwitch1 – Headend (HE) Network
    - NET2 - vSwitch2 - RepDB Network

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), the secondary server 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.

Setup Replicated Database

Important: If you are using a vSphere ESXi client to deploy VMs, refer to ***Setting Up RepDB Using an ESXi Client*** (on page 123).

This section provides instructions to set up RepDB by cloning the primary VM into a secondary 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 DTACS updates are suspended during the cloning process
  - Go to ***Cloning When the Primary VM is Shutdown*** (on page 75)
- **Cloning while the Primary VM is powered on and running**
  - Cloning may cause DTACS performance issues depending on the size of the system
  - The primary DTACS will be processing transactions without the interruption of interactive services
  - Go to ***Cloning While the Primary VM is Running*** (on page 77)

Cloning When the Primary VM is Shutdown

Note: In this example, HOSTA is the primary DTACS.

1 As **admin** user on the *primary* DTACS, 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@berlin ~]$ sudo vi /etc/hosts
```

2 Save and close the file.

3 Enter the following command to verify the RepDB entries.

```
[admin@berlin ~]$ less /etc/hosts | grep -i host
```

Example Output:

```
172.16.3.131   HOSTA
172.16.3.132   HOSTB
```

4 As **dncs** user, type the following commands to stop DTACS processes.

   a `dtacsStop`

   b `dtacsKill`

5 Disable all DTACS billing interfaces.

6 From the **root** terminal window, type the following command to shutdown the *primary* DTACS.

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

7 From the VMware vSphere Web UI, right-click the *primary* server and select **Clone to Virtual Machine**. The Clone Existing Virtual Machine window appears.

8 From the **Enter a name for the virtual machine** text box, enter a name for the *secondary* host.

9 Select the appropriate datastore and then click **Next**.

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 appears.

12 Ensure the following settings exist and then click **Next**. The Select clone option window appears.

   - The "Select virtual disk format" field is set to **Same format as source**.
   - The correct datastore is selected.

13 Click **Next** again.

14 Review the settings and then click **Finish**.

15 Monitor the **Recent Tasks** area to verify that the cloned VM completed successfully.

16 When the VM clone completes, select and right-click the *primary* VM and select **Power On**.

17 From a terminal window, login as **dtacsadmin**.

18 As **dncs** user, type the following command to start the DTACS processes.

```
[dncs@berlin ~]$ dtacsStart
```

19 Go to ***Configure the Secondary Host After Cloning*** (on page 78).

Cloning While the Primary VM is Running

Complete the following steps to clone HOSTA while the *primary* VM is running.

Note: In this example, HOSTA is the *primary* DTACS.

1. As **admin** user on the *primary* DTACS, 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@berlin ~]$ sudo vi /etc/hosts
   ```

2. Save and close the file.
3. Enter the following command to verify the RepDB entries.

   ```
   [admin@berlin ~]$ less /etc/hosts | grep -i host
   ```

   Example Output:

   ```
   172.16.3.131   HOSTA
   172.16.3.132   HOSTB
   ```

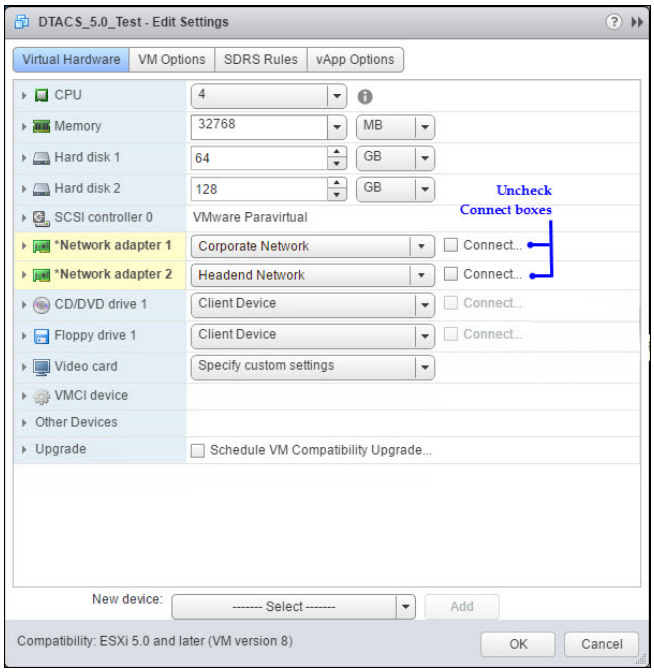
4. From the VMware vSphere Web UI, right-click the *primary* server and select **Clone to Virtual Machine**. The Clone Existing Virtual Machine window appears.
5. From the **Enter a name for the virtual machine** text box, enter a name for the *secondary* host.
6. Select the appropriate datastore and then click **Next**.
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 appears.
9. Ensure the following settings exist and then click **Next**. The Select clone option window appears.
   - The "Select virtual disk format" field is set to **Same format as source**.
   - The correct datastore is selected.
10. Click **Next** again.
11. Review the settings and then click **Finish**.
12. Monitor the **Recent Tasks** area to verify that the cloned VM completed successfully.
13. When the VM clone completes, go to the next section.

Configure the Secondary Host After Cloning

1 From the vSphere Web UI, right-click the *secondary* VM and select **Edit Settings**.

2 Uncheck the **Connect** box for all Network adapters.

Note: If this is ***not*** a new install and a Network adapter 3 interface is present, uncheck the **Connect** box for that adapter as well.



3 Click **OK**.

4 Monitor the **Recent Tasks** area until the *secondary* VM is successfully reconfigured.

5 Right-click the *secondary* VM and select **Power On**.

6 Right-click the *secondary* VM again and click **Open Console**.

7 In the console window, login as **admin** user.

8 Enter the following command to remove the **70-persistent-net.rules** file.

```
[admin@berlin ~]$ sudo rm
/etc/udev/rules.d/70-persistent-net.rules
```

9 When prompted to confirm the removal of the file, type **y**.

```
[root@berlin rules.d]# rm /etc/udev/rules.d/70-persistent-net.rules
rm: remove regular file `/etc/udev/rules.d/70-persistent-net.rules'? y
[root@berlin rules.d]#
```

10 Enter the following command to verify that the interfaces are mapped correctly.

Note: If this is ***not*** a new install, the output will also include an entry for ifcfg-eth2.

```
[admin@berlin ~]$ ls -latr
/etc/sysconfig/network-scripts/ifcfg*
```

```
-rw-r--r--. 1 root root 113 Aug 11 09:42 /etc/sysconfig/network-scripts/ifcfg-lo:1
-rw-r--r--. 1 root root 120 Aug 11 09:42 /etc/sysconfig/network-scripts/ifcfg-eth1
-rw-r--r--. 1 root root 162 Aug 11  2017 /etc/sysconfig/network-scripts/ifcfg-eth0
-rw-r--r--. 1 root root 254 Aug 11  2017 /etc/sysconfig/network-scripts/ifcfg-lo
```

11 Do you want the *secondary* VM accessible remotely and/or the Admin Node to only be reachable on the Corporate Network?

- If **yes**, go to the next step.
- If **no**, go to Step 17.

12 Enter the following command to open the **ifcfg-eth0** file in a text editor.

```
[admin@berlin ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-eth0
```

13 From the **IPADDR** line, modify the IP address as it should be unique to the IP address of the primary VM.

14 Save and close the file.

15 Open the **/etc/hosts** file in a text editor and update the IP to the IP address you entered in Step 13.

16 Save and close the file.

17 Enter the following command to verify if an **ifcfg-eth2** file is present? If present, this configuration file represents the RepDB network.

```
[admin@berlin ~]$ ls -ltr
/etc/sysconfig/network-scripts/ifcfg-eth2
```

18 Is the **ifcfg-eth2** file present?

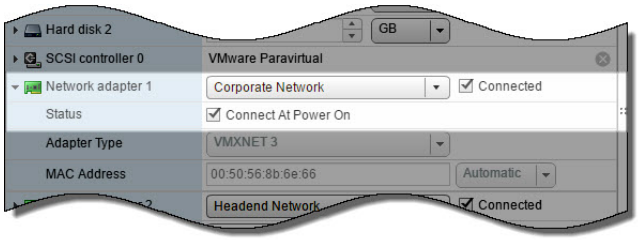
- If **no**, go to the next step.
- If **yes**, enter the following command to update the IP address to the IP for the *secondary* RepDB server. Then save and close the file and go to the next step.

  ```
  [admin@berlin ~]$ sudo vi
  /etc/sysconfig/network-scripts/ifcfg-eth2
  ```

19 From the vSphere Web UI, right-click the *secondary* VM and select **Edit Settings**.

20 From the **Network adapter 1** (corporate network) row, click the **Connected** and the **Connect At Power On** boxes and then click **OK**.

Note: If Network adapter 2 (RepDB network) is present, make sure to click the **Connected** and the **Connect At Power On** boxes for that entry as well.



21 From the console window, type **reboot** to reboot the *secondary* server.

22 From a terminal window, log into the *secondary* VM as **admin** user.

23 Enter the following command to verify that the interfaces are mapped properly.

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

24 Go to ***Configure RepDB*** (on page 80).

Configure RepDB

Complete the following procedures to configure the RepDB network on the primary and the secondary servers.

Adding the RepDB Network Adapter on the Primary and Secondary VMs

Complete the following procedure to add a network adapter for RepDB to the primary and the secondary DTACS.

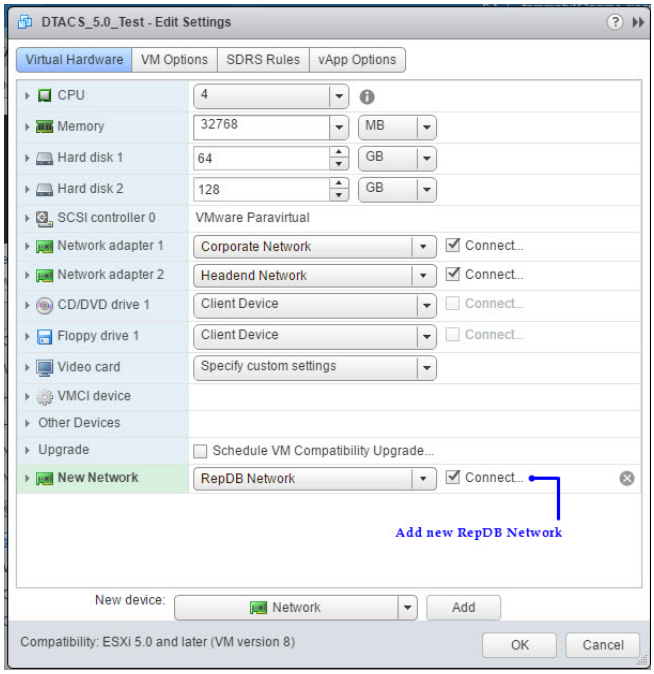
1 From the vSphere Web UI, right-click the *primary* VM and select **Edit Settings**.

2 From the **New device** dropdown menu, select **Network** and then click **Add**. A New Network entry is added to the list of Virtual Hardware.

3 From the **New Network** dropdown menu, select the appropriate replicated database network label.

4 Ensure the **Connect** check box is selected.

Example: Primary DTACS



5 Click **OK**. The VM is reconfigured.

6 Monitor the **Recent Tasks** area until the task is completed.

7 Right-click the *secondary* VM and select **Edit Settings**.

8 From the **New device** dropdown menu, select **Network** and then click **Add**. A New Network entry is added to the list of Virtual Hardware.

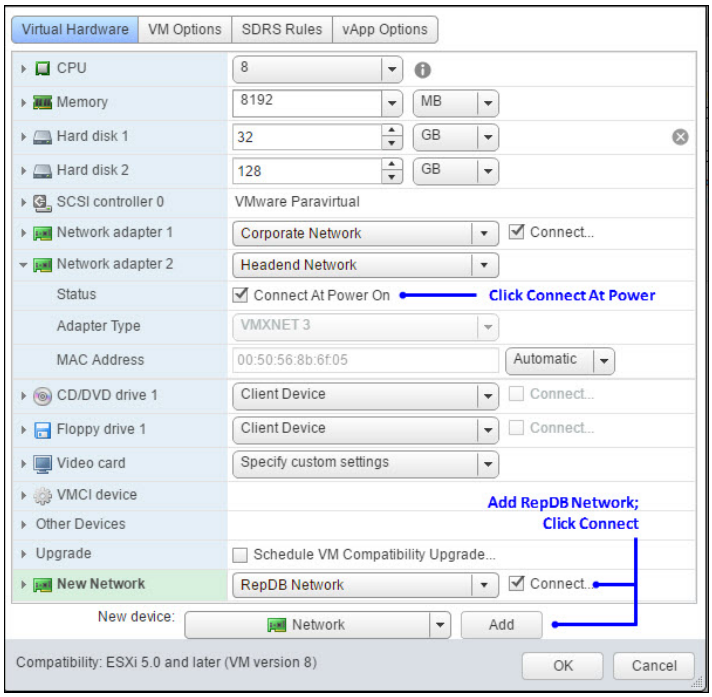
9 From the **New Network** dropdown menu, select the label for the replicated database network.

10 Ensure the **Connect** check box is selected.

11 Click the arrow adjacent to **Network adapter 2**. The configuration for the adapter displays.

12 Click the **Connect At Power On** check box.

Example: Secondary DTACS



13 Click **OK**. The VM is reconfigured.

14 Monitor the **Recent Tasks** area until the task is completed.

15 Did you execute an upgrade from DTACS 5.0.x to DTACS 5.0.y?

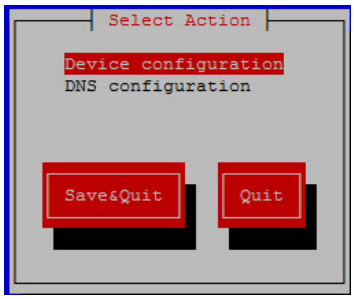
- If **no**, go to the next section.
- If **yes**, go to *Enabling RepDB* (on page 87).

Creating an Interface Configuration File for RepDB

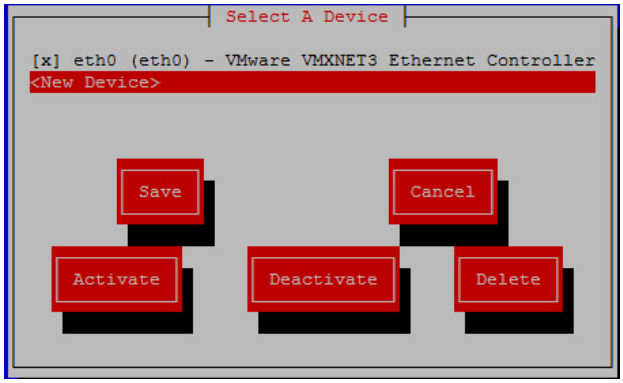
Complete the following steps to add a network interface for RepDB.

1 As **admin** user on the *primary* DTACS, enter the following command to configure the RepDb (eth2) interface. The Select Action window displays.

```
[admin@berlin ~]$ sudo system-config-network
```

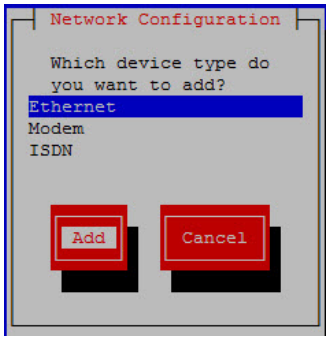


2 With Device configuration selected, press **Enter**. The Select a Device window displays.



3 Press the down arrow key on your keyboard to highlight **<New Device>** and then press **Enter**. The Network Configuration window displays.

4 With **Ethernet** highlighted, press the **Tab** key until **Add** is highlighted; then press **Enter**.



5 In the **Name** text box, type **eth2** and then press **Tab**.

6 In the **Device** text box, type **eth2** and then press **Tab** twice.

7 In the **Static IP** field, type the IP address for the RepDb interface and then press **Tab**.

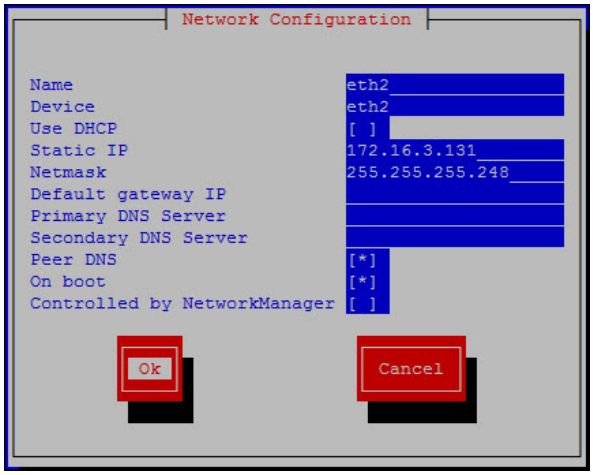
8 In the **Netmask** field, type the netmask for the RepDb interface.

9 Press the **Tab** key until your cursor is in the **Peer DNS** field.

10 Press the **spacebar** to select this option. An asterisk, *, appears in the field.

11 Press the **Tab** key until your cursor is in the **On boot** field.

12 Press the **spacebar** to select this option. An asterisk, *, appears in the field.



13 Press the **Tab** key until the **Ok** button is highlighted and then press **Enter**. You are returned to the Select a Device window.

14 Press the **Tab** key until **Save** is highlighted and then press **Enter**. You are returned to the Select Action window.

15 Press the **Tab** key until **Save&Quit** is highlighted and then press **Enter**. The network configuration menu closes and you are returned to the admin user prompt.

16 Open the **ifcfg-eth2** file in a text editor.

```
[admin@berlin ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-eth2
```

17 Delete the **HWADDR** line.

18 Save and close the file.

19 Enter the following command to bring the eth2 interface up.

```
[admin@berlin ~]$ sudo /etc/sysconfig/network-scripts/ifup
eth2
```

20 Repeat Steps 1 through 19 on the *secondary* DTACS.

Note: Make sure you define the IP address for the *secondary* DTACS.

21 Test the connection between the hosts.

On HOSTA

```
[admin@berlin ~]$ ping HOSTB
```

On HOSTB

```
[admin@berlin ~]$ ping HOSTA
```

22 Can the two hosts ping each other?

- If **yes**, go to the next procedure.
- If **no**, go back over the steps in this procedure to review configurations and settings.

Setting Up SSH Login Between the DTACS Servers Without a Password

Complete this procedure to setup password-less SSH access between the primary and the secondary DTACS. This will enable RepDB features to function properly.

1 As **admin** user on the *primary* DTACS, 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 /export/admin/.ssh directory.

```
[admin@berlin ~]$ ssh-keygen
```

2 When prompted for the location to save the key, press **Enter** to accept the default.

3 Did an **Overwrite (y/n)?** message display?

- If **yes**, enter **y** and press **Enter**. Then go to the next step.
- If **no**, go to the next step.

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.

```
[admin@berlin ~]$ ssh-keygen <-----generate keys
Generating public/private rsa key pair.
Enter file in which to save the key (/home/admin/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/admin/.ssh/id_rsa.
Your public key has been saved in /home/admin/.ssh/id_rsa.pub.
The key fingerprint is:
b4:7e:0c:43:b6:07:be:e1:f2:13:ee:22:59:74:42:13 admin@berlin
The key's randomart image is:
+--[ RSA 2048]----+
|      E.         |
|      o          |
|     . .=        |
|      o=.+       |
|     . oS .      |
|      .o.B       |
|     o..+.o      |
|    o .oo.       |
|     . oo.       |
+-----------------+
```

6 Enter the following command to copy the keys to the *secondary* DTACS.

Note: The authorized_keys file is saved in the /home/admin/.ssh directory on the remote server.

Command Syntax:

```
ssh-copy-id [secondary_hostname]
```

Example:

```
[admin@berlin ~]$ 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.

```
[admin@berlin ~]$ ssh-copy-id HOSTB <-----Copy the keys to HOSTB
The authenticity of host 'hostb (172.16.3.132)' can't be established.
RSA key fingerprint is 07:a7:d6:24:ca:6d:38:1f:8b:0d:06:83:77:cb:f5:fc.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'hostb,172.16.3.132' (RSA) to the list of known hosts.

|----------------------------------------------------------------------|
| This system is for the use of authorized users only.                 |
| To protect the system from unauthorized use and to ensure the        |
| system is functioning properly, activities on this system are        |
| monitored and recorded.                                              |
|                                                                      |
| Anyone using this system expressly consents to such monitoring       |
| and recording.  If such monitoring reveals possible                  |
| evidence of criminal activity, system personnel may provide the      |
| evidence of such monitoring to law enforcement officials and         |
| it could lead to criminal and civil penalties.                       |
|                                                                      |
| Please contact your system administrator for a login id.             |
|----------------------------------------------------------------------|

admin@hostb's password:
Now try logging into the machine, with "ssh 'HOSTB'", and check in:

  .ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.
```

9 Enter the following command on the *primary* host to test the password-less SSH connection to the secondary host.

```
[admin@berlin ~]$ ssh HOSTB
```

Result: You are logged into the *secondary* host without having to enter a password.

10 Type **exit** to close the session.

11 Repeat Steps 1 through 10 on the *secondary* DTACS.

Copying the SSH Keys Between the DTACS and the EC Servers

Complete the following procedure to exchange the SSH keys generated on each DTACS server to the appropriate EC server, as well as to exchange the SSH keys on each EC server to the appropriate DTACS server. This will enable proper communication of the database between the EC and DTACS servers.

1 On the *primary* DTACS, enter the following command to copy the SSH key to the *primary* EC. An **Are you sure you want to continue connecting (yes/no)?** message displays.

Command Syntax:

```
ssh-copy-id [primary_EC_IP]
```

Example:

```
[admin@dtacsA_berlin ~]$ ssh-copy-id 10.90.167.95
```

2 Enter **y** and press **Enter**.

3 Enter the following command to test the connection from the *primary* DTACS and *primary* EC.

Command Syntax:

```
ssh [primary_EC_IP]
```

Example:

```
[admin@dtacsA_berlin ~]$ ssh 10.90.167.95
```

Result: You are logged into the *primary* EC without having to enter a password.

4 From the *primary* EC that you are SSH'd into, enter the following command to copy it's SSH keys to the *primary* DTACS server.

Command Syntax:

```
ssh-copy-id [primary_DTACS_IP]
```

Example:

```
[admin@ecA_berlin ~]$ ssh-copy-id 10.90.167.53
```

Result: You are logged into the *primary* DTACS without having to enter a password.

5 Type **exit** and then type **exit again** to return to the original *primary* DTACS session.

6 As **admin** user on the *secondary* DTACS, enter the following command to copy the SSH key to the *secondary* EC. An **Are you sure you want to continue connecting (yes/no)?** message displays.

Command Syntax:

```
ssh-copy-id [secondary_EC_IP]
```

Example:

```
[admin@dtacsB_berlin ~]$ ssh-copy-id 10.90.167.93
```

7 Enter **y** and press **Enter**.

8 Enter the following command to test the connection from the *secondary* DTACS and *secondary* EC.

Command Syntax:

```
ssh [secondary_EC_IP]
```

Example:

```
[admin@dtacsB_berlin ~]$ ssh 10.90.167.93
```

Result: You are logged into the *secondary* EC without having to enter a password.

9 From the *secondary* EC that you are SSH'd into, enter the following command to copy it's SSH keys to the *secondary* DTACS server.

Command Syntax:

```
ssh-copy-id [secondary_DTACS_IP]
```

Example:

```
[admin@ecB_berlin ~]$ ssh-copy-id 10.90.167.52
```

Result: You are logged into the *secondary* DTACS without having to enter a password.

10 Type **exit** and then type **exit again** to return to the original *secondary* DTACS session.

Enabling RepDB

Complete the following steps to enable RepDB.

1 As **admin** user on the *primary* DTACS, enter the following command to change to the **/opt/cisco/repdb** directory.

```
[admin@berlin ~]$ cd /opt/cisco/repdb
```

2 Enter the following command to configure RepDB.

```
[admin@berlin repdb]$ sudo ./configRepDb
```

Note: This can take up to 30 minutes or more, depending on the size of the database.

3 When prompted for the hostname of the *primary* node, enter the hostname (i.e. HOSTA) of the *primary* system's RepDB interface.

4 When prompted for the hostname of the *secondary* node, enter the hostname (i.e. 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.

```
[admin@berlin repdb]# sudo ./configRepDb
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
Secondary hostname: HOSTB

Primary: HOSTA
Primary IP:172.16.3.131
Secondary: HOSTB
Secondary IP:172.16.3.132

Continue with these host settings? (y/n): y
```

5 Verify that the entries are correct and when prompted to continue, type **y**.

Results: The RepDB environment is set up on the primary and the secondary hosts.

6 When prompted to run formatDbSpace on the *secondary* DTACS, type **y** and press **Enter**. The database setup begins and, if active database sessions are found, you are prompted to kill them.

7 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.

8 Observe the output and verify that Database Replication is successfully enabled on both systems and a **Replication has been SUCCESSFULLY ENABLED** message displays.

```
##############################################################################
# NOTICE * NOTICE * NOTICE * NOTICE * NOTICE * NOTICE * NOTICE * NOTICE * #
##############################################################################
Enabling database replication on HOSTA.
Successfully enabled Database Replication on HOSTA.
```

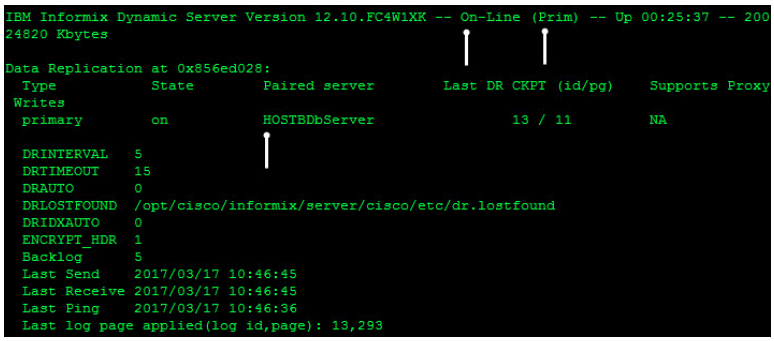
```
##############################################################################
# NOTICE * NOTICE * NOTICE * NOTICE * NOTICE * NOTICE * NOTICE * NOTICE * #
##############################################################################
Enabling database replication on HOSTB.
Successfully enabled Database Replication on HOSTB.
Created file /etc/no_system_start on the system.
Completed all tasks.
Database Replication has been ENABLED for the secondary server.
```

```
Replication has been SUCCESSFULLY ENABLED.
```

9 As **root** user, source the environment variables.

10 Type the following command and press **Enter** on the *primary* server. The output should indicate that the database is **On-Line (Prim)** and data replication is paired to the secondary server.

```
[root@berlin repdb]$ onstat -g dri
```



11 Repeat Step 9 on the *secondary* DTACS. The output should indicate that the database is **Read-Only (Sec)** and is paired to the primary server.

12 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@berlin repdb]# /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.

```
[root@berlin repdb]# ./checkRepDb
PING HOSTB (172.16.3.132) 56(84) bytes of data.
64 bytes from HOSTB (172.16.3.132): icmp_seq=1 ttl=64 time=0.337 ms
64 bytes from HOSTB (172.16.3.132): icmp_seq=2 ttl=64 time=0.303 ms

--- HOSTB ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.303/0.320/0.337/0.017 ms
RepDb: Primary=HOSTADbServer (HOSTA), Secondary=HOSTBDbServer (HOSTB)
RepDb: Secondary is behind 0 log(s) at Fri Mar 17 10:59:10 EDT 2017
RepDb: PrimaryLog=13 (2.49% used), SecondaryLog=13 (2.48% used)
```

2 Repeat Step 1 on the *secondary* server.

Note: Ensure that you change to the /opt/cisco/repdb directory on the *secondary* server to run the checkRepDb script.

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@berlin repdb]# crontab -l
```

Command Syntax:

```
15,45 * * * * /opt/SAIrepdb/syncKeyFiles -l [PRIMARY HOSTNAME]
-r [SECONDARY HOSTNAME] -n > /var/log/syncKeyFiles.out 2>&1
```

Example Output:

```
15,45 * * * * /opt/SAIrepdb/syncKeyFiles -l HOSTA -r HOSTB
-n > /var/log/syncKeyFiles.out 2>&1
```

2 Type the following command to verify the last modification time of the output from the syncKeyFiles crontab entry. The date and time should be several minutes after the passage of the syncKeyFiles cron event.

```
[root@berlin repdb]# ls -l /var/log/syncKeyFiles.out
```

3 Type the following command to view the output from the crontab entry. The status of the primary and secondary VMs and the ssh/scp between the servers is displayed.

```
[root@berlin repdb]# cat /var/log/syncKeyFiles.out
```

4 Review the KeyFiles2Sync log file to further check the status of the key file sync,

```
[root@berlin repdb]# less /var/log/KeyFiles2Sync.log
```

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@berlin 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.

4 Type the following command on the *primary* server to edit the KeyFiles2Exclude.list file in a text editor.

```
[root@berlin repdb]# vi /opt/cisco/repdb/KeyFiles2Exclude.list
```

5 Add or delete any unique files, as needed.

6 Save and close the file.

A

Hardware Configuration Procedures for the Cisco UCS C240

Introduction

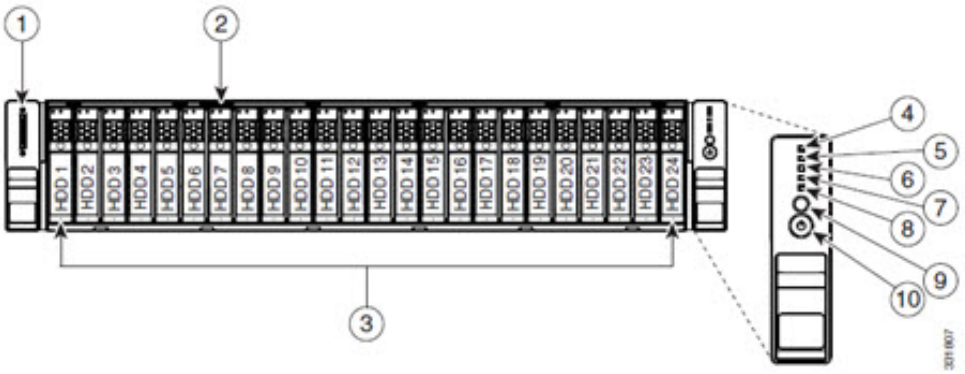
This chapter contains procedures for configuring Cisco's UCS C240 M3 and UCS C240 M4 server for use with System Release 5.0.

In This Appendix

- Hardware Diagram of the Cisco UCS C240 M3 Server 94
- Hardware Diagram of the Cisco UCS C240 M4 Server 97
- Hardware Requirements for a New UCS Install 100
- Cisco UCS C240 Server CIMC Configuration 101
- Cisco UCS C240 Host Configuration 102
- RAID Configuration.....103
- ESXi Installation 113
- Configure the VM Host 119

Hardware Diagram of the Cisco UCS C240 M3 Server

Chassis Front View

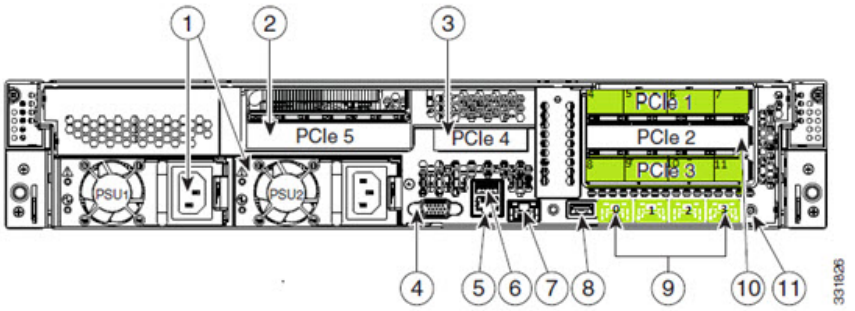


Slot	Description	Slot	Description
1	KVM connector (Used with KVM cable that provides two USB, one VGA, and one serial connector)	6	Temperature status LED
2	Asset tag (serial number)	7	Fan status LED
3	Drives (up to 24 2.5-inch hot-swappable drives)	8	System status LED
4	Network link activity LED	9	Identification 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.

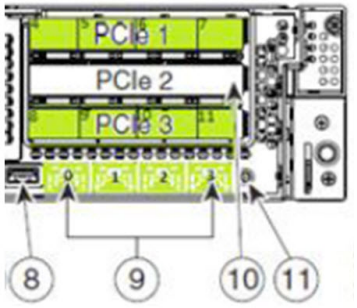
Note: Only the essential features of the rear panel are shown. A more detailed image follows.



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

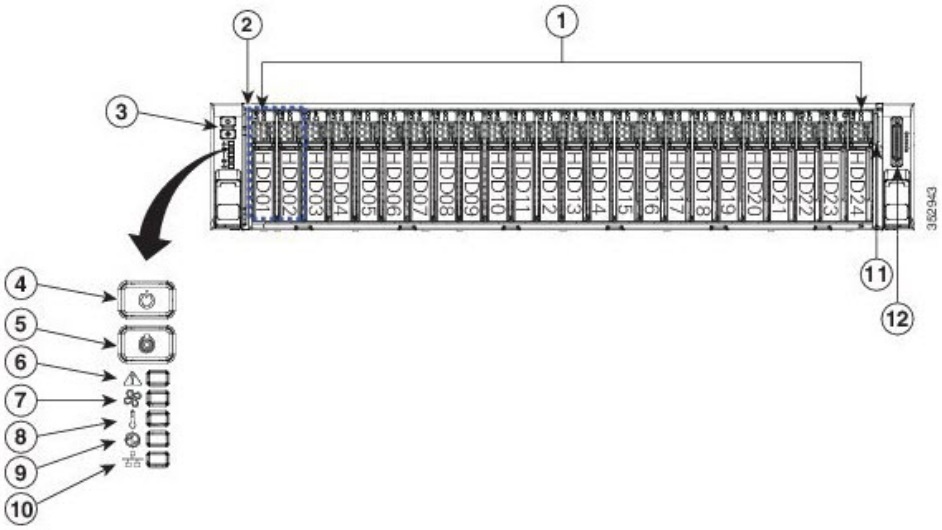
Network ports are numbered and marked as green. Cables should be run to the below designated ports.

- 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

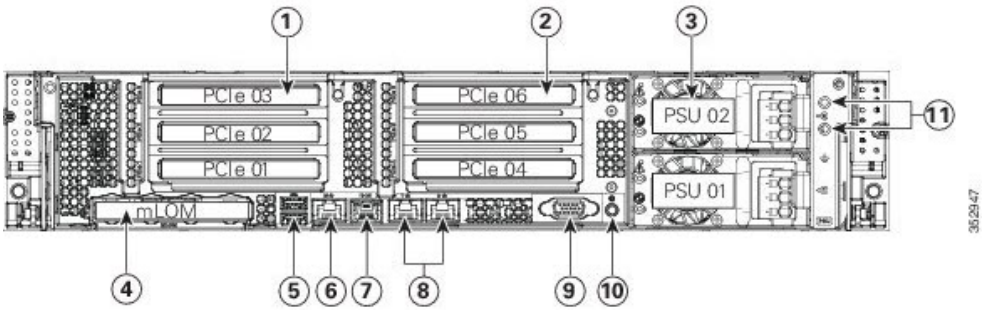


Slot	Description	Slot	Description
1	Drive bays 1-24 supports SAS/SATA drives	7	Fan status LED
2	Drive bays 1 and 2 supports NVMe PCIe SSDs and SAS/SATA drives	8	Temperature status LED
3	Operations panel buttons and LEDS Drives (up to 24 2.5-inch hot-swappable drives)	9	Power supply status LED
4	Power 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*** (on page 2).

- 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:

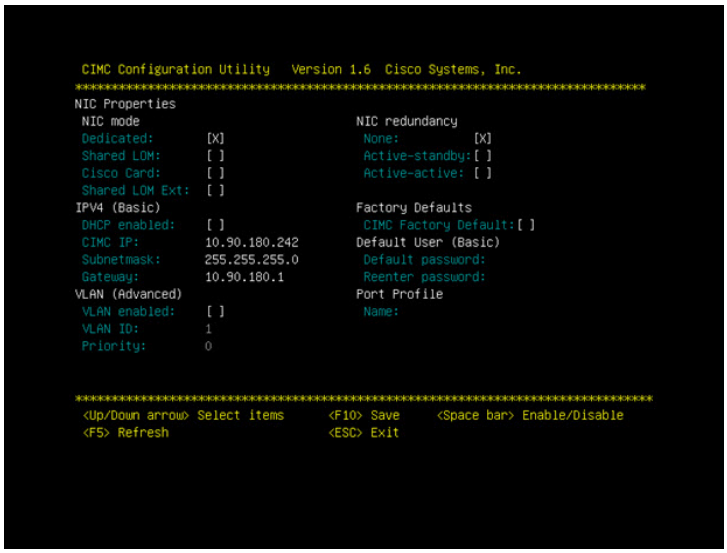
- This procedure is used for both the C240 M3 and C240 M4 servers and only needs to be performed once — when you initially install the server.
- Make sure that you use configuration data that pertains to the system that you are migrating. The screen-capture in Step 5 is to be referenced as an example 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 101)) 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 103)
- *Configuring RAID for UCS C240 M4 Servers* (on page 110)

Configuring RAID for UCS C240 M3 Servers

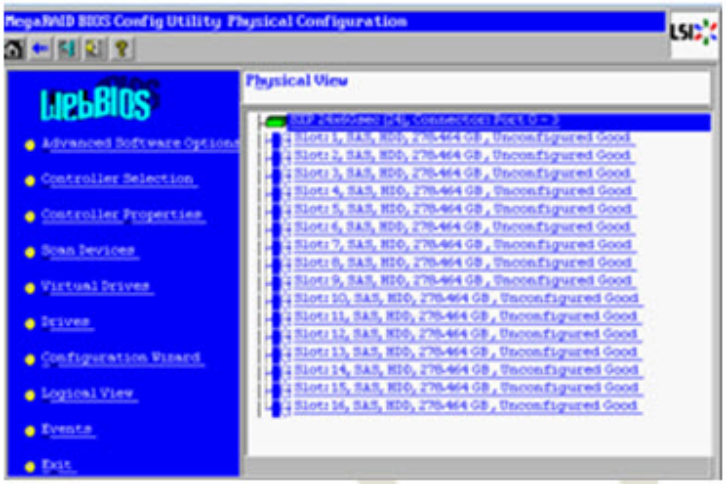
Important: This procedure only needs to be performed once — when you initially install the UCS C240 server.

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.

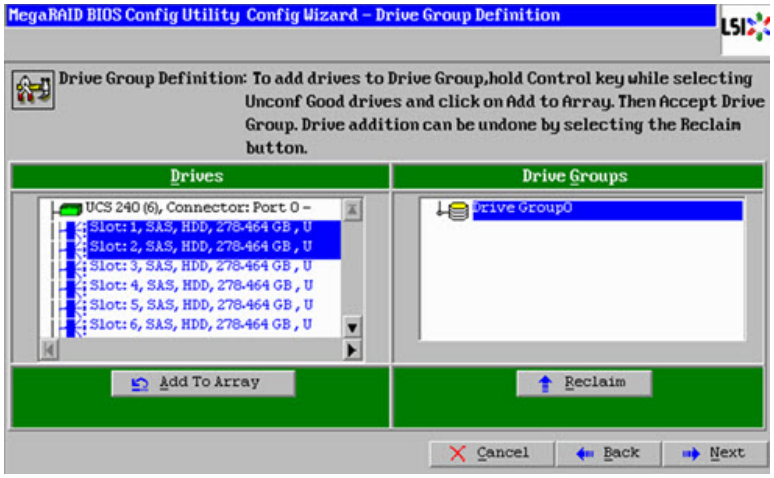
5 Click **New Configuration** and click **Next**. The utility prompts you to clear the existing configuration.

6 Click **Yes**.

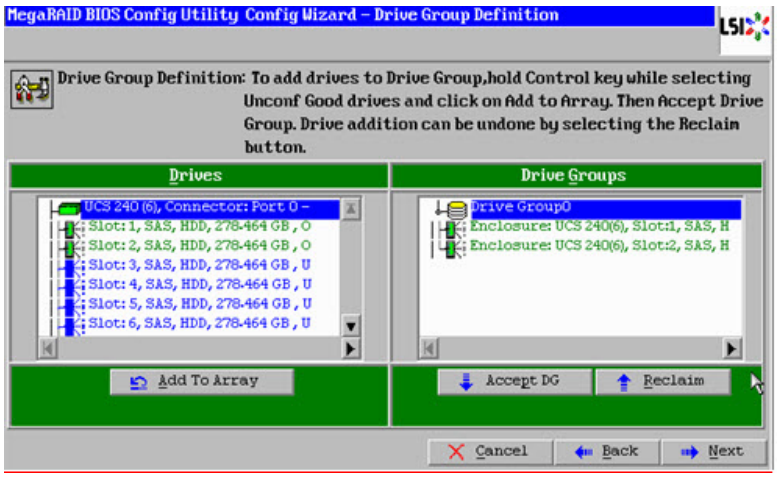
7 Click **Manual Configuration** and click **Next**. The Drive Group Definition screen appears.

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

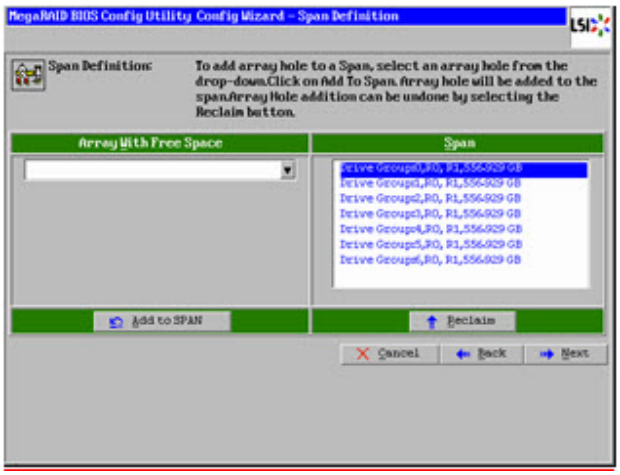
Slots 13 and 14

Result: The system creates a drive group for each pair.

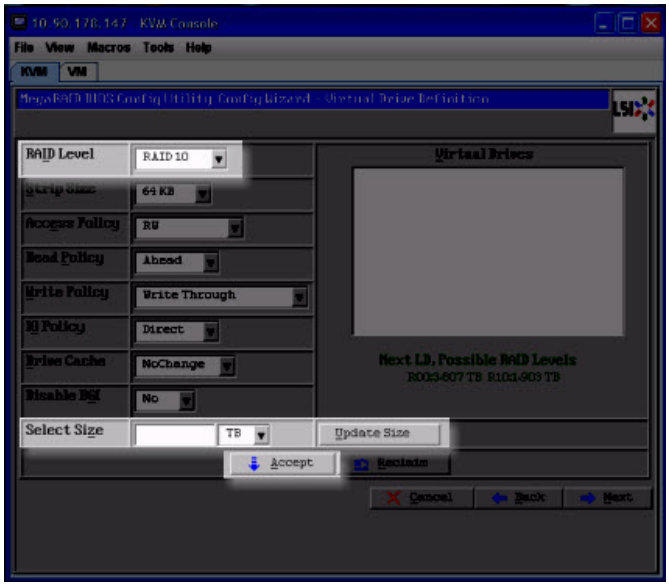
Note: When you complete this step, you should have 7 drive groups (0 - 6).

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.

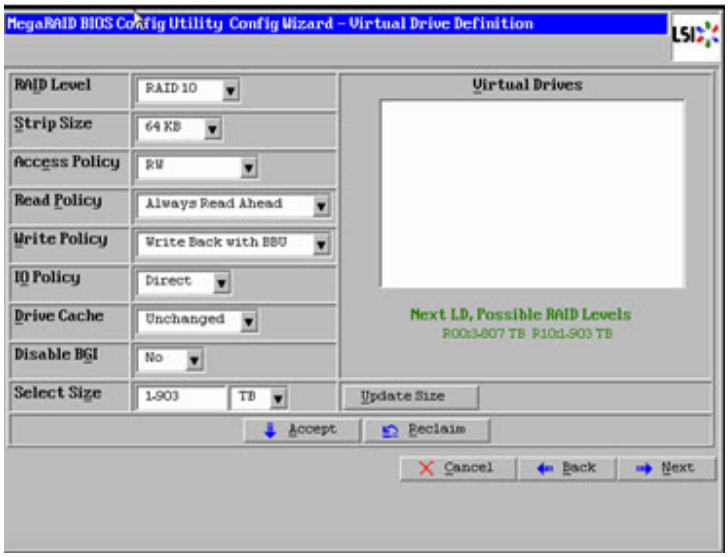


14 Click **Next**. The Virtual Drive Definition window appears.



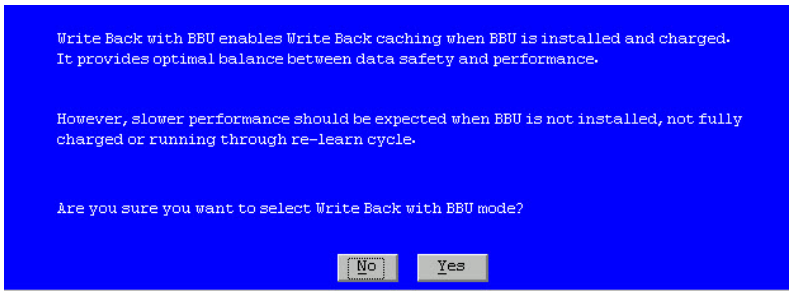
15 Select **RAID 10** from the RAID Level drop-down menu.

16 Click **Update Size**. The maximum allowed size for the selected RAID level populates the **Select Size** field.

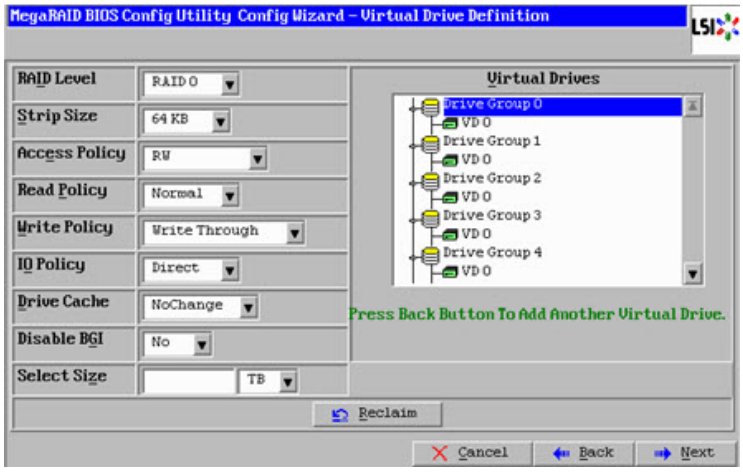


17 Record the **Select Size** here: _____

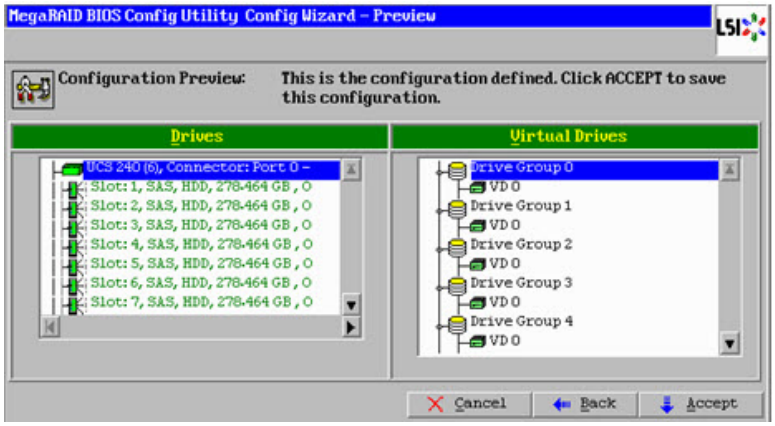
18 Click **Accept**. The Write Policy window appears.



19 Click **Yes** to confirm the default write policy. The total list of Vdisks created from Drive Groups 0-6 appears.

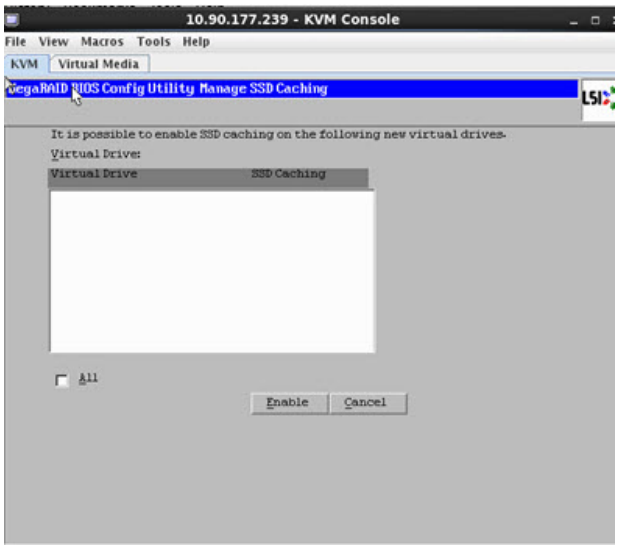


20 Click **Next**.

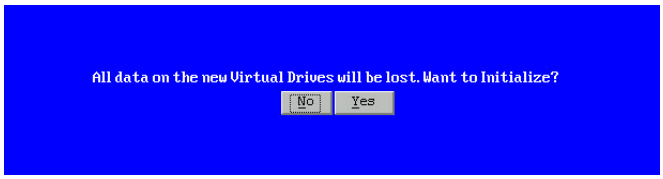


21 Examine the configuration preview to verify that the virtual drives match the previous list and click **Accept**. The system prompts to confirm saving the configuration.

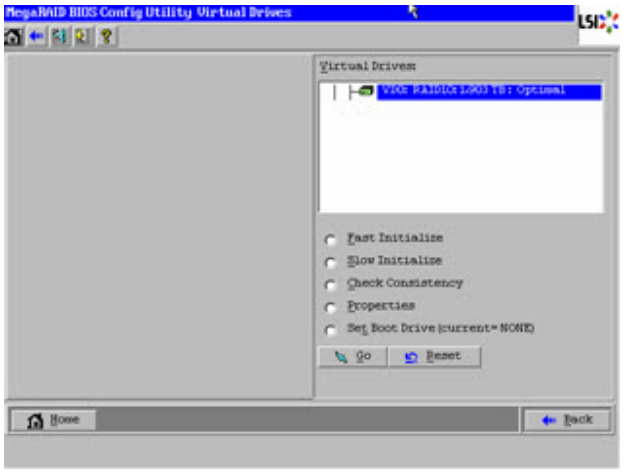
22 Click **Yes**. A warning message appears and indicates that you may lose data.



Note: After canceling the previous screen, you are prompted to initialize the new virtual drives.

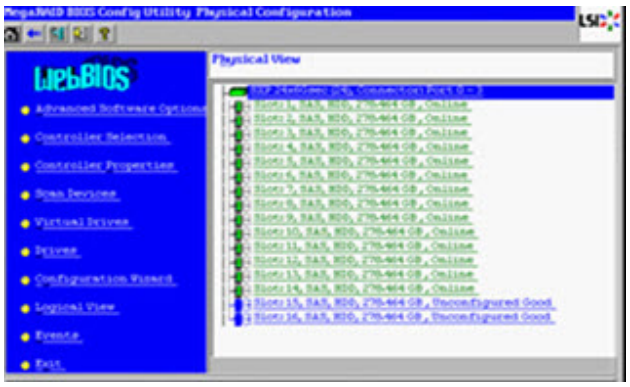


23 Click **Yes** to initialize. The Virtual Drive VD0 is displayed.



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.

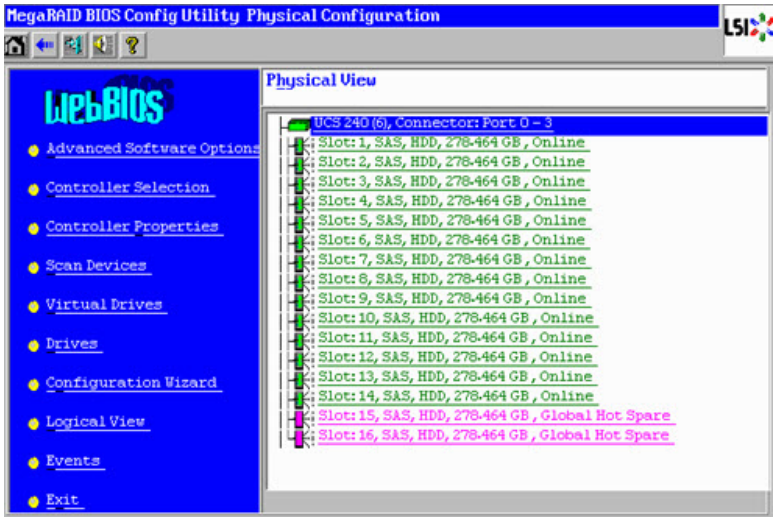


26 Click the drive on Slot 15 in the Physical View.

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.

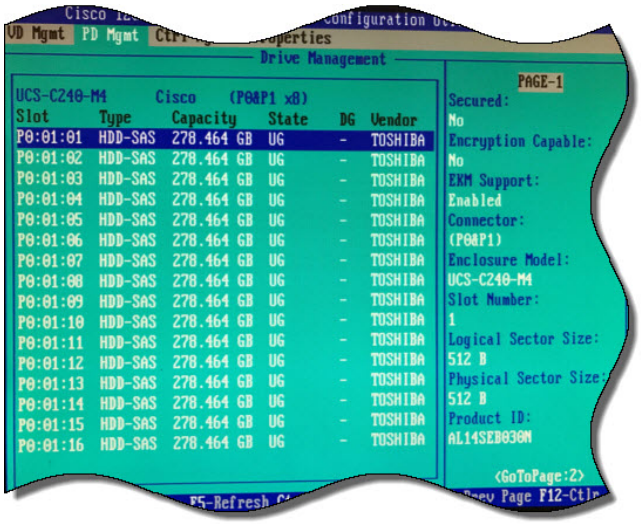
5 Complete the following steps to change the disks from Just a Bunch Of Disks (JBOD) to **Unconfigured Good (UG)**.

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**.

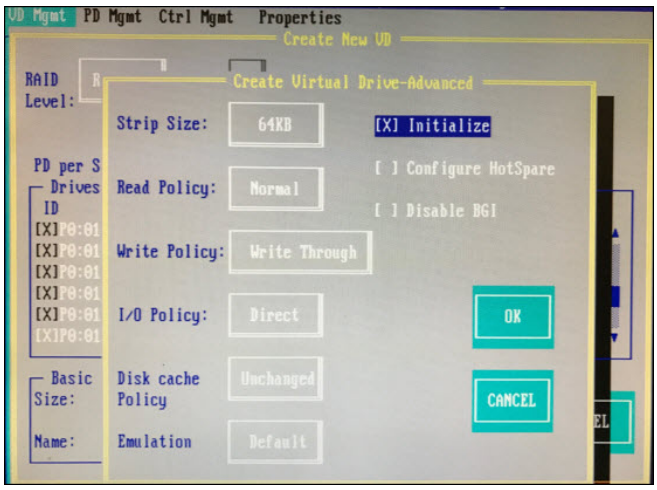
   c From PD per Span area, enter **2**.

   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.

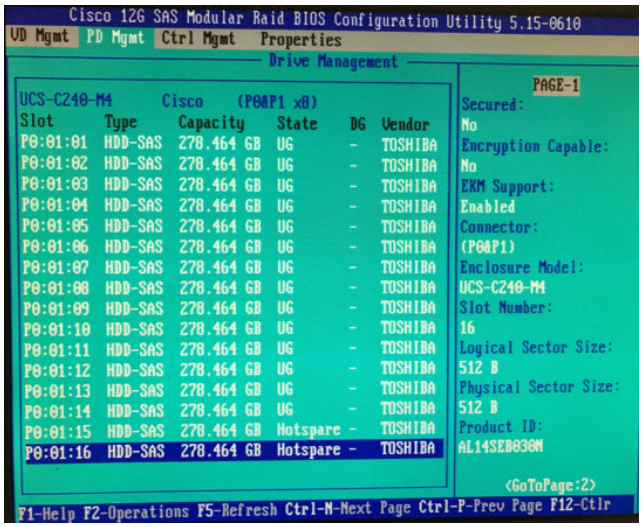
15 Click **CTRL+N** to return to the **PD Mgmt** window.

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 101).
2. Log onto the server using the admin password or the password that you set in ***Cisco UCS C240 Server CIMC Configuration*** (on page 101).

Power Policy

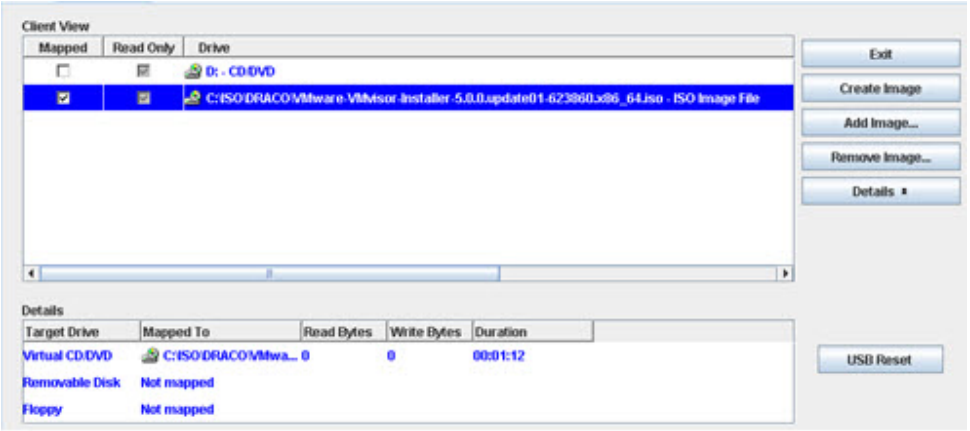
1. Click **Power Policies**.
2. Choose **Restore Last State** from the menu.
3. Click **Save Changes**.
4. Click **Summary** on the Server tab in the CIMC.
5. Click **Launch KVM Console** from the Server Summary window.
6. Select open using java viewer in the dialog box. The KVM Console is displayed.

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.

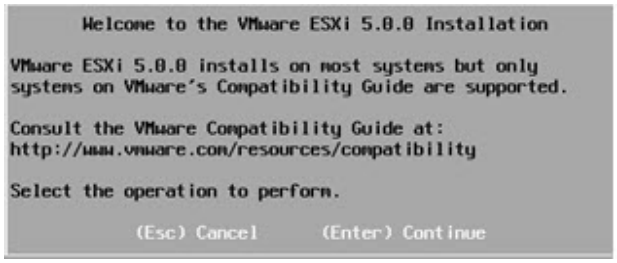
5 Make the following selections:

- 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.

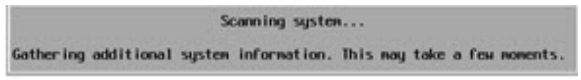
Note: This action selects the disk. Select the disk that matches the size of the Virtual Disk that was recorded in RAID Configuration, Step 17.

11 Press **Enter** to continue.

12 Select the appropriate keyboard layout (for example, **US default**) and press **Enter**.

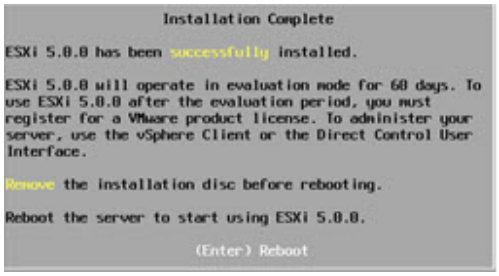
13 Enter and confirm a new **root** password for the ESXi host.

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.

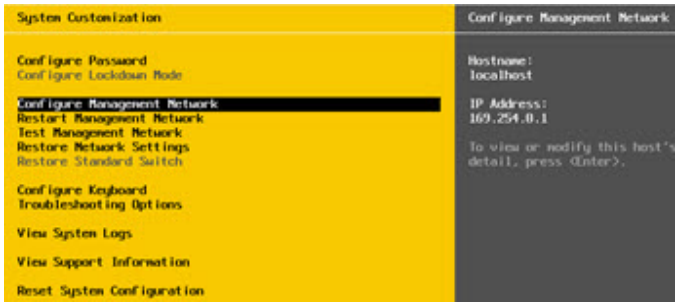


Important: Let the system boot into ESXi. If you press F2 too early (during boot-up), the BIOS configuration screen appears, which is not what you want.

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**.

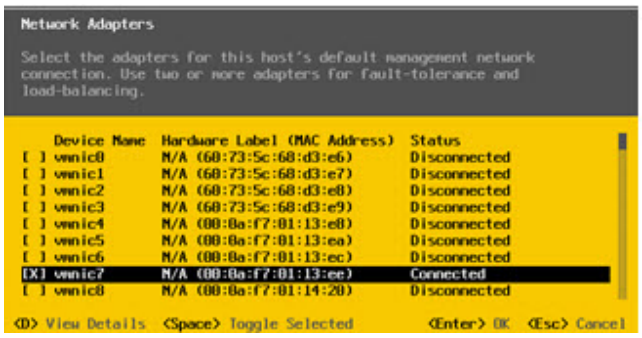


20 Select **Network Adapters** and press **Enter**.

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.

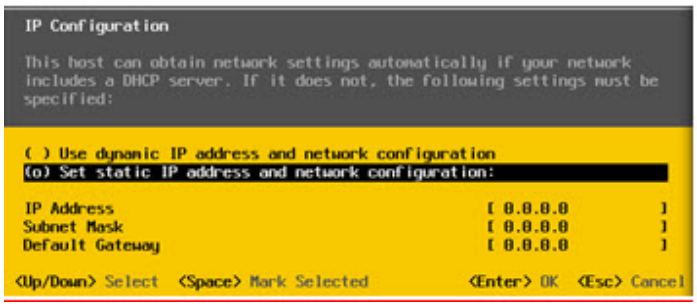
22 Verify that the devices you enabled in step 21 show a **Connected** status.



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 VM Host

Important: This procedure only needs to be performed once — when you initially install the UCS C240 server.

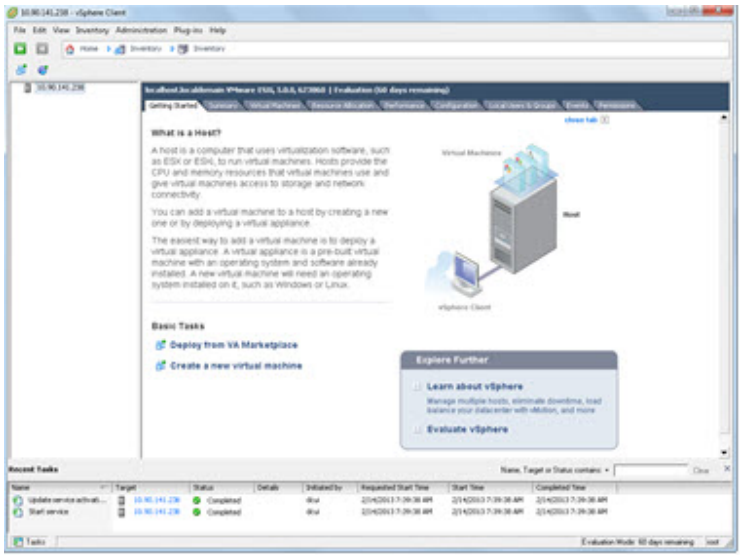
You must have a Windows, Linux, or Mac OS system with vSphere installed to complete the installation and migration of SR 5.0.

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 Client to connect the vCenter server. Provide the IP Address, username, and password for authentication.

3 If you are using vCenter and the Home view is displayed, click on **Hosts and Clusters**, and highlight the new ESXi host in the left pane to begin configuring resources.

Result: vSphere should go to the Inventory display. If not, click **Inventory** to display the ESXi Host.



4 Click the **Configuration** tab.

5 From the **Software** menu, choose **Time Configuration** to modify the date and time.

6 Click **Properties** and enter the correct date and time.

7 Click **NTP Client Enabled**.

8 Click **Options** and click **Start and Stop with host**.

9 Click **NTP Settings** and click **Add**.

10 Enter the **NTP Server Address** and click **OK**.

11 Select **Restart NTP Service** to apply changes and click **OK**.

12 Verify that **NTP Client Enabled** is enabled and click **OK**.

13 From the **Hardware** menu, select **Networking**. Switch vSwitch 0 is displayed.

14 Select **Properties** for vSwitch 0.

15 Select **VM Network** and click **Remove**. You are prompted to confirm this request.

16 Click **Yes**.

17 Click the **Network Adapters** tab and then click **Add**.

18 Refer to the chart that follows to configure the proper management network adapter for your system. Click **Next** after selecting the proper network adapter.

Note: Use the data in this chart to help you configure the network host system settings.

Network	UCS 240-M3
ESXi Management	1, 7
Headend network	8, 4
Corporate network	9, 5
RepDB network	10, 6
Headend 2 network (DSG)	2, 11
TED crossover	0

19 Verify the adapter selection and click **Next**.

20 Click **Finish** to close the wizard.

21 Click **Close** to return to the **Configuration** tab.

22 Click **Add Networking**.

23 Select **Virtual Machine** and click **Next**.

24 Refer to the chart in step 18 to configure the proper headend network adapters for your system.

25 Click **Next**.

26 From the Port Group Properties area, enter **Headend Network** in the **Network Label** text box.

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.

27 Click **Next** and click **Finish**.

28 Repeat these procedures to configure the following networks shown in the network design that was created for the customer.

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.

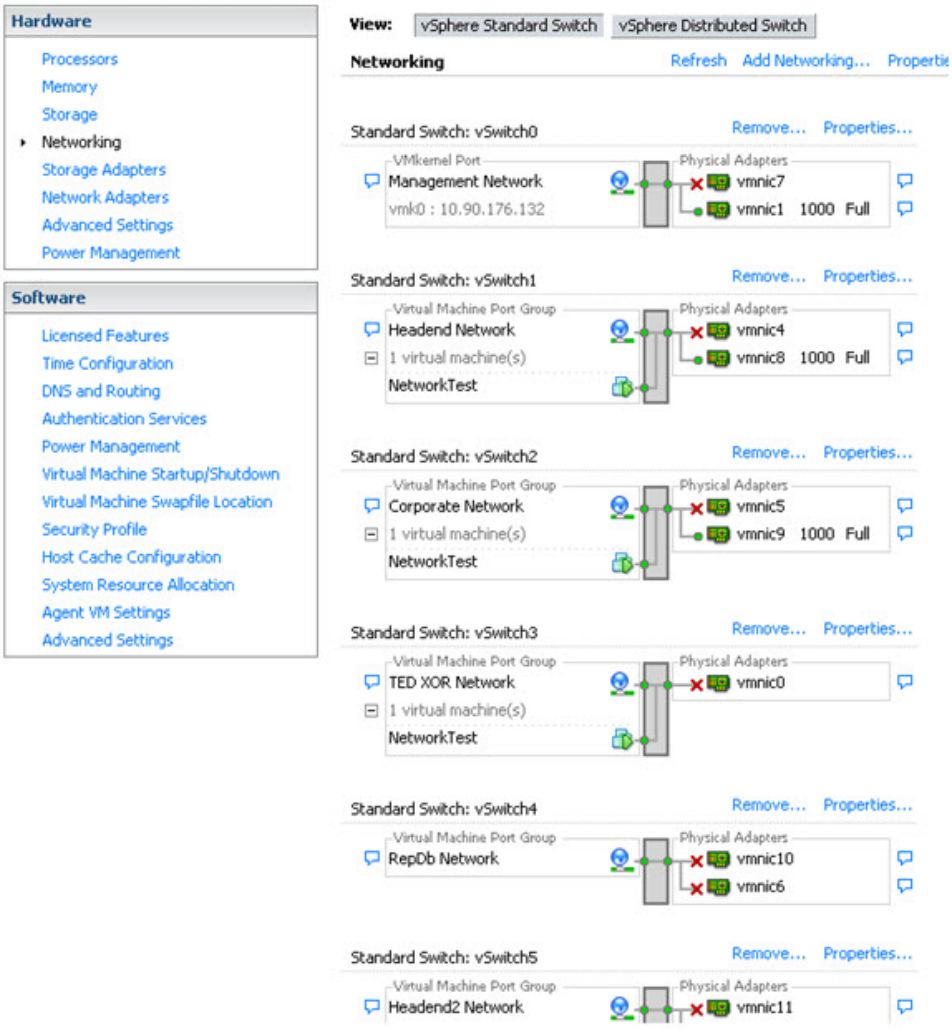
The following examples are for reference only.

- **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.

Example Networking Configuration



29 To configure the **Storage Configuration**, click **Storage** from the **Hardware** menu.

30 Select **datastore1** and right-click to display a drop-down menu.

31 Click **Rename** and rename to **<hostname>_local_storage1**. Click outside of the text box to save the name.

Note: Cisco engineers have seen some issues when the datastore name contains blank spaces. Do not include spaces when you rename the datastore.

32 If necessary, create an NFS mapping to the location of the image.

Note: The server and path are site-specific. The customer should have the ISO file on an NFS server accessible by the Virtual Machine (VM).

a Click **Add Storage**.

b Select **Network File System** and click **Next**.

c Input the server name or IP address, folder, select **Read Only**, and input a datastore name.

d Click **Next**.

e Verify the settings and click **Finish**.

B

Procedures When Using an ESXi Client

This appendix describes various procedure when deploying and reconfiguring VMs using an ESXi client.

In This Appendix

- Deploy and Configure a VM Using an ESXi Client.....124
- Modifying the Device Status for an Ethernet Adapter.....126
- Setting Up RepDB Using an ESXi Client.....127

Deploy and Configure a VM Using an ESXi Client

Deploying a Virtual Machine Using an vSphere Client

Complete the following steps to deploy a VM from the ESXi client.

1. Log on to the ESXi client.
2. Select the appropriate ESXi host and click **File > Deploy OVF Template**. The Source window displays.
3. Click **Browse** and navigate to the directory where the Cisco platform OVA resides.
4. Select the OVA and click **Open**. The absolute path to the OVA is added to the text box in the Source Window.
5. Click **Next**. The OVF Template Details window displays.
6. Review the details and click **Next**. The End User License Agreement displays.
7. Review the license agreement and click **Accept**. Then click **Next**. The Name and Location window display.
8. From the **Name** text box, type a name that describes the VM.
9. Click **Next**. The Deployment Configuration window displays.
10. From the **Configuration** dropdown, select **4 CPU 8GB RAM 20GB DISK** and then click **Next**. The Storage window displays.
11. Select the appropriate storage device and click **Next**. The Disk Format window displays.
12. Maintain the default selection, **Thick Provisioned Lazy Zeroed** and click **Next**. The Network Mapping window displays.
13. For the source network, click the dropdown in the **Destination Networks** column and select the corporate network.
14. Click **Next**. The Ready to Complete window displays.
15. Click **Finish**. The VM deployment starts. A window opens that shows the progress of the deployment, and when it completes, a **Completed Successfully** message appears.

Reconfiguring the Virtual Network Using a vSphere Client

Complete the following steps to reconfigure the virtual hardware for the DTACS 5.0 VM using vSphere client.

1. Select and right-click the new DTACS 5.0 VM. The Edit Settings window displays.
2. Click **Memory** and modify the value to **32 GB**.
3. Select **Hard disk 1** and modify the Provisioned Size to **64** GB.
4. Click the **Add** button. The Device Type window opens.
5. Select **Hard Disk** and then click **Next**.
6. Maintain the **Create a new virtual disk** selection and click **Next**.
7. Change the Disk Size to **128** and maintain the other default selections. Then click **Next**.
8. Click **Next** again. The Ready to Complete window displays.
9. Review the options and then click **Finish**. The new hard disk is added to the virtual machine list.
10. Click the **Add** button again and select **Ethernet Adapter**. Then click **Next**.
11. Maintain the VMXNET 3 adapter type and from the **Network** label dropdown menu, select the label that represents the **Headend** network. Then click **Next**. The Ready to Complete window displays.
12. Review the details and then click **OK**. The VM is reconfigured.
13. Review the options and then click **Finish**. The new Ethernet adapter is added to the virtual machine list.
14. Click **OK**.
15. Monitor the **Recent Tasks** area to confirm that the VM was reconfigured successfully.

Setting the Power Policy Using a vSphere Client

1. Click the **ESXi** Host and then click the **Configuration** tab.
2. From the **Software** area, click **Virtual Machine Startup/Shutdown**.
3. Click **Properties** (located at the top right of the Startup Order window).
4. Check the **Allow virtual machines to start and stop automatically with the system** checkbox.
5. Highlight the VM and click **Move Up** until it is under **Automatic Startup**.
6. Click **OK**.

Modifying the Device Status for an Ethernet Adapter

During various procedures, you are directed to enable or disable the Connected and/or the Connected at power on options for the device status of an Ethernet adapter.

To modify these settings using the vSphere client, complete the following steps.

1. From the vSphere client, select and right-click the appropriate VM.
2. Click **Edit Settings**. The Virtual Machine Properties window opens.
3. Select the appropriate Network adapter. Details for the network adapter appear in the right area of the window.
4. From the **Device Status** section, execute either or both of the following steps, as needed.
   a. Click/unclick the **Connected** check box.
   b. Click/unclick the **Connect at power on** check box.
5. Click **OK** to save the setting.

Setting Up RepDB Using an ESXi Client

Complete the following procedure to set up RepDB using an ESXi client. Because the client only has a connection to a specific ESXi host, you cannot utilize the cloning feature. Instead, you will deploy a secondary VM.

1 As **admin** user on the *primary* DTACS, 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@berlin ~]$ sudo vi /etc/hosts
```

2 Save and close the file.

3 Enter the following command to verify the RepDB entries.

```
[admin@berlin ~]$ less /etc/hosts | grep -i host
```

Example Output:

```
172.16.3.131   HOSTA
172.16.3.132   HOSTB
```

4 Go to the following sections, in order, to deploy a secondary VM.

- ***Deploy and Configure a VM Using vSphere Client*** (see "***Deploy and Configure a VM Using an ESXi Client***" on page 124)
- ***Power on the New DTACS VM*** (on page 17)
- ***Set Up the Network With a Static IP Configuration (Optional)*** (on page 19)
- ***DTACS 5.0 Installation*** (on page 23)

5 After completing the procedures listed in Step 4, go to the next procedure.

Adding the RepDB Network Adapter in an ESXi Client

Complete the following steps to add a network adapter for RepDB on the primary and the secondary ECs.

1 From the vSphere ESXi client, right-click the *primary* VM and then select **Edit Settings**.

2 Just above the **Hardware** area, select the **Add...** button. The Device Type window displays.

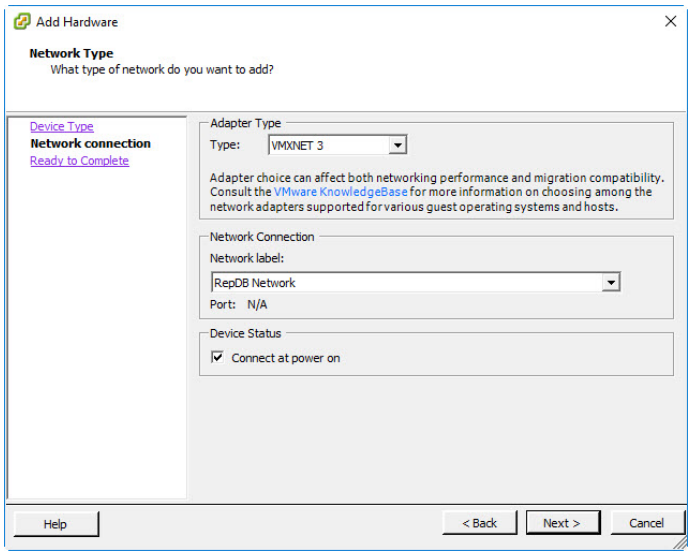
3 Select **Ethernet Adapter** and click **Next**.

4 From the **Type** dropdown menu, select **VMXNET 3**.

5 From the **Network label** dropdown, select the label for your RepDB network (e.g. RepDB network).

6 Ensure the **Connect at power on** check box is selected and then click **Next**. The Ready to Complete window displays.

Example: Primary DTACS



7 Review the settings and if they are correct, click **Finish**. You are returned to the Edit Settings Window and the new NIC is listed in the Hardware area.

8 Click **OK**. The *primary* VM is reconfigured.

9 Right-click the *secondary* VM and then select **Edit Settings**.

10 Just above the **Hardware** area, select the **Add...** button. The Device Type window displays.

11 Select **Ethernet Adapter** and click **Next**.

12 From the **Type** dropdown menu, select **VMXNET 3**.

13 From the **Network label** dropdown, select the label for your RepDB network (e.g. RepDB Network).

14 Ensure the **Connect at power on** check box is selected and then click **Next**. The Ready to Complete window displays.

15 Review the settings and if they are correct, click **Finish**. You are returned to the Edit Settings Window and the new NIC is listed in the Hardware area.

16 Click **Network adapter 2** and select the **Connect at power on** checkbox.

17 Click **OK**. The *secondary* VM is reconfigured.

18 Monitor the **Recent Tasks** area until the task successfully completes.

19 Go to ***Creating an Interface Configuration File for RepDB*** (on page 82).

C

SR 5.0 Rollback Procedures

Introduction

The SR 5.0 rollback procedures are intended for field service engineers who encounter problems while upgrading an existing digital system to SR 5.0. Prior to executing the SR 5.0 rollback procedures, contact Cisco Services.

In This Appendix

- Activate the Old System Release.....130

Activate the Old System Release

1. Complete the following procedure to restore the previous DTACS system.
2. As **dncs** user, type the following commands to stop system components.

   ```
   [dncs@dtacs_50 ~]$ dtacsStop
   [dncs@dtacs_50 ~]$ dtacsKill
   ```

3. As **admin** user, type the following command to shut down and power off the server.

   ```
   [admin@dtacs_50 ~]$ sudo shutdown -h now
   ```

4. From the vSphere Web UI, right-click the VM and select **All vCenter Actions > Power > Power Off**.
5. From the vSphere Web UI, right-click the SR 4.1 DTACS and select **Power On**.
6. Log onto the SR 4.1 DTACS as an administrative user.
7. Change to **dtacs** user.

   ```
   $ sux - dtacs
   ```

8. Type the following command and press **Enter** to start the EC processes:

   ```
   $ dtacsStart
   ```

9. Verify system functionality.

D

DTACS SR 5.0 Upgrade

This appendix provides the procedures to upgrade your system to a new version of DTACS SR 5.0.

In This Appendix

- DTACS SR 5.0 Upgrade Prerequisites 132
- Preparing for the Upgrade 133
- Upgrading the Secondary VM 134
- Cloning the Primary VM 138
- Enabling RepDB on the Upgraded System 142

DTACS SR 5.0 Upgrade Prerequisites

The following prerequisites are required prior to executing a DTACS SR 5.0 upgrade.

- **Admin Node**
  - Refer to Appendix C in the ***Admin Node User's Guide*** for the procedure to upgrade the application software repo.

    Important: The software repos ***must*** be updated before starting the DTACS upgrade.
- **DTACS System**
  - The active system is operating without issues.
  - Verify that dtacsdbsync is successful from the command line and from the DTACS Web UI.
  - Execute a file sync and Replicated Database check.
  - Verify available disk space on the primary and secondary ESXi hosts for cloning the new VMs (i.e. for a standard C240 installation, DTACS requires 160 GB of disk space).
  - The secondary VM must have access to the Admin Node.

Preparing for the Upgrade

Complete the following steps on the DTACS system to prepare the primary and secondary servers for the upgrade.

1 Stop all billing interfaces.

2 Disable RepDB on the *primary* and *secondary* servers.

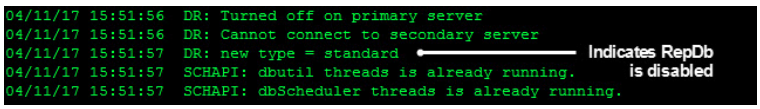
a As **admin** user on the *primary* server, type the following command.

```
[admin@berlin repdb]$ sudo ./RepDb -d
```

b When prompted, type **y**. Data replication is disabled.

c Type the following command to verify that data replication is disabled.

```
[admin@berlin repdb]$ sudo onstat -m
```



d Repeat Steps 2a through 2c on the *secondary* server.

3 Go to the next section.

Upgrading the Secondary VM

Cloning the Secondary VM

Important: If you are using an ESXi client then you cannot clone the secondary VM. Refer to ***Procedures When Using an ESXi Client*** (on page 123) to deploy a new secondary VM.

1 As **admin** user, enter the following command to shut down the *secondary* server.

```
[admin@berlin ~]$ sudo shutdown -h now
```

2 From the vSphere Web UI, right-click the *secondary* VM and select **All vCenter Actions > Power > Power Off**.

3 Monitor the **Recent Tasks** area until the task completes.

4 Right-click the *secondary* VM and select **Clone to Virtual Machine** to create a backup of the original VM. The Clone to Virtual Machine window appears.

5 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 Berlin3_HOSTB_5.0-upgrade_20170622

6 Select the datacenter where the cloned VM will be built. Then click **Next**.

7 Select the ESXi host and verify that the compatibility is validated in the **Compatibility** area of the window. Then click **Next**.

8 Select the storage destination which should be the same as the VM that is being cloned. Then click **Next**.

9 Click **Next** again and then click **Finish**.

10 Monitor the cloning of the VM in the **Recent Tasks** area and when it successfully completes, go to the next step.

11 From the vSphere Web UI, right-click the cloned VM and select **Edit Settings**.

12 Hover your cursor in the **Network adapter 3** (RepDB) line. An X icon, ⊗, appears.

13 Click the ⊗ icon to delete Network adapter 3.

14 Do any remaining Network Adapters share an IP address with the *primary* VM?

- If **yes**, click the check mark out of the **Connected** box. Then go to the next step.
- If **no**, go to the next step.

15 Click **OK**.

16 Right-click the cloned VM and select **Power On**.

17 Right-click the cloned VM and select **Open Console**.

18 Login as **admin** user.

19 Type the following command to delete the **70-persistent-net.rules** file.

```
[admin@berlin ~]$ sudo rm
/etc/udev/rules.d/70-persistent-net.rules
```

20 When prompted to confirm the deletion of the file, type **y**.

21 Enter the following command to reboot the DTACS.

```
[admin@berlin ~]$ sudo shutdown -r now
```

22 When the VM completes the boot process, login and check the network connectivity and verify that you can ping the Admin Node.

Note: If the VM has a unique IP address for eth0, you can log into the VM from a terminal window.

```
[admin@berlin ~]$ ifconfig -a
[admin@berlin ~]$ ping [Admin Node IP]
```

Upgrading the Software on the New Secondary DTACS

1 Change to **dncs** user, enter the following command and press **Enter** to kill the **dtacsInitd** process.

```
[dncs@berlin ~]$ dtacsKill
```

2 As **admin** user, type the following command to see if the **CSCOdtacs-lic-5.x.x** package is installed on your system.

```
[admin@berlin ~]$ rpm -qa | grep -i cscodtacs-lic
```

3 Is the **CSCOdtacs-lic** package installed on your system?

- If **yes**, go to Step 4.
- If **no**, go to Step 5.

4 Enter the following command to remove the **CSCOdtacs-lic** package.

Command:

```
rpm -e CSCOdtacs-lic-[version]
```

Command Example:

```
[admin@berlin ~]$ sudo rpm -e
CSCOdtacs-lic-5.0.11-1.201707250232.el6.x86_64
```

5 Type the following command to upgrade the DTACS software. A verification of the repos occurs and a check is done to verify which packages need upgraded.

```
[admin@berlin ~]$ 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 and, when complete, a **Complete!** message displays.

8 Did the yum update complete successfully?

- If **yes**, go to Step 9.
- If **no**, go to Step 10.

9 Enter the following command to reboot the server and then go to the next section in this appendix.

```
[admin@berlin ~]$ sudo shutdown -r now
```

10 Log back into the DTACS server.

11 As **admin** user, review the following log to see if any error messages exist.

```
[admin@berlin ~]$ sudo less /var/log/yum.log
```

12 If errors exist and you cannot determine the issue, execute one of the following options.

- Contact Cisco Services
- Rollback the upgrade

  Note: To rollback the upgrade, go to the next step.

13 Type the following command to shutdown the VM.

```
[admin@berlin ~]$ sudo shutdown -h now
```

14 From the vSphere Web UI, right-click the VM and select **All vCenter Actions > Power > Power Off**.

15 Monitor the **Recent Tasks** area to verify that the VM successfully powered off.

16 Right-click the original VM host and select **Power On**.

Shutting Down the Primary VM

1 As **dncs** user on the *primary* DTACS, enter the following commands to stop system processes.

```
[dncs@berlin ~]$ dtacsStop
[dncs@berlin ~]$ dtacsKill
```

2 As **admin** user, type the following command to shutdown the *primary* DTACS.

```
[admin@berlin ~]$ sudo shutdown -h now
```

3 Monitor the **Recent Tasks** area until the task completes.

Updating IP Addresses on the Secondary DTACS VM

Important: If the primary and secondary DTACS servers use the same IP address for the corporate network (i.e. eth0), then skip this section.

1 As **admin** user on the active *secondary* DTACS, enter the following command to copy the **ifcfg-eth0** file to a new file.

```
[admin@berlin ~]$ sudo cp
/etc/sysconfig/network-scripts/ifcfg-eth0
/etc/sysconfig/network-scripts/orig.ifcfg-eth0
```

2 Open the **/etc/sysconfig/network-scripts/ifcfg-eth0** in a text editor and update the IP address.

```
[admin@berlin ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-eth0
```

3 Save and close the file.

4 Execute the following commands to restart the network interface.

```
[admin@berlin ~]$ sudo /etc/sysconfig/network-scripts/ifdown eth0
[admin@berlin ~]$ sudo /etc/sysconfig/network-scripts/ifup eth0
```

5 Repeat Steps 1 through 4 for any other interface that uses a unique IP address.

Note: Make sure to substitute the appropriate file name for ifcfg-eth0.

6 Enter the following command to verify that the IP addresses are correct for each interface.

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

Reconfiguring the Network Adapters on the Secondary VM

Complete the following steps to reconfigure the network adapters on the secondary VM.

1 From the vSphere Web UI, right-click the *active secondary* VM and select **Edit Settings**.

2 Click the **Connect** box for all network adapters.

3 Click **OK**.

4 Monitor the **Recent Tasks** area to confirm that the task successfully completes.

Starting Processes on the Secondary DTACS

1 As **dncs** user on the *active secondary* DTACS, type the following command to start system processes.

```
[dncs@berlin ~]$ dtacStart
```

2 Type the following command to verify that system processes have started.

```
[dncs@berlin ~]$ pgrep -fl dvs
```

3 Log into the DTACS Web UI and verify that processes are coming up and eventually go green.

Note: This server is now the primary DTACS in the system.

Verifying the Functionality of the Upgraded DTACS

Verify that you can execute a dtacsdbSync from the command line and from the DTACS Web UI.

Note: If dtacsdbSync fails from either method, contact Cisco Services.

Cloning the Primary VM

Note: The original primary server has already been shutdown.

1 Right-click the original `primary` VM and select **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 Berlin3_HOSTA_5.0-orig_20170330

3 Select the datacenter where the cloned VM will be built. Then click **Next**.

4 Select the ESXi host and verify that the compatibility is validated in the Compatibility area of the window. Then click **Next**.

5 Select the storage destination which should be the same as the VM that is being cloned. Then click **Next**.

6 Click **Next** again and then click **Finish**.

7 Monitor the cloning of the VM in the Recent Tasks area and when it successfully completes, go to the next step.

8 From the vSphere Web Client, right-click the new, cloned primary VM and select **Edit Settings**.

9 Hover your cursor in the **Network adapter 3** (RepDB) line. An X icon,  , appears.

10 Click the icon to delete the network adapter for RepDB.

11 Do any of the other Network adapters share an IP address with the secondary VM?

- If **yes**, click the check mark out of the **Connected** box. Then go to the next step.
- If **no**, go to the next step.

12 Click **OK**.

13 Right-click the VM and select **Power On**.

14 Right-click the VM again and select **Open Console**.

15 Login to the VM **admin** user.

16 Type the following command to delete the **70-persistent-net.rules** file.

```
[[admin@berlin ~]$ sudo rm
/etc/udev/rules.d/70-persistent-net.rules
```

17 When prompted to confirm the deletion of the file, type **y**.

18 Enter the following command to reboot the DTACS.

```
[admin@berlin ~]$ sudo shutdown -r now
```

19 When the VM completes the boot process, login and check the network connectivity and verify that you can ping the Admin Node.

```
[admin@berlin ~]$ ifconfig -a
[admin@berlin ~]$ [Admin Node IP]
```

Cloning the Original Primary DTACS VM

Important: If you are using the vSphere client then you cannot clone this VM. Refer to ***Procedures When Using an ESXi Client*** (on page 123) to deploy a new VM.

Note: This server has already been shutdown.

1 Right-click the *original primary* VM and select **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 DTACS_50_HOSTA_5.0-upgrade_20170622

3 Select the datacenter where the cloned VM will be built. Then click **Next**.

4 Select the ESXi host and verify that the compatibility is validated in the **Compatibility** area of the window. Then click **Next**.

5 Select the storage destination which should be the same as the VM that is being cloned. Then click **Next**.

6 Click **Next** again and then click **Finish**.

7 Monitor the cloning of the VM in the **Recent Tasks** area. When it successfully completes, go to the next step.

8 From the vSphere Web UI, right-click the new, cloned VM and select **Edit Settings**.

9 Hover your cursor in the **Network adapter 3** (RepDB) line. An X icon,  , appears.

10 Click the **X** icon to delete the network adapter for RepDB.

11 Do any of the other Network adapters share an IP address with the new active VM in the system?

- If **yes**, click the check mark out of the **Connected** box. Then go to the next step.
- If **no**, go to the next step.

12 Click **OK**.

13 Right-click the VM and select **Power On**.

14 Right-click the VM again and select **Open Console**.

15 Login to the VM as **admin** user.

16 Type the following command to delete the **70-persistent-net.rules** file.

```
[admin@berlin ~]$ sudo rm
/etc/udev/rules.d/70-persistent-net.rules
```

17 When prompted to confirm the deletion of the file, type **y**.

18 Enter the following command to reboot the DTACS.

```
[admin@berlin ~]$ sudo shutdown -r now
```

19 When the VM completes the boot process, login as **admin** user.

20 Enter the following commands to check the network connectivity and to verify that you can ping the Admin Node.

```
[admin@berlin ~]$ ifconfig -a
[admin@berlin ~]$ [Admin Node IP]
```

Upgrading the Software on the New DTACS

Note: This will become the new secondary DTACS in the system you are upgrading.

1 As **dncs** user, enter the following command and press **Enter** to kill the dtacsInitd process.

```
[dncs@berlin ~]$ dtacsKill
```

2 As **admin** user, type the following command to see if the **CSCOdtacs-lic-5.0.x** package is installed on your system.

```
[admin@berlin ~]$ rpm -qa | grep -i cscodtacs-lic
```

3 Is the **CSCOdtacs-lic** package installed on your system?

- If **yes**, go to Step 4.
- If **no**, go to Step 5.

4 Enter the following command to remove the **CSCOdtacs-lic** package.

Command:

```
sudo rpm -e CSCOdtacs-lic-[version]
```

Command Example:

```
[admin@berlin ~]$ sudo rpm -e
CSCOdtacs-lic-5.0.10-3.201706061031.el6.x86_64
```

5 Type the following command to upgrade the DTACS software. A verification of the repos occurs and a check is done to verify which packages need upgraded.

```
[admin@berlin ~]$ 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 and, when complete, a **Complete!** message displays.

8 Did the yum update complete successfully?

- If **yes**, go to Step 6.
- If **no**, go to Step 7.

9 Enter the following command to reboot the server and then go to the next section in this appendix.

```
[admin@berlin ~]$ sudo shutdown -r now
```

10 Log back into the DTACS and review the following log to see if any error messages exist.

```
[admin@berlin ~]$ sudo less /var/log/yum.log
```

11 If errors exist and you cannot determine the issue, execute one of the following options.

- Contact Cisco Services
- Rollback the upgrade

  Note: To rollback the upgrade, go to the next step.

12 Type the following command to shutdown the VM.

```
[admin@berlin ~]$ sudo shutdown -h now
```

13 From the vSphere Web UI, right-click the VM and select **All vCenter Actions > Power > Power Off**.

14 Monitor the **Recent Tasks** area to verify that the VM successfully powered off.

15 Right-click the original VM host and select **Power On**.

Enabling RepDB on the Upgraded System

To enable RepDB on the upgraded system, refer to the following two sections in Chapter 7, ***Configure and Operate the Replicated Database***.

- ***Adding the RepDB Network Adapter on the Primary and Secondary VMs*** (on page 80)
- ***Enabling RepDB*** (on page 87)

E

DTACS 5.0 Patch Installs

This section describes the procedures to install a patch to the *primary* and *secondary* DTACS servers in your NextX system.

The format for a DTACS patch is:
CSCOdtacs-patch-[VERSION].[DATE].[PLATFORM].rpm

The version for the first CSCOdtacs-patch package is always "-2" (i.e. CSCOdtacs-patch-5.0.11-**2**.[VERSION].[DATE].[PLATFORM].rpm). The version for any future patches is numbered incrementally (i.e. CSCOdtacs-patch-5.0.11-**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 Install 144
- Installing a DTACS Patch 145
- Uninstalling a DTACS Patch 148

Preparing for a Patch Install

Complete the following steps prior to executing the patch upgrade.

1 Are you using vSphere Web UI or vSphere client?

- If **yes**, clone your *primary* system to create a full system backup.
- If **no** and you are using an ESXi client, back up the database and key files to an NFS mount.

Note: For details about cloning and system backups, refer to the ***Backup and Restore User Guide for EC 8.0 and DTACS 5.0*** document.

2 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. If a patch is present, an entry for CSCOdtacs-patch is listed.

URL Syntax:

```
http://[Admin_Node_IP]/repos/nextx/8.0/
```

Example:

```
http://10.90.47.60/repos/nextx/8.0/
```

3 Is the **CSCOdtacs-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 Installation Guide*** to update the NextX repo with the patch software.

Installing a DTACS 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@dtacs_50 ~]$ sudo /opt/cisco/repdb/RepDb -d
```

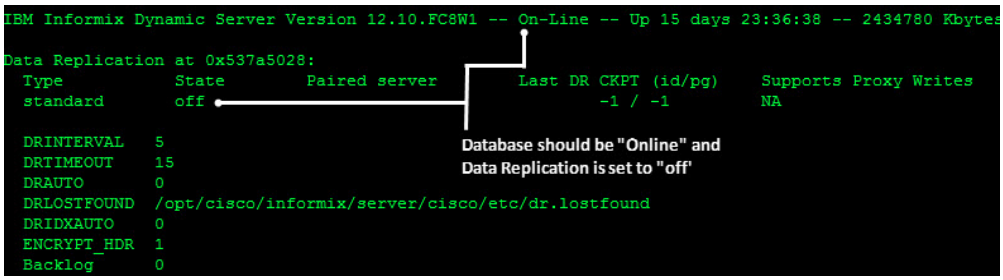
2 Enter the following command to deactivate RepDB on *the* primary server.

```
[dncs@dtacs_50 ~]$ 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@dtacs_50 ~]# onstat -g dri
```



5 As **dncs** user on the *primary* server, enter the following commands to stop processes.

```
[dncs@dtacs_50 ~]$ dtacsStop
[dncs@dtacs_50 ~]$ dtacsKill
```

6 Enter the following command to verify if a **CSCOdtacs-patch** package is currently installed on the DTACS server?

```
[dncs@dtacs_50 ~]$ rpm -qa | grep -i CSCOdtacs-patch
```

7 Does a **CSCOdtacs-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 a DTACS patch, enter the full package name in the installation command.

  Command Syntax:

  ```
  sudo yum install
  CSCOdtacs-patch-[VERSION].[DATE].[PLATFORM]
  ```

Example:

```
[admin@dtacs_50 ~]$ sudo yum install
CSCOdtacs-patch-5.0.11-2.201707261548.el6.x86_64
```

- If **yes** and you are installing a newer CSCOdtacs-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 DTACS patch that is in the NextX repo.

  ```
  [admin@dtacs_50 ~]$ sudo yum update CSCOdtacs-patch*
  ```

8 Type **y** and press **Enter**. The installation continues and when finished, a **Complete!** message displays.

  Note: The output from the patch install may display other packages that were downloaded and installed if dependencies exist.

9 Enter the following command to verify that the **CSCOdtacs-patch** package successfully installed.

  ```
  [admin@dtacs_50 ~]$ rpm -qa CSCOdtacs-patch
  ```

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 CSCOdtacs-patch-[VERSION].[DATE].[PLATFORM]
  ```

  Example:

  ```
  [admin@dtacs_50 ~]$ rpm -q --changelog
  CSCOdtacs-patch-5.0.11-2.201707261548.el6.x86_64
  ```

11 Enter the following command to reboot the server.

  ```
  [admin@dtacs_50 ~]$ sudo shutdown -r now
  ```

12 Log back into the server and, as **dncs** user, enter the following commands to start processes.

  ```
  [dncs@dtacs_50 ~]$ dtacsStart
  ```

13 Verify server functionality.

14 Is your server functioning properly?

- If **yes**, and you successfully installed the patch on the *primary* DTACS, go to the next step.
- If **yes** and you successfully installed the patch on the *primary* and the *secondary* DTACS 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 ***Configure RepDB*** (on page 80) to re-enable replicated database on your system.

Uninstalling a DTACS Patch

Complete the following steps to uninstall a DTACS 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@dtacs_50 ~]$ dtacsStop
[dncs@dtacs_50 ~]$ dtacsKill
```

2 Enter the following command to verify the current version of the **CSCOdtacs-patch**.

```
[dncs@dtacs_50 ~]$ rpm -qa | grep -i CSCOdtacs-patch
```

3 As **admin** user, enter the following command to obtain the **ID** of the CSCOdtacs-patch installation.

```
[admin@dtacs_50 ~]$ sudo yum history package-list
CSCOdtacs-patch\*
```

4 From the **ID** column, record the ID number for the CSCOdtacs-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@dtacs_50 ~]$ sudo yum history undo 69
```

6 Type **y** and press **Enter**. The downgrade proceeds, and when finished, a **Complete!** message displays.

Note: Some patch uninstalls may downgrade other packages if they were upgraded as dependencies when the patch was installed.

7 Enter the following command to verify the current version of the patch.

Note: If this was the first time a CSCOdtacs-patch was installed, no output is displayed for this package because it was deleted.

```
rpm -qa | grep -i CSCOdtacs-patch
```

8 Enter the following command to reboot the server.

```
[admin@dtacs_50 ~]$ sudo shutdown -r now
```

9 Log back into the server and, as **dncs** user, enter the following command to start processes.

```
[dncs@dtacs_50 ~]$ dtacsStart
```

10 Verify DTACS functionality.

11 Is your DTACS functioning properly?

- If **yes**, go to the next step.
- If **no**, refer to the ***Backup and Restore User Guide for EC 8.0 and DTACS 5.0*** to restore your system.

12 Refer to ***Configure RepDB*** (on page 80) to re-enable replicated database on your system.

F

Configure Multiple Interfaces in a CentOS Environment

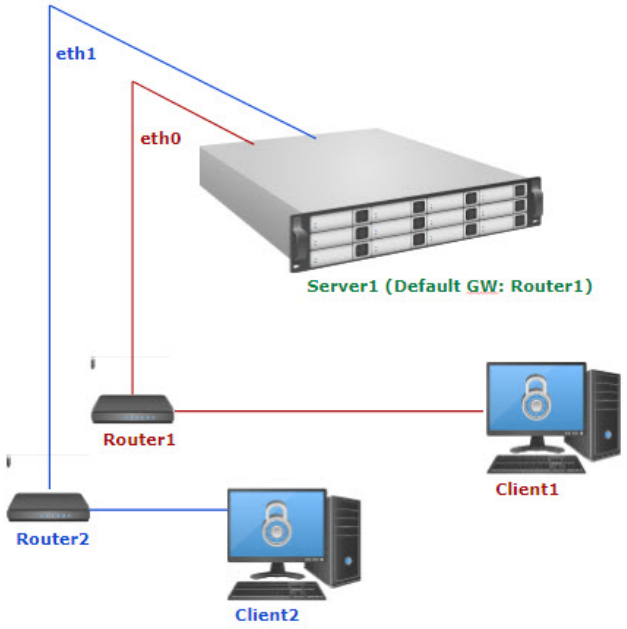
The instructions in this appendix describe how to configure multiple network interfaces in a CentOS environment.

In This Appendix

- Background.....152
- Solution to this Issue.....153

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 eth0.
- Server1 receives the request via eth0.
- Server1 tries to respond back using Router2 (default GW) but fails as Router2 is only accessible via a different interface from where the request originated (eth0).

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 each eth0 and eth1 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, eth0 and eth1, and two routing tables, table 1 for eth0, and table 2 for eth1.

  Example: Network Interface Configuration

  Important: Make sure to substitute the values for your system for the eth0 and eth1 interfaces, as well as for the global default gateway.

	IP Address/Mask Bits	Gateway
eth0	10.90.167.208/24	10.90.167.1
eth2	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@NextXvm ~]$ 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 **eth0** interface (for example, from the previous table).

```
[admin@NextXvm ~]$ sudo vi
/etc/sysconfig/network-scripts/route-eth0
```

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 eth0 table 1
default via 10.90.167.1 dev eth0 table 1
```

4 Save and close the file.

5 Enter the following command to configure the routes for the **eth1** interface (table 2).

```
[admin@NextXvm ~]$ sudo vi
/etc/sysconfig/network-scripts/route-eth1
```

Example Input:

```
224.0.0.0/4 dev eth1  #(Optional) Specific multicast static route for
table 2
10.90.47.0/24 dev eth0  #(Optional) Specific unicast static route for
table 2
10.253.6.0/24 dev eth 1 table 2
default via 10.253.6.254 dev eth1 table 2
default via 10.253.6.254 dev eth1 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 **eth0** interface.

```
[admin@NextXvm ~]$ sudo vi
/etc/sysconfig/network-scripts/rule-eth0
```

Example Input:

```
iif eth0 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 **eth1** interface.

```
[admin@NextXvm ~]$ sudo vi
/etc/sysconfig/network-scripts/rule-eth1
```

Example Input:

```
iif eth1 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@NextXvm ~]$ 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@NextXvm ~]$ ip rule
```

Example Output:

```
0:      from all lookup local
32762:  from 10.253.6.2 lookup 2
32763:  from all iif eth1 lookup 2
32764:  from 10.90.167.208 lookup 1
32765:  from all iif eth0 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@NextXvm ~]$ ip route show table 1
```

Example Output:

```
10.90.167.0/24 dev eth0 scope link
default via 10.90.167.1 dev eth0
```

```
[admin@NextXvm ~]$ ip route show table 2
```

Example Output:

```
10.253.6.0/24 dev eth1 scope link
default via 10.253.6.254 dev eth1
```

```
[admin@NextXvm ~]$ ip route show table 254
```

Note: The routing table 254 is the default routing table.

Example Output:

```
10.253.6.0/24 dev eth1 proto kernel scope link src 10.253.6.2
10.90.167.0/24 dev eth0 proto kernel scope link src 10.90.167.208
default via 10.253.6.254 dev eth
```

3 Were the rules and routing tables set up correctly?

- If **yes**, you have completed this procedure.
- If **no**, refer to Configuring Multiple Interfaces in CentOS to make sure your network is configured correctly.

Index

A

Accessing the root and dncs User Accounts • 45
Activate the Old System Release • 130
Adding the RepDB Network Adapter in an ESXi Client • 127
Adding the RepDB Network Adapter on the Primary and Secondary VMs • 80
Additional IP Address and NAS Interface Requirements • 6
Advantages of RepDB • 73

B

Background • 152

C

CentOS cron and anacrontab Overview • 63
Cisco UCS C240 Host Configuration • 102
Cisco UCS C240 Server CIMC Configuration • 101
Cloning the Original Primary DTACS VM • 139
Cloning the Primary VM • 138
Cloning the Secondary VM • 134
Cloning When the Primary VM is Shutdown • 75
Cloning While the Primary VM is Running • 77
Configure and Operate the Replicated Database • 71
Configure RepDB • 80
Configure the Secondary Host After Cloning • 78
Configure the VM Host • 119
Configuring DTACS BOSS Proxy (Optional) • 61
Configuring Multiple Interfaces in CentOS • 153
Configuring RAID for UCS C240 M3 Servers • 103
Configuring RAID for UCS C240 M4 Servers • 110
Configuring the DTACS Server for the EC • 52
Configuring the EC for DTACS • 54
Copying the SSH Keys Between the DTACS and the EC Servers • 86
Copying the VCS Deployment Zip File to the VM • 24
Creating a Directory for SFTP File Transfers • 58
Creating a User for SFTP Support • 57
Creating an Admin User on the DTACS 4.1 Server • 36
Creating an Administrative User Account • 46
Creating an Interface Configuration File for RepDB • 82
Creating the config.json File on the DTACS • 27
Creating User Accounts • 44
cron and anacron Features • 63

D

Default cron Jobs • 64
Deploy and Configure a VM Using an ESXi Client • 124
Deploy the DTACS Virtual Machine • 9
Deploying a Virtual Machine Using an vSphere Client • 124
Deploying the VM From the Linux Platform Template • 10
Descriptions and Options for the Migrate Scripts • 37
Determine Which Optional Features to Enable • 8
DTACS 5.0 Installation • 23
DTACS SR 5.0 Upgrade Prerequisites • 132

E

Editing the Key Files Sync File Lists • 91
Enabling RADIUS and LDAP (Optional) • 69
Enabling RepDB • 87
Enabling RepDB on the Upgraded System • 142
Estimated Time to Complete the Upgrade • 7
Estimated Timeline • 7
ESXi Installation • 113

H

Hardware Diagram of the Cisco UCS C240 M3 Server • 94

Hardware Diagram of the Cisco UCS C240 M4 Server • 97
Hardware Requirements • 2
Hardware Requirements for a New UCS Install • 100

I

Installing a DTACS Patch • 145
Installing DTACS 5.0 • 25

L

Limitations of the Replicated Database • 74

M

Migrate DTACS 4.1 to DTACS 5.0 • 35
Migrating Key Files • 38
Migrating Key Files and Database to DTACS 5.0 • 37
Migrating the Database and Key Files • 40
Migrating Users • 39
Modifying the Device Status for an Ethernet Adapter • 126

O

Overview of the Replicated Database Package • 73

P

Planning the Install or Migration • 1
Post RepDB Verifications • 90
Post Upgrade Procedures • 43
Power on the New DTACS VM • 17
Preparing for a Patch Install • 144
Preparing for the Upgrade • 133
Preparing the System for the Installation or Migration • 15
Prerequisites for RepDB • 72

R

RAID Configuration • 103
Reconfiguring the Network Adapters on the Secondary VM • 137
Reconfiguring the Virtual Hardware Settings on the VM • 12
Reconfiguring the Virtual Network Using a vSphere Client • 125
RepDB Package and Components • 73
Replicated Database and Failover • 74
Restarting Apache and Tomcat Services • 62
Restricting SFTP Access to a Single Directory • 59

S

SCID Sharing Support Feature (Optional) • 70
Set Up the Network With a Static IP Configuration (Optional) • 19
Setting the Power Policy • 13
Setting the Power Policy Using a vSphere Client • 125
Setting Up RepDB Using an ESXi Client • 127
Setting Up SFTP Support • 57
Setting Up SSH Login Between the DTACS Servers Without a Password • 84
Setup Replicated Database • 75
Shutdown the Secondary SR 4.1 DTACS VM • 16
Shutting Down the Primary VM • 136
Site Requirements • 2
Software Requirements • 4
Solution to this Issue • 153
Starting DTACS Processes • 67
Starting Processes on the Secondary DTACS • 137

T

Testing dbsync from the DTACS Web UI • 68
Testing Synchronization Between the DTACS and EC Databases • 56
Testing the Setup of the Network Interfaces • 155
Transfer HTTPS X.509 Certificates to the DTACS Server • 27
Transferring DTACS Certificates Created From the Admin Node • 28

U

Uninstalling a DTACS Patch • 148
Updating IP Addresses on the Secondary DTACS VM • 136
Updating the DTACS Configuration • 42
Updating the site_info Database Table for a Hostname Change • 49
Upgrading the Secondary VM • 134
Upgrading the Software on the New DTACS • 140
Upgrading the Software on the New Secondary DTACS • 135
User Account Types • 44

V

Verifying Remote File Copying • 90
Verifying That RepDB is Running • 90
Verifying the crontab Entries • 65
Verifying the crontab Entries Managed by cron • 65
Verifying the DTACS Certificate Configuration • 30
Verifying the Functionality of the Upgraded DTACS • 137
Verifying the SFTP Configuration • 60
Verifying User-Defined CRON Entries on the Migrated VM • 66

W

Web Browser Requirements • 5

X

X.509 CA Certificate and Associated Private Key Requirements • 5

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

March 2018

Part Number TP-00108-02