Admin Node 1.0 Installation 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)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

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

Introduction

The Admin Node is used to access the collection of software for Linux/CentOS distribution onto destination servers, e.g. EC 8.0, DTACS 5.0 and ECS 3.0 server nodes. These destination servers are configured to communicate with the Admin Node to quickly and easily download the appropriate software from Yellowdog Updater Modified (YUM) repositories (repos) defined in configuration files.

This guide is also used to create and distribute the NextX X.509 root CA certificate to each node in your NextX system, as well as X.509 certificates specific to each node.

Audience

This guide is written for field service engineers and system operators who are responsible for installing the Admin Node Virtual Machine (VM)), as well as the nodes for the entire NextX solution.

Required Skills and Expertise

System operators or engineers who install or upgrade the Admin Node software need the following skills:

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

Site Requirements

- VMware ESXi (5.5 or later) and vCenter infrastructure (software, license, and a running vCenter machine)
- A vCenter user name and datacenter created for you that includes privileges to create hosts and add VMs.
- An NTP server with NTP v4.x or later

Document Version

This is the first formal release of this document.

Revision History

Date	Revision	Section
20170902	Added prerequisite concerning the requirement of the **/home/admin/.ssh** directory.	***Create NextX X.509 Certificates*** (on page 27)

1

Plan the Deployment

Before you deploy the Admin Node, make sure your system environment meets the hardware and software prerequisites defined in this chapter.

In This Chapter

Hardware Requirements

The following hardware prerequisites are required to deploy an Admin Node VM.

- 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, in the ***SR 8.0 Installation and Migration Guide*** or the ***DTACS 5.0 Installation and Migration Guide***, for procedures to configure a new server. This must be completed prior to deploying the OVA.

  Refer to ***UCS Hardware and Software Compatibility*** (***https://ucshcltool.cloudapps.cisco.com/public/***) for further details.

- Cisco UCS hardware should have adequate CPU, Memory and hard disk capacities

CPUs	Memory (GB)	Hard Disks (GB)	Network Interface
2	4	1 x 32 1 x 128	1 Public

- NET0 – vSwitch0 – Public interface

  Note: Cisco recommends that you configure this interface on a subnet that is accessible to all intended NextX clients (e.g. Corporate Intranet, Lab network).

Software Requirements

The following software prerequisites are required to deploy an Admin Node virtual machine (VM).

- Requires a vCenter Web UI or client login to connect and perform management tasks; login must have admin privileges to deploy VMs .
- Reserve a static IP address for the VM (vCenter Web UI only) and obtain the associated domain name server, default gateway and network mask values from your system administrator.
- Download the appropriate software for your site from your customer-specific forum on Cisco's File Exchange Server and save it to a local directory that is accessible to the vSphere or the ESXi host.

  Important: This is an inclusive list. All of the software may not be required for your site. Only download the software specific to your system needs.

Software	Syntax for TAR File	Required on this NextX Node
Linux VMware OVA	CSCOlxplat-[VERSION].ova	Admin Node **Note**: All nodes if deploying VMs from vSphere Client
CSCOlxplat Base and Updates Yum Repos	CSCOlxplat-*.rpms.tar	Admin Node
Admin Node	admin-node-[VERSION].zip	Admin Node
Oracle RAC (new install only)	oracle-rac-12c-v3.0.x.tar oracle-rac-ee-3.0.3_20161129.tar RAC_8CPU_64GBRAM_80GBHDD_RHEL6U8/RAC_8CPU_64GBRAM_80GBHDD_RHEL6U8.ovf	Oracle RAC Nodes
Cisco VCS Deployment	cisco-vcs-deployment-[VERSION].zip	Admin Node EC DTACS
EC System Release	ec-system-release-[VERSION].tar	EC
EC Pre-Upgrade Check	ecpuc_[VERSION].tar	EC
DTACS System Release	dtacs-system-release-[VERSION].tar	DTACS

Software	Syntax for TAR File	Required on this NextX Node
Cisco VCS Infra	cisco-vcs-infra-[VERSION].tar	Admin Node
ECS System Release	ecs-[VERSION].tar	ECS
VCS Console	vcsconsole-[VERSION].tar	VCS Console
Alert Manager	am-x.tar	VCS Console
Billing Adaptor	billingAdaptor-[VERSION].tar	BOA
Billing Adaptor UI	BillingAdaptorUI-[VERSION.tar	VCS Console

2

Create a Linux Platform Template

Important: All instructions and screen shots in this document are executed via vCenter v5.5 Web UI login. If you are not using the vSphere Web UI and you are deploying your VMs from an ESXi client, you cannot create a template. Instead, skip this chapter and go to Appendix A, ***Deploy the Virtual Machine from an ESXi Client*** (on page 39).

This chapter provides the procedures to create a Linux platform template in the vSphere Web UI. The template will be used to quickly deploy the Admin Node VM, as well any NextX application VMs such as EC 8.0, DTACS 5.0 servers and VMs deployed for ECS 3.0.

Note: This template will not be used to deploy PCG VMs. Refer to the ***PowerKEY CAS Gateway 4.0 Installation and Configuration Guide*** for details.

The following software is required to create the Linux platform template.

Important: This software should have been downloaded to your local PC as mentioned in ***Software Requirements*** (on page 3). If you have not downloaded the software, please do so now.

- CSCOlxplat-[VERSION].ova
- cisco-vcs-deployment-[VERSION].zip
- cisco-vcs-infra-[VERSION].tar

In This Chapter

Deploying the Linux Platform Template

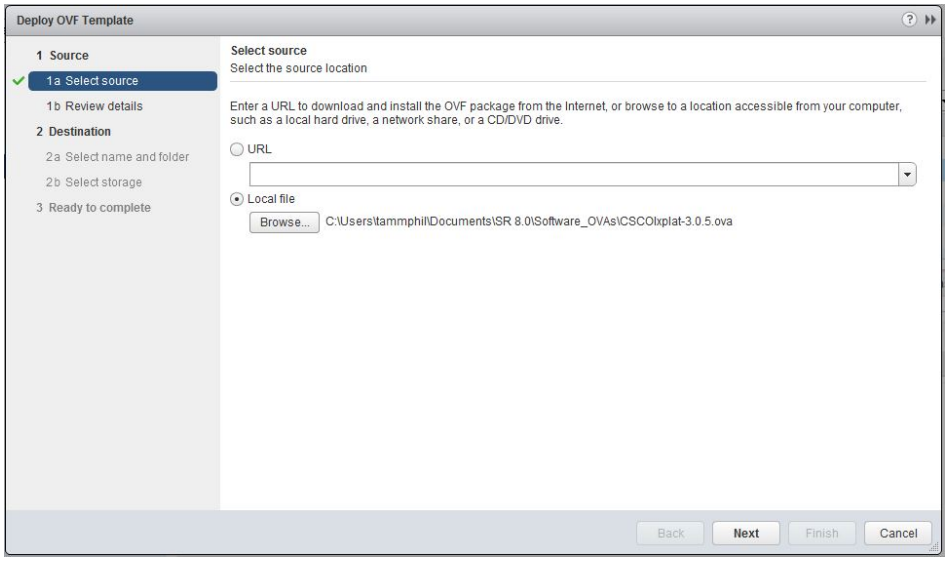
Follow these steps to deploy the OVA.

1 Via a web browser, login to your vCenter Web client.

2 From vCenter, click the **Home** icon, , and then click **Hosts and Clusters.**

3 Select the ESXi host or cluster where you will deploy the VM instance.

4 Right-click the ESXi host and select **Deploy OVF Template**. The Deploy OVF Template window opens.



5 Click **Local file** and select the **CSCOlxplat** OVA file from the folder on your local machine and click **Open**. Then click **Next**.

6 Review the OVF template details and click **Next**.

7 Review the End User License Agreement and click **Accept**. Then click **Next**. The Select name and folder window appears.

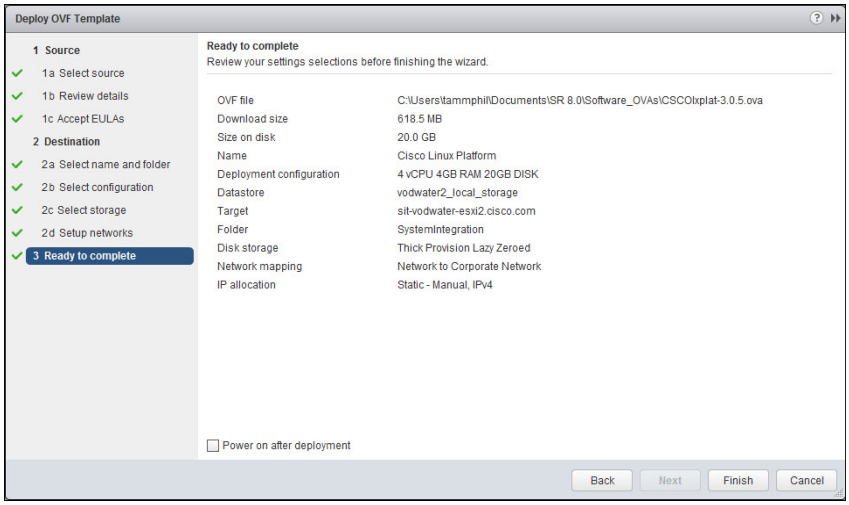
8 In the **Name** text box, enter a name that describes the VM you are deploying and select the datacenter where the VM is to be located. Then click **Next**.

Note: Make sure that you name the VM in a way that identifies it as the Linux platform template (i.e. Cisco Linux Platform) as it will be used to deploy future NextX application VMs.

9 From the **Configuration** dropdown menu, select the **4CPU 4GB RAM 20GB** disk configuration and click **Next**.

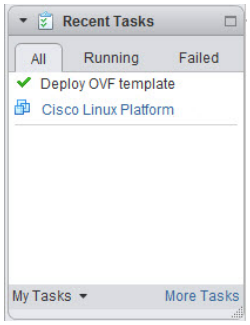
10 From the **Select virtual disk format** drop-down menu, select **Thick Provision Lazy Zeroed** and click **Next**.

11 Select the network that the deployed template should use (management network) and click **Next**. The Ready to Complete window appears.



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

13 Monitor the **Recent Tasks** area to verify that the VM deployed successfully.



14 Go to the next section.

Configuring the Linux Platform VM

Complete the following steps to configure the Linux platform virtual machine

1. Right-click the Linux Platform VM and select **Power On**.
2. Select and right-click the VM and select **Open Console**.
3. Log into the VM with the following credentials:

   User Name: admin

   Password: password

   Important: The admin user has full root privileges via the sudo command. Direct root access is not permitted.
4. When prompted to change the password. Please change it to something appropriate for your environment.

   Note: The new password you define will be used for all future VMs that you create from the Linux Platform template.
5. At the **(current) UNIX password** prompt, enter the default password which is **password**.
6. At the **New password** prompt, enter a new password.
7. At the **Retype new password** prompt, re-enter the new password.
8. Enter the following command to configure a static IP address for the Admin Node.

   Important: This is a temporary IP address and must be within the management network IP range provided by your system administrator.

   Command Syntax:

   ```
   sudo ifconfig eth0 [Temporary_IP] netmask [Netmask} up
   ```

   Example:

   ```
   [admin@platform ~]$ sudo ifconfig eth0 10.90.47.182 netmask
   255.255.252.0 up
   ```
9. If necessary, add a default route.

   Command Syntax:

   ```
   sudo route add default gw [Gateway_IP]
   ```

   Example:

   ```
   [admin@platform ~]$ sudo route add default gw 10.90.47.1
   ```
10. Close the VMware console window.
11. Using scp, copy the **cisco-vcs-deployment** zip file to the **/tmp** directory on the VM.

    Command Syntax:

    ```
    scp cisco-vcs-deployment*.zip admin@[temp_IP]:/tmp
    ```

Example:

```
[admin@platform ~]$ scp cisco-vcs-deployment-*.zip
admin@10.90.47.5:/tmp
```

12 Change to the **/tmp** directory.

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

13 Unzip the **cisco-vcs-deployment** zip file.

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

14 Enter the following command to execute the prepare script. This script prepares the VM for conversion into a VM template.

```
[admin@platform tmp]$ sudo
cisco-vcs-deployment*/scripts/prepare-linux-template.sh
```

Result: The VM will shut down.

Converting the VM Into a Template

Complete the following steps to convert the the VM into a template.

Important: Remember that this template will be used to deploy all future NextX VMs.

1. From the vSphere Web Client, right-click the VM and select **All vCenter Actions > Convert to Template**.
2. Monitor the **Recent Tasks** area until the status for this task changes to **Completed**.
3. Click the **Home** icon , and select **VMs and Templates**.
4. Verify that the Linux platform template you created is present.

3

Deploy the Admin Node Using the Linux Platform Template

Important: If you are deploying your virtual machine from a vSphere ESXi client, go to ***Deploy the Virtual Machine from an ESXi Client*** (on page 39).

This chapter describes how to deploy the Admin Node VM using the Linux platform template that you just created. Once the VM is created, you will customize the virtual hardware and the network interface to values required for your environment.

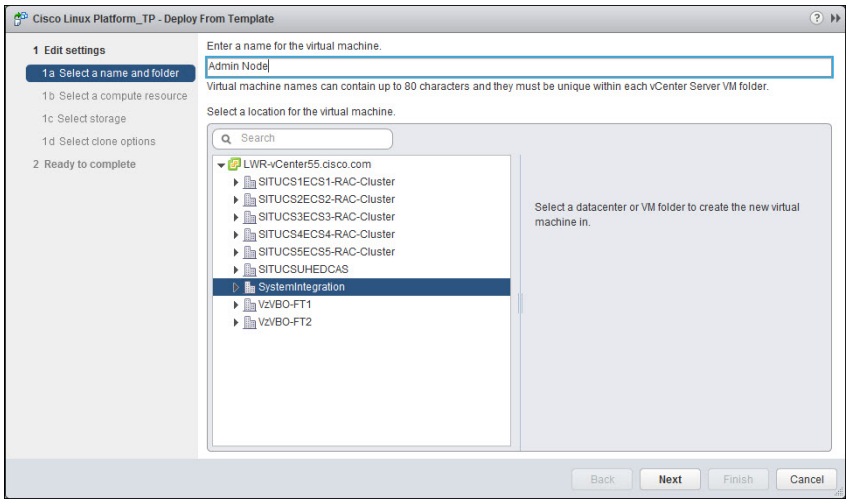
In This Chapter

Deploying the Admin Node From the Template

Complete the following steps to deploy the OVA.

Note: The screen shots in this procedure may differ if you are using a vSphere Web UI that is later than version 5.5.

1 From vCenter Web client, right-click the Linux platform template and select **Deploy VM from this Template**. The Deploy From Template window opens.

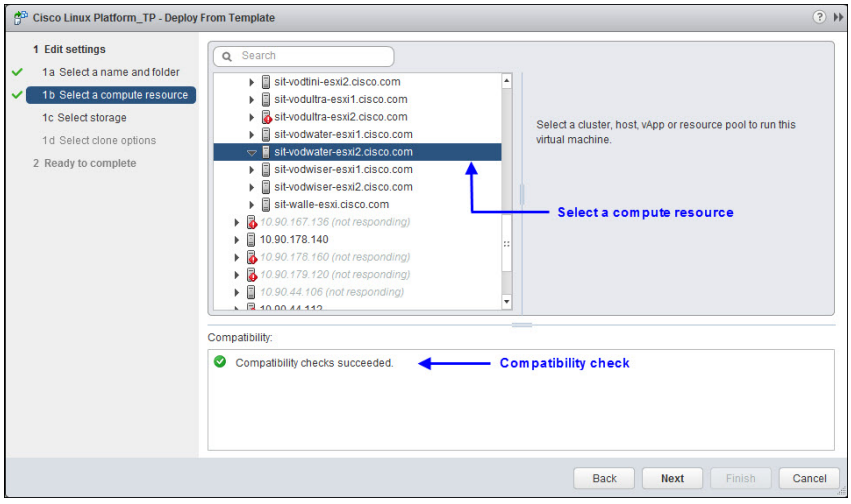


2 From the **Enter a name for this virtual machine** text box, enter a name that represents the Admin Node.

3 Select the appropriate host where you want to deploy the VM and click **Next**.

4 Select the compute resource where the Admin Node VM will reside.

Result: A compatibility check occurs and the results are displayed in the Compatibility area.



5 Click **Next**. The Select Storage window appears.

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

7 Click **Next** and then click **Next** again.

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

9 Monitor the **Recent Tasks** area to verify that the VM cloned successfully from the template.

10 Go to the next section in this chapter.

Reconfiguring the Admin Node Virtual Hardware

Complete the following steps to reconfigure the virtual hardware for the Admin Node virtual machine.

1 From the vSphere Web UI, click the **Home** icon, , and then click **Hosts and Clusters**.

2 Locate and select the Admin Node VM.

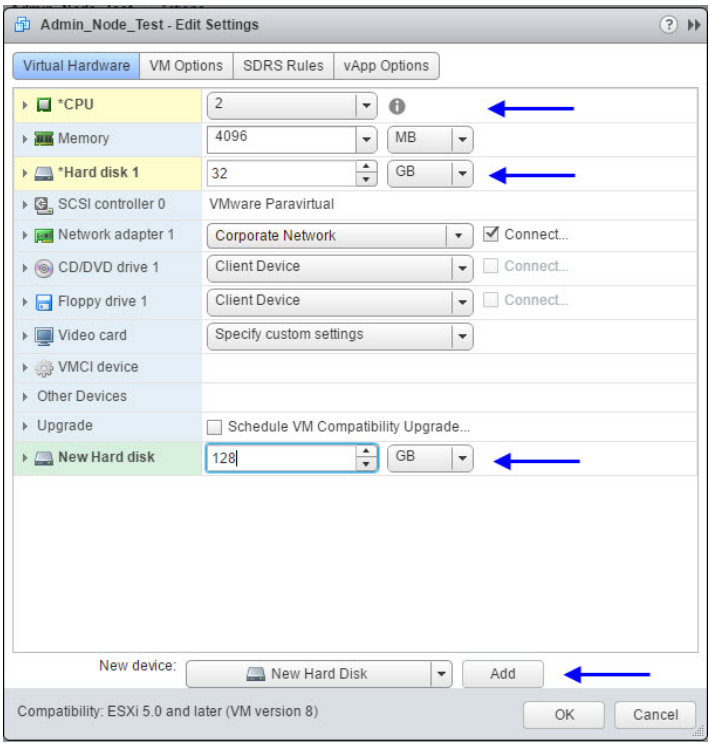
3 Right-click the VM and select **Edit Settings**. The Edit Settings window appears.

4 From the **CPU** row, decrease the number of CPUs to **2**.

5 From the **Hard disk 1** row, increase the size of hard disk to **32 GB**.

6 From the **New device** dropdown menu at the bottom of the window, select **New Hard Disk**. Then click **Add**. A row for the new hard disk is added to the virtual hardware list.

7 Modify the disk size for the new hard drive to **128 GB**.



8 Click **OK**.

9 Monitor the **Recent Tasks** area to confirm that the VM virtual hardware reconfigured successfully.

10 Go to the next section in this chapter.

Reconfiguring the Network Interface With a Static IP Address

Complete the following steps to reconfigure the network interface with a static IP address.

Note: Your network administrator should have provided you with a static IP address, default gateway and a network mask value. It is optional to add associated domain name servers (DNS).

1 Select and right-click the Admin Node VM and then select **Power On**.

2 Select and right-click the Admin Node VM again and select **Open Console**. A VMware console window opens in a new tab.

3 Log into VM with the following credentials.

Note: If you deployed the VM from the vSphere ESXi client, enter the default password which is **password**. Then respond to prompts to change the password.

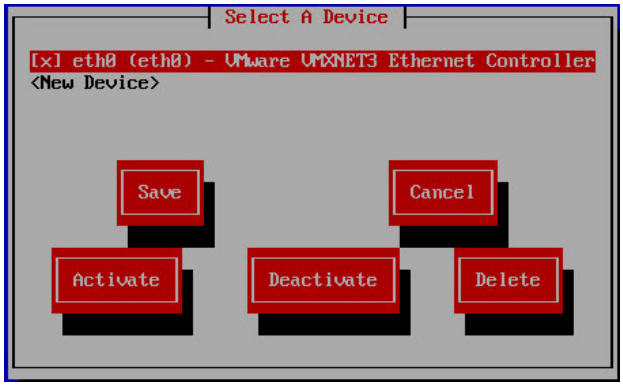
Username: admin

Password: [password created in *Configuring the Linux Platform VM* (on page 8)]

4 Type the following command line utility to configure the network and the DNS settings. The Select Action window appears.

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

5 Select **Device configuration** and press **Enter**. The Select a Device window appears.



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

7 Press the **Tab** key until **Use DHCP i**s highlighted. Then press the **Spacebar** to unselect this option.

8 Tab to each field to enter the following values.

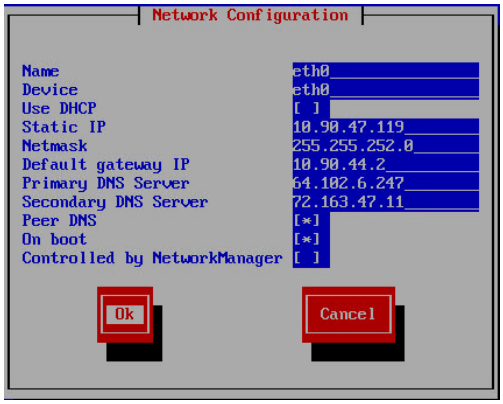
Note: DNS entries are optional.

- **Static IP**
- **Netmask**

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

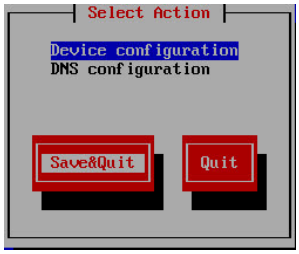
9 Verify that **Peer DNS** is selected.

10 Press the **Tab** key until **Controlled by NetworkManager i**s highlighted. Then press the **Spacebar** to unselect this option.



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

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



13 Click **Save&Quit**.

14 Restart the network service to update the interface configuration.

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

15 Close the VMware console window.

16 Using an SSH client, log into the Admin Node VM using the IP address you defined for eth0.

17 Go to *Install the Software* (on page 17).

4

Install the Software

This chapter provides the procedures to install the software on the Admin Node and to create the YUM repositories required for your system needs.

Important: This software should have been downloaded to your local PC as mentioned in ***Software Requirements*** (on page 3). If you have not downloaded the software, please do so now.

In This Chapter

Installing the Software

Complete the following procedure to install the software onto the Admin Node.

1. As **admin** user, enter the following command to create a staging directory for the deployment scripts.

   ```
   [admin@platform ~]$ sudo mkdir -p
   /opt/cisco/software/admin_node
   ```

2. Change the ownership of the **/opt/cisco/software** directory, on all files and directories in the path recursively, to **admin:admin**.

   ```
   [admin@platform ~]$ sudo chown -R admin:admin
   /opt/cisco/software
   ```

3. Enter the following command to change to the **/opt/cisco/software/admin_node** directory.

   ```
   [admin@platform ~]$ cd /opt/cisco/software/admin_node
   ```

4. Copy the CSCOadmin-node and cisco-vcs-deployment zip files from your local PC to the **/opt/cisco/software/admin_node/** directory.

5. Type the following command to verify that the following files are present in the directory.

   ```
   [admin@platform admin_node]$ ls -ltr
   ```

   ```
   total 11376
   -rw-r--r--.  1 admin admin 11615187  Jun 8  19:17  CSCOadmin-node-1.0.5.zip
   -rw-r--r--.  1 admin admin    30161  Jun 8  19:18  cisco-vcs-deployment-1.0.6.zip
   ```

6. Enter the following commands to unzip each file.

   ```
   [admin@platform admin_node]$ unzip CSCOadmin-node-*.zip
   [admin@platform admin_node]$ unzip cisco-vcs-deployment-*.zip
   ```

7. Enter the following command to install the admin node RPMs.

   ```
   [admin@platform admin_node]$ sudo rpm -Uvh *.rpm
   ```

   ```
   [admin@platform admin_node]$ sudo rpm -Uvh *.rpm
   warning: apr-1.3.9-5.el6_2.x86_64.rpm: Header V3 RSA/SHA1 Signature, key ID c105
   b9de: NOKEY
   warning: puppet-server-3.8.7-1.el6.noarch.rpm: Header V4 RSA/SHA1 Signature, key
    ID 4bd6ec30: NOKEY
   Preparing...                ########################################### [100%]
      1:apr                    ########################################### [ 10%]
      2:apr-util               ########################################### [ 20%]
      3:apr-util-ldap          ########################################### [ 30%]
      4:httpd-tools            ########################################### [ 40%]
      5:puppet-server          ########################################### [ 50%]
      6:mailcap                ########################################### [ 60%]
      7:httpd                  ########################################### [ 70%]
      8:cisco-vcs-puppet-module########################################### [ 80%]
      9:cisco-vcs-consul       ########################################### [ 90%]
     10:CSCOadmin-node         ########################################### [100%]
   [admin@platform admin_node]$
   ```

8. Go to the **/opt/cisco/software/admin_node/cisco-vcs-deployment-*/scripts** directory.

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

9. Edit the **adminnode.envfile** in a text editor.

   ```
   [admin@platform scripts]$ sudo vi adminnode.envfile
   ```

10 Enter the following values as they pertain to your system.

- admin_domain=
- hostname=
- ntp_servers=

Notes:

- Add an entry for ntp_servers. This entry is a comma separated (no space after comma) list of NTP servers for all nodes in the domain.
- The admin_domain, hostname and ntp_servers entries are mandatory parameters.
- The admin_domain entry is the DNS style domain that this admin node will control.
- Parameters specified on the command line overwrite values set in the envfile; DO NOT set parameters in both the environment file and on the command line.

Example:

```
admin_domain=vcs.prod
hostname=adminnode
ntp_servers=10.90.44.40,10.90.44.1
```

11 Save and close the file.

12 Enter the following command to execute the **deploy-adminnode.sh** script. This deploys the Admin Node onto the VMware infrastructure based on the environment files and parameters you have defined.

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

Result: The installation completes and the server reboots.

13 Log back into the Admin Node as **admin** user.

14 Enter the following command to verify that the CSCO packages are installed.

```
[admin@adminnode scripts]$ rpm -qa | grep CSCO
```

```
CSCOlxsecurity-2.0.4-1.201702271216.el6.noarch
CSCOadmin-node-1.0.3-1.201612201645.el6.noarch
CSCOlxplat-3.0.6-1.0.x86_64
CSCOcert-mgmnt-1.0.0-1.201705041647.el6.noarch
```

Installing the CSCOlxplat Base and Updates YUM Repos

Complete the following steps to install the CSCOlxplat base and updates YUM repositories on the Admin Node.

Note: You should have the CSCOlxplat rpms.tar file downloaded to your local PC. If you do not, refer to ***Software Requirements*** (on page 3) to download it now.

1 Copy the **CSCOlxplat-*.rpms.tar** file from your local PC to the **/opt/cisco/software/admin_node/** directory.

2 Go to the **/opt/cisco/software/admin_node/** directory.

3 Enter the following command to deploy the CSCOlxplat tar file.

Notes:

- Enter this command on one continuous line.
- The –s option defines the solution/version
- The –v option defines the CSCOlxplat version

Command Syntax:

```
/etc/puppet/modules/cisco_vcs/files/bootstrap/reposerver/bin/
vcs-admin init -s nextx/8.0 -v [version]
/opt/cisco/software/admin_node/CSCOlxplat-[version].rpms.tar
```

Example: This example uses CSCOlxplat-3.0.6.rpms.tar

```
[admin@admin_node admin_node]$ sudo
/etc/puppet/modules/cisco_vcs/files/bootstrap/reposerver/bin/
vcs-admin init -s nextx/8.0 -v 3.0.6
/opt/cisco/software/admin_node/CSCOlxplat-3.0.6.rpms.tar
```

Result: When the script completes, the VM automatically reboots.

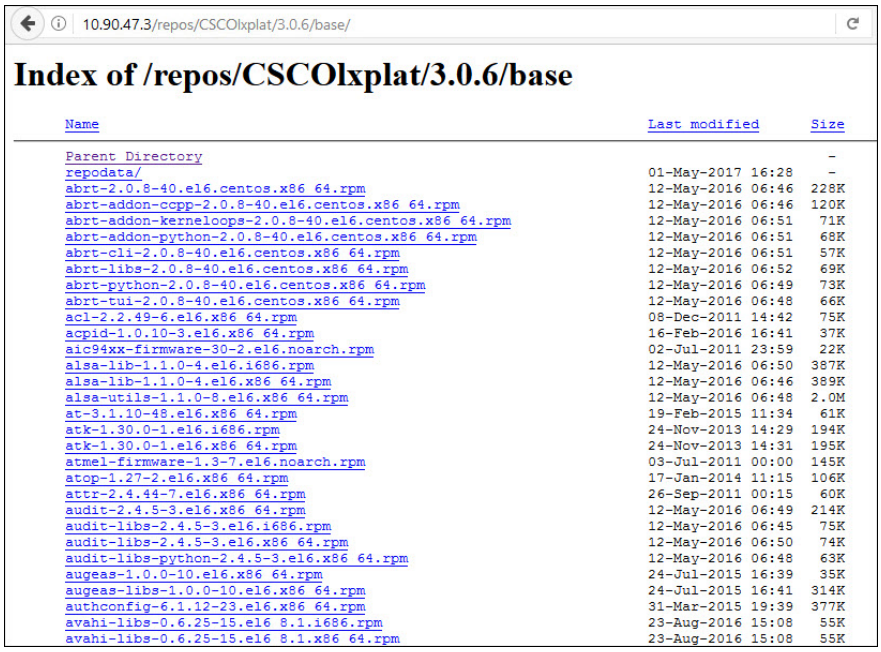
4 Using the Admin Node IP address, browse to the repo URL via a Web browser and verify that the RPMs are present.

Command Syntax:

```
http://[admin node IP]/repos/CSCOlxplat/[version]/base/
```

Example:

`http://10.90.47.3/repos/CSCOlxplat/3.0.6/base/`



Deploying the Repo for the Application Packages

Complete the following procedure to deploy the tar files for the application packages you wish to install.

Note: You should have already downloaded the appropriate tar files to your local PC. If you have not, refer to ***Software Requirements*** (on page 3) to do so now.

1 From an SSH client, log back into the Admin Node as **admin** user.

2 Create the following directory for the software packages you plan to deploy.

```
[admin@adminnode ~]$ mkdir /opt/cisco/software/nextx-8.0
```

3 Copy the appropriate application tar files from your local PC to the **/opt/cisco/software/nextx-8.0** directory.

4 Enter the following command to deploy the solution repos.

Note: The example uses a wildcard to download all of the repos at once.

```
[admin@adminnode ~]$ sudo
/opt/cisco/vcs/bootstrap/bin/vcs-admin deploy-bundle
/opt/cisco/software/nextx-8.0/*.tar
```

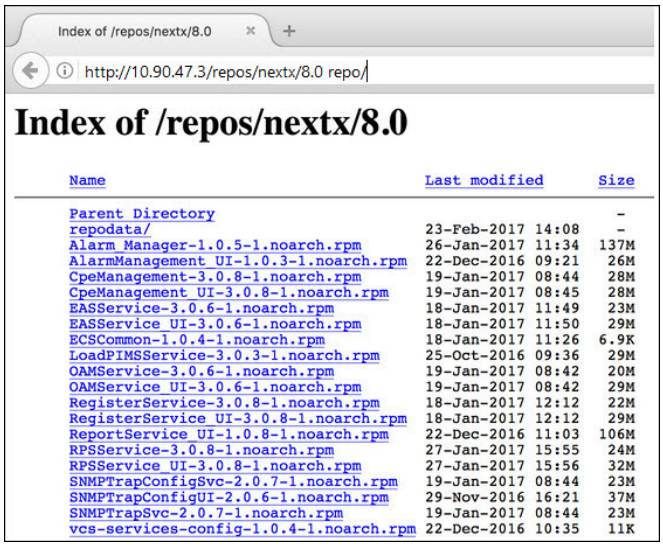
5 Using the Admin Node IP address, browse to the **nextx/8.0** repo via a Web browser and verify that the appropriate RPMs are present.

Command Syntax:

```
http://[admin node IP]/repos/nextx/8.0/
```

Example:

```
http://10.90.47.3/repos/nextx/8.0/
```



5

Create Environment Files for NextX Nodes

This chapter includes the procedure to create the environment file for all nodes in your NextX system. The environment file is required to generate the certificate/key pair for certificates signed by either an internal root CA or an external CA.

In This Chapter

Prerequisites for Creating Environment Files

To create the environment file for each node you plan to build in your NextX system, you must have the following information:

- The hostnames for each node
- The fully qualified domain names (FQDN) for each node
- The IP addresses for each node

Creating the Client VM Environment Files

Complete the following procedure to create the environment files for each respective node in your NextX system.

Important: Each environment file includes a **NODETYPE=** field. Depending on the node, you will set this to one of the following values:

- boa
- ec
- ecs
- dtacs
- vcs
- consul

Note: This example is written to create the environment file for an EC node with the hostname vodwater.

1 As **admin** user, enter the following command to change to the **/opt/cisco/ca** directory.

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

2 Enter the following command to copy the server.example.env file to a **[hostname].env** file where [hostname] is the unique hostname for the node.

Command Syntax:

```
sudo cp server.example.env [hostname].env
```

Example:

```
[admin@adminnode ca]$ sudo cp server.example.env vodwater.env
```

3 Open the **[hostname].env** file in a text editor.

Command Syntax:

```
vi [hostname].env
```

Example:

```
[admin@adminnode ca]$ sudo vi vodwater.env
```

4 Go the the **NODETYPE=** line and delete all values except for the value that represents the respective node.

Example: environment file is being defined for an EC

```
NODETYPE=ec
```

5 Next, modify the values to the right of the equals sign for the following fields.

```
C=Country (2 letters)
ST=State (spelled out)
L=City ( spelling out)
O=Organization (spelled out)
OU=Department (spelled out)
CN=Common name (FQDN)
```

Note: The CN should be the Fully qualified domain name (FQDN) (i.e. host.achme.com).

```
emailAddress=somebody@somecompany.com
DNS.1 = FQDN 1
```

Note: The FDQN as found in DNS; this value should be the same as the CN value.

```
#DNS.2 = FQDN 2 (if applicable)
IP.1 = IP address 1 of the ec node
#IP.2 = valid IP address 2 (if applicable)
```

Note: If this node uses a virtual name and IP for failover purposes, uncomment the DNS.2 and the IP.2 lines and provide the virtual name as found in DNS and VIP.

Example:

6 Save and close the file.

7 Repeat Steps 2 through 6 for each node you plan to deploy in your NextX system.

Note: Remember to modify the **NODETYPE=** entry for each environment file you create. It must match the node that the file is defined for.

8 Go to ***Create NextX X.509 Certificates*** (on page 27).

6

Create NextX X.509 Certificates

This section describes the procedures to either create an internal or external root CA on the Admin Node. as well as to create certificates for all nodes in your NextX system.

Notes:

- These procedures should be completed as **root** user.
- The NextX CA root key and certificate will be stored in the /etc/pki/CA directory.
- The HTTPs X.509 certificates for each NextX node will be stored in the /etc/pki/CA/certs directory.
- The HTTPs X.509 keys for each NextX node will be stored in the /etc/pki/CA/private directory.

Prerequisite: The **/home/admin/.ssh** directory *must* exist on the Admin Node before you execute the manageCerts script. If it does not exist, as **admin** user, type `$ssh admin@localhost`. This creates the .ssh directory along with the correct owner and privileges.

In This Chapter

Create and Generate Certificates Using an Internal CA

Important: If you are using an external signing authority, skip this section and go to *Create and Generate Certificates Using an External CA* (on page 34).

This section provides the procedures to create an internal root CA. This internal root CA will then be used to sign the certificates you generate for each node that will be built in your NextX system. This includes the following nodes:

- EC 8.0
- DTACS 5.0
- ECS 3.0
  - Consul
  - VCS Console
  - ECS
  - BOA

Creating the Root CA Private Key and Certificate

Important: This procedure should only be executed once for a NextX system. It is not necessary to create the NextX X.509 CA certificates more than once on the Admin Node.

Complete the following procedure to create a root CA on the Admin Node. This will be used to sign the NextX X.509 certificates. The root CA consists of the root key and the root certificate.

The root key is required to create the root certificate and should be protected with a passphrase. The passphrase prevents the root key from being in the clear when it is not in use. It is best practice to keep the root key secure as anyone in possession of the root key can issue trusted certificates.

1 As **admin** user, go to the **/opt/cisco/ca** directory.

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

2 Enter the following command to copy the certificate.authority.env file to **rootca.env**.

```
[admin@adminnode ca]$ sudo cp certificate.authority.env
rootca.env
```

3 Open the **rootca.env** file in a text editor.

```
[admin@adminnode ca]$ sudo vi rootca.env
```

4 Modify the values to the right of the equals sign for each field *except* the CN field. This value must remain as "NextX CA".

Example:

```
#This file should be used to create the NextX CA
# Replace the values below with appropriate values for your configuration
# Note that the CN will always be "NextX CA" when creating the NextX CA
C=US
ST=GA
L=Lawrenceville
O=Cisco
OU=SPVTG
CN="NextX CA"
emailAddress=johndoe@cisco.com
```

5 Save and close the file.

6 Enter the following command and press **Enter** to create the self-signed root CA.

```
[admin@adminnode ca]$ sudo ./manageCerts -c rootca.env
```

Example:

```
==========20170522.082612==========
./manageCerts -c rootca.env
validating parameters for the DN...
Creating the Root Pair for Cisco NextX CA
You will need to enter a passphrase for the Root key
openssl req -x509 -extensions v3_ca -days 1825 -sha384 -newkey rsa:3072 -keyout /etc/pki/CA/c
akey.pem -out /etc/pki/CA/cacert.pem
    -subj /C=US/ST=GA/L=Atlanta/O=Cisco/OU=SPVTG/CN=NextX CA/emailAddress=tammphil@cisco.com
Generating a 3072 bit RSA private key
..++
.....................................................++
writing new private key to '/etc/pki/CA/cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

7 When prompted, enter a passphrase for the root key.

Important: You will need to safely guard the private key password and yet make it accessible to create or revoke future certificates.

Results:

- The root key (e.g. cakey.pem) and the root certificate (e.g. cacert.pem) are generated and saved to the /etc/pki/CA directory.
- The Certificate Revocation List (CRL) is generated.

8 When prompted for the passphrase again, re-enter the password for the root key. The script completes.

9 Review the log, **/var/log/manageCerts[date].log**, in the **/var/log/** directory.

Confirming the Root Certificate Parameters

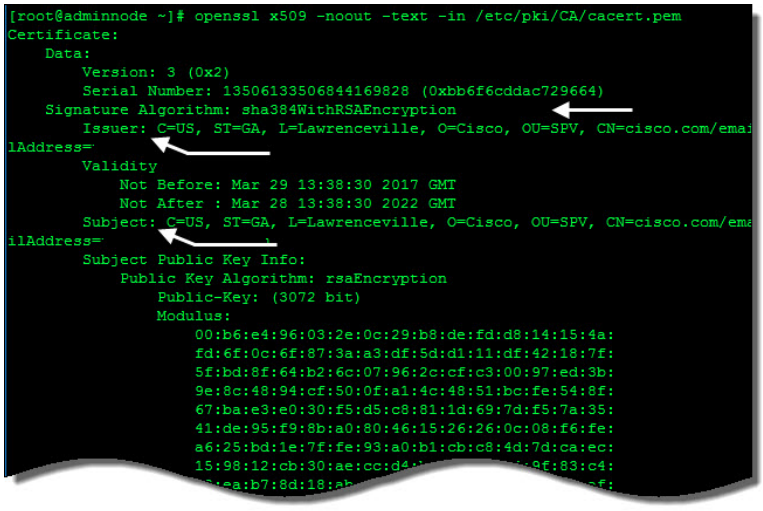
1 Execute the following command to confirm the information defined for the root certificate.

```
[admin@adminnode ca]$ sudo /usr/bin/openssl x509 -noout -text
-in /etc/pki/CA/cacert.pem
```

2 Verify the following information in the output from Step 1.

- Signature Alogrithm (should be sha384WithRSAEncryption)
- Issuer and Subject lines should identical
- Validity of the certificate
- Subject of the certificate
- CA:TRUE

Example:



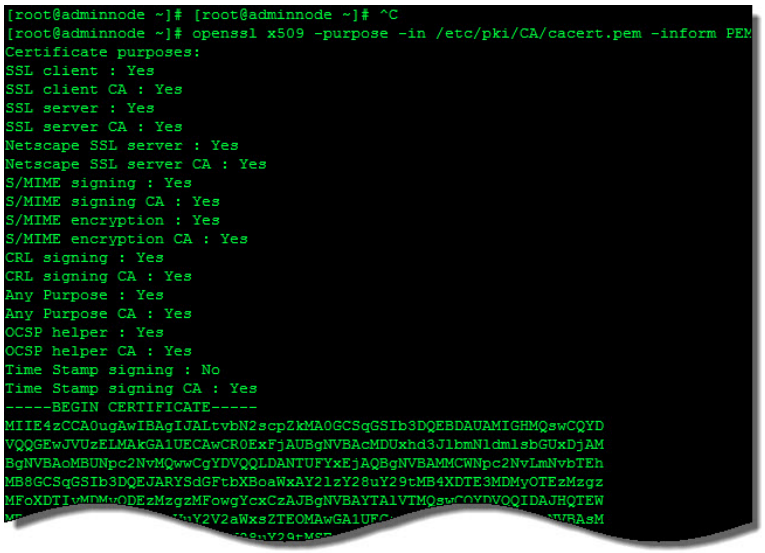
3 Go to the next section.

Confirming Root Privileges for the Root CA

1 Execute following command to verify the privileges defined for the newly created CA.

```
[admin@adminnode CA]$ sudo /usr/bin/openssl x509 -purpose -in
/etc/pki/CA/cacert.pem -inform PEM
```

2 Review the output; it should look similar to the following example.



3 Go to next section.

Generating Certificates for NextX VMs Using an Internal Root CA

Important: Before continuing with this section, make sure that you created the appropriate .env environment files for each NextX node. If you have not yet done so, refer to ***Create Environment Files for NextX Nodes*** (on page 23) to create them now.

Complete the following steps to generate the certificate files for each node you plan to deploy in your NextX system using the internal root CA on the Admin Node. The certificates will be signed by the internal root CA on the Admin Node.

Note: This procedure is executed on the Admin Node. You should still be logged into the terminal window for the Admin Node from the previous procedure.

1 From the terminal window for the Admin Node, change to the following directory.

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

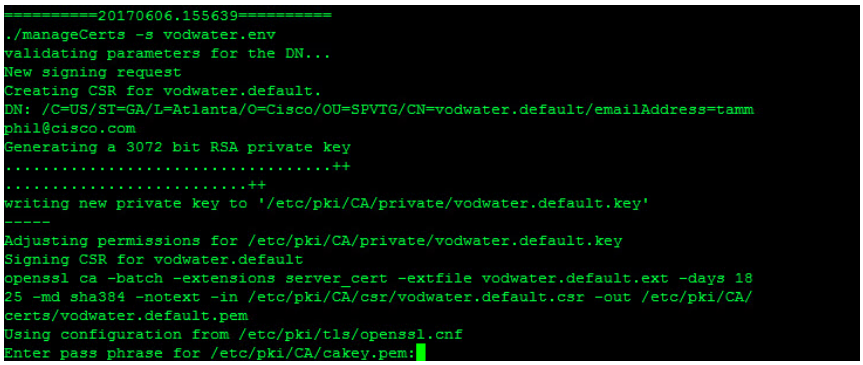
2 Enter the following command and press **Enter** to generate the self-signed certificate and key pair for the appropriate NextX node.

Command Syntax:

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

Example:

```
[admin@adminnode ca]$ sudo ./manageCerts -s vodwater.env
```



Results:

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

3 When prompted, enter the pass phrase for the root CA key, cakey.pem and then press **Enter**.

4 When prompted again for the passphrase, re-enter the passphrase and press **Enter**.

Results:

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

5 When prompted to transfer the private key and certificate to the appropriate host, type **n** and press **Enter**. The script completes and a **./manageCerts finished** message displays.

Important: Do not push the certificates to the host as the host nodes are not yet built.

```
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Subject Alternative Name:
                DNS:vodwater.default, IP Address:10.90.167.184
Certificate is to be certified until Jun  5 19:57:27 2022 GMT (1825 days)

Write out database with 1 new entries
Data Base Updated
CSR for vodwater.default successfully signed
vodwater.default.pem located in /etc/pki/CA/certs
Done

Do you want to try and transfer /etc/pki/CA/private/vodwater.default.key and /etc/pki/CA/ce
ts/vodwater.default.pem to vodwater.default (y/n)?n
Done

Please check log file [/var/log/manageCerts20170606.log] for results

./manageCerts finished
```

6 Enter the following command to verify that the certificate for the node is now present in the **/etc/pki/CA/certs** directory.

```
[admin@adminnode ca]$ ls -ltr /etc/pki/CA/certs
```

Example:

```
total 8
-rw-r--r--. 1 root root 2065 Jun  6 08:44 berlin_hosta.cfet.berlin.pem
-rw-r--r--. 1 root root 2041 Jun  6 15:57 vodwater.default.pem
```

New certificate

7 Enter the following command to verify that the certificate for the node is now present in the **/etc/pki/CA/private** directory.

```
[admin@adminnode ca]$ ls -ltr /etc/pki/CA/private
```

Example:

```
total 8
-rw-r--r--. 1 root root 2484 Jun  6 08:44 berlin_hosta.cfet.berlin.key
-r--------. 1 root root 2484 Jun  6 15:56 vodwater.default.key
```

New key

8 Repeat Steps 1 through 6 for each node you plan to deploy in your NextX system.

Note: You should have a .env file created for each of the nodes.

9 Refer to one of the following documents to start deploying the appropriate nodes for your NextX system.

- ***EC 8.0 Installation and Migration User Guide***
- ***DTACS 5.0 Installation and Migration Guide***
- ***Explorer Controller Suite 3.0 Installation and Upgrade Guide***

Create and Generate Certificates Using an External CA

Important: If you are using an internal signing authority, skip this section and go to *Create and Generate Certificates Using an Internal CA* (on page 28).

This section provides the procedures to create the root CA using an external signing authority and to generate the certificates for all nodes you plan to build in your NextX system. Once the certificates are generated, you will send them to your signing authority, who will then return signed certificates back to you.

Certificates can be generated for the following node types:

- EC 8.0
- DTACS 5.0
- ECS 3.0
  - Consul
  - VCS Console
  - ECS
  - BOA

Generating Certificates for NextX VMs Using an External Root CA

Important: Before continuing with this section, make sure that you created the appropriate .env environment files for each NextX node. If you have not yet done so, refer to *Create Environment Files for NextX Nodes* (on page 23) to create them now.

Complete the following steps to generate the certificate files for each node you plan to deploy in your NextX system using an external signing authority.

Note: This procedure is executed on the Admin Node. You should still be logged into the terminal window for the Admin Node from the previous procedure.

1 Using the **[hostname].env** file, enter the following command on the Admin Node, to generate a certificate signing request for the appropriate node. The CSR path will be displayed when the process is completed.

Command Syntax:

```
./manageCerts -g [hostname].env
```

Example:

```
[admin@adminnode ca]$ sudo ./manageCerts -g vodwater.env
```

```
==========20170522.203147==========
./manageCerts -g vodwater2.env
validating parameters for the DN...
New CSR for vodwater2.domain to be signed by external CA
DN: /C=US/ST=GA/L=Atlanta/O=Cisco/OU=SPVTG/CN=vodwater2.domain/emailAddress=tammphil@cisco.com
cat /etc/pki/tls/openssl.cnf vodwater2.domain.ext | grep -v authorityKey > /tmp/25857.ext
openssl req -nodes -newkey rsa:3072 -sha384 -keyout /etc/pki/CA/private/vodwater2.domain.key -
out /etc/pki/CA/csr/vodwater2.domain.csr -reqexts server_cert -subj /C=US/ST=GA/L=Atlanta/O=Ci
sco/OU=SPVTG/CN=vodwater2.domain/emailAddress=tammphil@cisco.com -config /tmp/25857.ext
Generating a 3072 bit RSA private key
.....................++
.....................................................................++
writing new private key to '/etc/pki/CA/private/vodwater2.domain.key'
-----
Adjusting permissions for /etc/pki/CA/private/vodwater2.domain.key
Key and CSR located at /etc/pki/CA/private/vodwater2.domain.key and /etc/pki/CA/csr/vodwater2.
domain.csr

Please check log file [/var/log/manageCerts20170522.log] for results

./manageCerts finished
```

2 Repeat Step 1 for each node in your system.

Sending CSR Files to the External Certificate Authority

Complete the following steps to send the all of the CSR files to your external certificate authority.

1 Send all of the **/etc/pki/CA/csr/[FQDN].csr** files to your signing authority. Your signing authority will return a signed certificates to you.

Notes:

- The "Key Usage" X509v3 extension in the issued certificate MUST contain "Digital Signature" and "Key Encipherment", if specified.
- The "Extended Key Usage" X509v3 extension in the issued certificate MUST contain "TLS Web Server Authentication" and "TLS Web Client Authentication", if specified.
- The CSR will contain these extensions and associated values but it is up to the CA to include them in the signed certificate

2 Retrieve the signed certificates and save them to your local PC.

Copying the Signed Certificates to the Admin Node

Complete the following steps to copy all of the signed certificate files to your Admin Node.

1 Copy the signed certificate, in PEM format, from your PC to the **/etc/pki/CA/certs/CN.pem** (i.e. vodwater.domain.pem) directory on the Admin Node.

Note: The certificate returned may be a series of certificates, from the node up to the root, however, it will all will be in one file. Make sure to include only the node certificate in the /etc/pki/CA/certs/CN.pem file.

Example Output:

2 From the terminal window for the Admin Node, execute the following command to verify each signed node certificate.

Command Syntax:

```
openssl x509 -noout -text -in /etc/pki/CA/certs/[cert.pem]
```

Example:

```
[admin@adminnode ca]$ sudo openssl x509 -noout -text -in
/etc/pki/CA/certs/vodwater.domain.pem
```

Notes:

- The Subject common name (CN) must match the hostname of the node.
- The current date must fall within Validity dates.

Example Output:

3 Repeat Step 2 for each signed certificate.

Creating a CA Certificate Chain Using an External Certificate Authority

Important: This procedure should only be executed once for a NextX system. It is not necessary to create the CA certificate chain more than once on the Admin Node.

Complete the following steps to create the CA certificate chain file when using an external certificate authority to sign NextX X.509 certificates.

1 Obtain the CA certificate chain in PEM format from the Certificate Authority you are using for signing SSL certificates.

2 As **admin** user, change to the **/etc/pki/CA** directory.

```
[admin@adminnode ~]$ cd /etc/pki/CA
```

3 Copy the concatenated CA certificate chain file to **/etc/pki/CA/cacert.pem** on the Admin Node.

Important:

- The CA certificate chain can contain one or more individual CA certificates. It must have the root CA certificate and will have all intermediate CA certificates between the root and the intermediate CA that signed the end-entity certificate.
- The certificate order for the concatenated file must have the signing intermediate CA at the top of the file and the root CA certificate at the bottom of the file.
- The certificate management script will extract the root CA certificate from the bottom of the file to populate the trust store on a node.

4 Execute the following command to verify the order of the CA certificates in the cacert.pem file.

```
[admin@adminnode ~]$ sudo openssl crl2pkcs7 -nocrl -certfile
"cacert.pem" | openssl pkcs7 -print_certs -noout
```

Example Output:

```
subject=/C=US/ST=Georgia/L=Lawrenceville/O=Cisco/OU=VCU Engineering/CN=NextX Intermediate
 CA/emailAddress=nextxintca@ted.com
issuer=/C=US/ST=GA/L=Lawrenceville/O=Cisco/OU=VCS Engineering/CN=NextXRootCA/emailAddress
=nextxrootca@cisco.com
subject=/C=US/ST=GA/L=Lawrenceville/O=Cisco/OU=VCS Engineering/CN=NextXRootCA/emailAddres
s=nextxrootca@cisco.com
issuer=/C=US/ST=GA/L=Lawrenceville/O=Cisco/OU=VCS Engineering/CN=NextXRootCA/emailAddress
=nextxrootca@cisco.com
```

5 Refer to one of the following documents to start deploying the appropriate nodes for your NextX system.

- ***EC 8.0 Installation and Migration User Guide***
- ***DTACS 5.0 Installation and Migration Guide***
- ***Explorer Controller Suite 3.0 Installation and Upgrade Guide***

A

Deploy the Virtual Machine from an ESXi Client

This appendix describes how to deploy the Admin Node using an ESXi client.

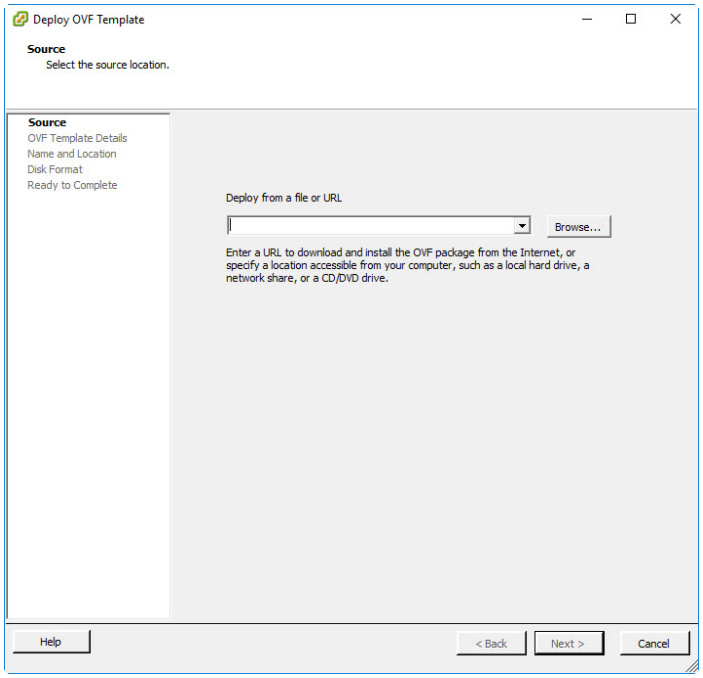
Important: The following software should have been downloaded to your local PC as mentioned in ***Software Requirements*** (on page 3). If you have not downloaded this software, please do so now.

- CSCOlxplat-[VERSION].ova
- cisco-vcs-deployment-[VERSION].zip
- cisco-vcs-infra-[VERSION].tar

In This Appendix

Deploying the Virtual Machine from an ESXi Client

1. Log on to the ESXi client.
2. From the File menu, select **Deploy OVF Template**. The Source window displays.



3. Click **Browse** and navigate to the directory where the Cisco platform OVA (i.e. CSCOlxplat-3.0.6.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. In the **Name** text box, enter a name to describe the Admin Node VM. Then click **Next**. The Disk Format window displays.
9. From the **Configuration** dropdown menu, select the **4CPU 4RAM 20GB** disk configuration and click **Next**. The Disk Format window displays.
10. Click the **Thick Provision Lazy Zeroed** radio button and click **Next**. The Network Mapping window displays.
11. Select the network that the deployed template should use (management network) and click **Next**. The Ready to Complete window appears. The virtual machine appears in the vSphere Client Inventory view.
12. After the **Success** message appears, click **Close**.
13. Go to the next section in this appendix.

Reconfiguring the Admin Node Virtual Hardware from an ESXi Client

Complete the following procedure to reconfigure the virtual hardware using an ESXi client.

1. In the left area of the ESXi client window, click the "**+**" icon to expand the host inventory.
2. Select and right-click the new VM and click **Edit Settings**. The Edit Settings window appears.
3. Click **CPUs** and then from the Number of virtual sockets dropdown list, select **2**.
4. Click **Hard disk 1** and in the **Disk Provisioning** area, change the Provisioned Size to **32** GB.
5. Click the **Add** button. The Device Type window opens.
6. Select **Hard Disk** and then click **Next**.
7. Maintain the **Create a new virtual disk** selection and click **Next**.
8. Change the Disk Size to **128** and maintain the other default selections. Then click **Next**.
9. Click **Next** again. The Ready to Complete window displays.
10. Review the options and then click **Finish**. The new hard disk is added to the virtual machine list.
11. Click the **Add** button again and select **Ethernet Adapter**. Then click **Next**.
12. 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.
13. Review the details and then click **OK**. The VM is reconfigured.
14. Review the options and then click **Finish**. The new Ethernet adapter is added to the virtual machine list.
15. Go to the next section in this appendix.

Configuring a Static IP Address Using the ESXi Client

Complete the following procedure to configure a static IP address on the Admin Node.

1 From the ESXi client, right-click the VM and select **Power On**.

2 Right-click the VM again and select **Open Console**. A new console window appears.

3 Log into the VM with the following credentials.

User Name: admin

Password: password

Important: The admin user has full root privileges via the sudo command. Direct root access is not permitted.

4 When prompted to change the password, enter a password that is appropriate for your environment.

5 At the **(current) UNIX password** prompt, enter the default password which is **password**.

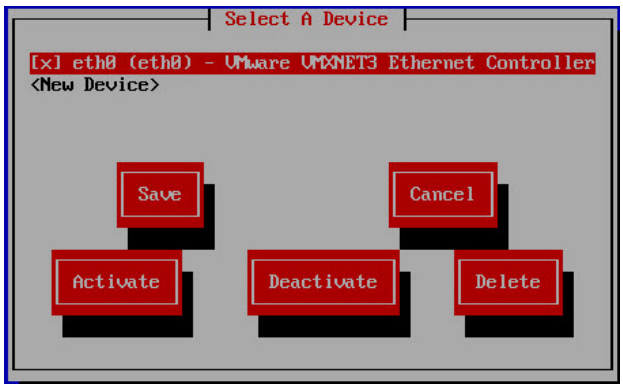
6 At the **New password** prompt, enter a new password.

7 At the **Retype new password** prompt, re-enter the new password. An admin password prompt appears/

8 Type the following command line utility to configure the network and the DNS settings. The Select Action window appears.

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

9 Select **Device configuration** and press **Enter**. The Select a Device window appears.



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

11 Press the **Tab** key until **Use DHCP i**s highlighted. Then press the **Spacebar** to unselect this option.

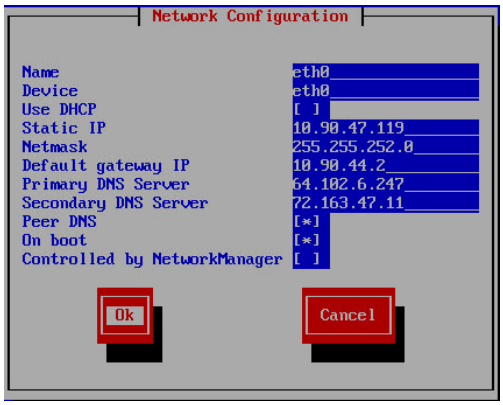
12 Tab to each field to enter the following values.

Note: DNS entries are optional.

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

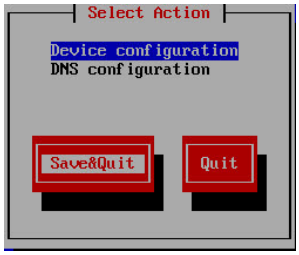
13 Verify that **Peer DNS** is selected.

14 Press the **Tab** key until **Controlled by NetworkManager i**s highlighted. Then press the **Spacebar** to unselect this option.



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

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



17 Click **Save&Quit**.

18 Restart the network service to update the interface configuration.

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

19 Close the VMware console window.

20 Using an SSH client, log into the Admin Node VM using the IP address you defined for eth0.

21 Go to *Install the Software* (on page 17).

B

Verify Inter-node Encrypted Communication

This appendix describes the procedure to the verify encrypted communication status between the NextX nodes that are installed on your system.

In This Appendix

Verifying Inter-Node Encrypted Communication

Important: Do not execute this procedure until all nodes in your NextX system are installed with their respective X.509 certificates.

Complete the following steps to verify communication encrypted with the NextX X.509 certificates.

1 As **admin** user, change to the **/opt/cisco/ca** directory.

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

2 Enter the following command to verify the inter-node communication encrypted with the deployed X.509 certificates.

```
[admin@adminnode ca]$ sudo ./checkConnnect
```

Example Output:

```
==========20170531.174401==========
./checkConnect
Found boa @  10.90.47.118
Found ec @  10.90.178.166 10.90.45.181 10.90.45.182
Found ecs @  10.90.47.159 10.90.47.97
Found vcsconsole @  10.90.47.145 10.90.47.189
Found consulserver @  10.90.47.109 10.90.47.177 10.90.47.108
Found dtacs @  10.90.47.104

boa ec 443 /dncs/soap/bossreq /dncs/soap/bossrep /dncs/soap/bosssync /dncs/soap/loadPIMS /DataAccess
... succeeded from boa@10.90.47.118 to ec@10.90.178.166 using port 443
... succeeded from boa@10.90.47.118 to ec@10.90.45.181 using port 443
... succeeded from boa@10.90.47.118 to ec@10.90.45.182 using port 443

ecs boa 8443 /CpeManagement/bosssync /BillingAdaptor/BossreqDocument /LoadPIMSService/loadPIMS
... succeeded from ecs@10.90.47.159 to boa@10.90.47.118 using port 8443
... succeeded from ecs@10.90.47.97 to boa@10.90.47.118 using port 8443
.
.
ec ecs 8443 /RegisterService /EASService/eas/SendMessage /OAM /OAMbackuprestore
... succeeded from ec@10.90.178.166 to ecs@10.90.47.159 using port 8443
... succeeded from ec@10.90.45.181 to ecs@10.90.47.159 using port 8443
... succeeded from ec@10.90.45.182 to ecs@10.90.47.159 using port 8443
... succeeded from ec@10.90.178.166 to ecs@10.90.47.97 using port 8443
... succeeded from ec@10.90.45.181 to ecs@10.90.47.97 using port 8443
... succeeded from ec@10.90.45.182 to ecs@10.90.47.97 using port 8443
.
.
Checking consul connections
Checking 10.90.47.118
Checking 10.90.178.166
.
.

Please check log file [/var/log/checkConnect20170531.log] for results

./checkConnect finished
```

3 Were any errors reported?

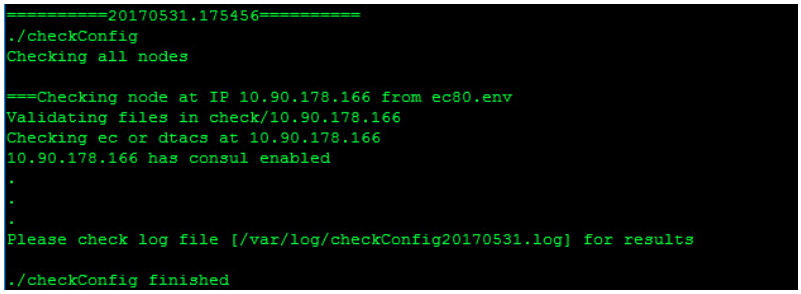
- If **no**, you have completed this procedure.
- If **yes**, go to the next step.

4 Enter the following command to verify the X.509 certificate configuration on each node.

Note: Make sure you execute this command on the appropriate node in your NextX system.

```
[admin@adminnode ca]$ ./checkConfig
```

Example Output:



5 Did any errors display?

- If **yes**, attempt to resolve the issues. If you cannot resolve the issues, contact Cisco Services.
- If **no**, contact Cisco Services.

C

Update the Admin Node

This appendix includes the procedures to update the Admin Node when there are changes to any of the following files:

- admin-node-[VERSION].zip
- CSCOlxplat-[VERSION].rpms.tar
- CSCOcert-mgmnt-[VERSION].rpm

In This Appendix

Updating the admin-node ZIP File or the CSCOxplat TAR File

Important: If the admin-node ZIP file and/or the CSCOxplat tar file are updated, you are *required* to deploy a new Admin Node.

Complete the following procedures to build a new Admin Node VM.

1 Download the **admin-node-[VERSION].zip** file and/or the **CSCOlxplat-[VERSION].rpms.tar** file from your customer-specific forum on Cisco's File Exchange Server and save it to a local directory that is accessible to vSphere or the ESXi host.

2 Copy the following certificates from the current Admin Node to a local directory.

If Using an Internal Certificate Authority

- /opt/cisco/ca/rootca.env
- /etc/pki/CA/cacert.pem
- /etc/pki/CA/cakey.pem
- /etc/pki/CA/crl/nextXca.crl.pem

If Using an External Certificate Authority

- /etc/pki/CA/certs/[CN].pem files (i.e. vodwater.domain.pem)
- /etc/pki/CA/cacert.pem

3 As **admin** user, type the following command to shutdown the current Admin Node VM.

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

4 Complete the procedures in Chapter 2, ***Deploy the Admin Node Using the Linux Platform Template*** (on page 11).

Note: During these procedures you will define a static IP address for the eth0 interface. Make sure to use the same IP address as the original Admin Node.

5 Complete the procedures in Chapter 3, ***Install the Software*** (on page 17).

Important: Do *not* complete any procedures in the ***Create NextX X.509 Certificates*** (on page 27).

6 Copy the following certificates from your local directory to the new Admin Node.

Note: You must copy the files to the same directory path where they were in the previous release (see Step 2).

7 Complete the procedures in Appendix B, ***Verify Inter-node Encrypted Communication*** (on page 45).

Updating the CSCOcert-mgmnt RPM File

Important: If any other RPM packages or the CSCOlxplat requires an update, you must deploy a new Admin Node. Skip this section and go to ***Updating the admin-node ZIP File or the CSCOxplat TAR File*** (on page 50).

Complete the following procedure to update *only* the CSCOcert-mgmnt-[VERSION].rpm package on the Admin Node.

1. Download the **CSCOcert-mgmnt-[VERSION].rpm** file from your customer-specific forum on Cisco's File Exchange Server and save it to a local directory that is accessible to vSphere or the ESXi host.
2. As **admin** user on the Admin Node, enter the following command to verify the current version of the **CSCOcert-mgmnt** package.

   ```
   [admin@adminnode ~]$ sudo rpm -qa CSCOcert-mgmnt
   ```

   Example Output:

   ```
   [root@adminnode admin_node]# ls| grep cert
   CSCOcert-mgmnt-1.0.1-1.201705241503.el6.noarch
   ```

3. Create a new directory in the **/opt/cisco/software** directory where you want to save the new CSCOcert RPM.

   Command Syntax:

   ```
   mkdir /opt/cisco/software/[New_Directory]
   ```

   Example:

   ```
   [admin@adminnode ~]$ sudo mkdir
   /opt/cisco/software/CSCOcert_upgrade
   ```

4. Copy the **CSCOcert-mgmnt-[VERSION].rpm** file from your local directory to the new directory created in Step 3.
5. Go to the directory you created in Step 3.

   Command Syntax:

   ```
   cd /opt/cisco/software/[New_Directory]
   ```

   Example:

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

6. Enter the following command to update the **CSCOcert-mgmnt** package. The update environment is set up and dependencies to upgrade the package are verified.

   Command Syntax:

   ```
   yum update CSCOcert-mgmnt-[VERSION].rpm
   ```

Example:

```
[admin@adminnode ~]$ sudo yum update
CSCOcert-mgmnt-1.0.2-1.rpm
```

```
[root@adminnode CSCOcert_upgrade]# yum update CSCOcert-mgmnt-1.0.2-1.rpm
Loaded plugins: fastestmirror, presto, security
Setting up Update Process
Examining CSCOcert-mgmnt-1.0.2-1.rpm: CSCOcert-mgmnt-1.0.2-1.201706071513.el6.no
arch
Marking CSCOcert-mgmnt-1.0.2-1.rpm as an update to CSCOcert-mgmnt-1.0.1-1.201705
251346.el6.noarch
Loading mirror speeds from cached hostfile
lwr-dbds-nexus1-yum                                       | 1.5 kB     00:00
Resolving Dependencies
--> Running transaction check
---> Package CSCOcert-mgmnt.noarch 0:1.0.1-1.201705251346.el6 will be updated
---> Package CSCOcert-mgmnt.noarch 0:1.0.2-1.201706071513.el6 will be an update
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package        Arch   Version                   Repository               Size
================================================================================
Updating:
 CSCOcert-mgmnt noarch 1.0.2-1.201706071513.el6   /CSCOcert-mgmnt-1.0.2-1 117 k

Transaction Summary
================================================================================
Upgrade       1 Package(s)

Total size: 117 k
Is this ok [y/N]:
```

7 When prompted to continue with the upgrade, enter **y** and press **Enter**. The CSCOcert-mgmnt package is updated.

```
Is this ok [y/N]: y
Downloading Packages:
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Updating   : CSCOcert-mgmnt-1.0.2-1.201706071513.el6.noarch              1/2
  Cleanup    : CSCOcert-mgmnt-1.0.1-1.201705251346.el6.noarch              2/2
  Verifying  : CSCOcert-mgmnt-1.0.2-1.201706071513.el6.noarch              1/2
  Verifying  : CSCOcert-mgmnt-1.0.1-1.201705251346.el6.noarch              2/2

Updated:
  CSCOcert-mgmnt.noarch 0:1.0.2-1.201706071513.el6

Complete!
```

8 Enter the following command to verify the current version of the **CSCOcert-mgmnt** package is upgraded.

```
[admin@adminnode ~]$ rpm -qa CSCOcert-mgmnt
```

Example Output:

```
[admin@adminnode ~]$  rpm -qa CSCOcert-mgmnt
CSCOcert-mgmnt-1.0.2-1.201706071513.el6.noarch
```

D

Update the NextX Application Repo

This appendix includes the procedure to update the NextX application repo to the most current software released for your solution.

Application packages can include all or any of the following tar files.

Software	Syntax for TAR Files
EC System Software	ec-system-release-[VERSION].tar
DTACS System Software	dtacs-system-release-[VERSION].tar
ECS System Release	ecs-[VERSION].tar
VCS Console	vcsconsole-[VERSION].tar
Alert Manager	am-x.tar
Billing Adaptor	billingAdaptor-[VERSION].tar
Billing Adaptor UI	BillingAdaptorUI-[VERSION.tar

In This Appendix

Updating the Application Packages Repo

Complete the following steps to update NextX packages in your software repo.

Note: In this example, we will update the EC application tar file from ec-system-release-8.0.15-4-201706061029.tar to ec-system-release-8.0.16-1-201706091356.tar.

1. Download the appropriate software for your site from your customer-specific forum on Cisco's File Exchange Server and save it to a local directory.
2. As **admin** user, enter the following command to clean up your existing repo.

   ```
   [admin@adminnode ~]$ sudo rm -f -r
   /opt/cisco/vcs/bootstrap/data/yum/repos/nextx*
   ```
3. Enter the following command to change to the **/opt/cisco/software/nextx-8.0** directory.

   ```
   [admin@adminnode ~]$ cd /opt/cisco/software/nextx-8.0
   ```
4. Remove the tar files for the packages you plan to upgrade.

   Example: if upgrading the EC application

   ```
   [admin@adminnode nextx-8.0]$ sudo rm
   ec-system-release-8.0.15-4-201706061029.tar
   ```
5. You are prompted to confirm the deletion.
6. Type **y** and press **Enter**.
7. Copy the appropriate tar packages from your local directory to the **/opt/cisco/software/nextx-8.0** directory.

   Note: For this example, we will copy ec-system-release-8.0.16-1-201706091356.tar to this directory.
8. Enter the following command to deploy the application packages.

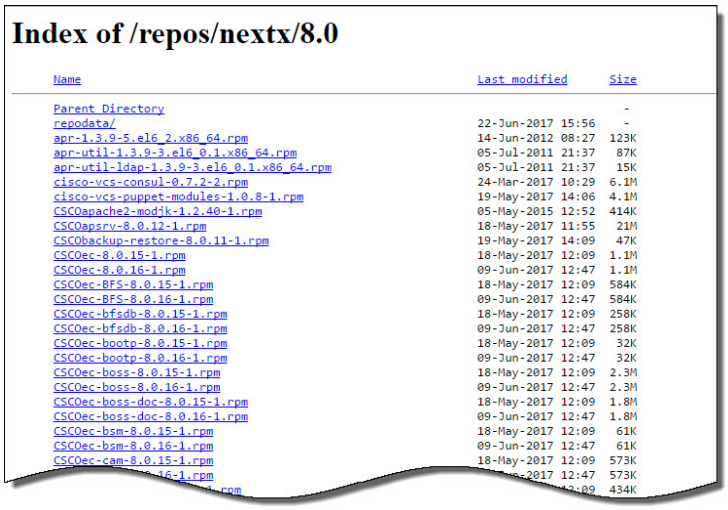
   ```
   [admin@adminnode nextx-8.0]$ sudo
   /opt/cisco/vcs/bootstrap/bin/vcs-admin deploy-bundle
   /opt/cisco/software/nextx-8.0/*.tar
   ```
9. Using the Admin Node IP address, browse to the **nextx/8.0** repo via a Web browser and verify that the appropriate RPMs are present.

   Command Syntax:

   ```
   http://[admin node IP]/repos/nextx/8.0/
   ```

Example:

`http://10.90.47.3/repos/nextx/8.0/`



Index of /repos/nextx/8.0

Name	Last modified	Size
Parent Directory		-
repodata/	22-Jun-2017 15:56	-
apr-1.3.9-5.el6_2.x86_64.rpm	14-Jun-2012 08:27	123K
apr-util-1.3.9-3.el6_0.1.x86_64.rpm	05-Jul-2011 21:37	87K
apr-util-ldap-1.3.9-3.el6_0.1.x86_64.rpm	05-Jul-2011 21:37	15K
cisco-vcs-consul-0.7.2-2.rpm	24-Mar-2017 10:29	6.1M
cisco-vcs-puppet-modules-1.0.8-1.rpm	19-May-2017 14:06	4.1M
CSCOapache2-modjk-1.2.40-1.rpm	05-May-2015 12:52	414K
CSCOapsrv-8.0.12-1.rpm	18-May-2017 11:55	21M
CSCObackup-restore-8.0.11-1.rpm	19-May-2017 14:09	47K
CSCOec-8.0.15-1.rpm	18-May-2017 12:09	1.1M
CSCOec-8.0.16-1.rpm	09-Jun-2017 12:47	1.1M
CSCOec-BFS-8.0.15-1.rpm	18-May-2017 12:09	584K
CSCOec-BFS-8.0.16-1.rpm	09-Jun-2017 12:47	584K
CSCOec-bfsdb-8.0.15-1.rpm	18-May-2017 12:09	258K
CSCOec-bfsdb-8.0.16-1.rpm	09-Jun-2017 12:47	258K
CSCOec-bootp-8.0.15-1.rpm	18-May-2017 12:09	32K
CSCOec-bootp-8.0.16-1.rpm	09-Jun-2017 12:47	32K
CSCOec-boss-8.0.15-1.rpm	18-May-2017 12:09	2.3M
CSCOec-boss-8.0.16-1.rpm	09-Jun-2017 12:47	2.3M
CSCOec-boss-doc-8.0.15-1.rpm	18-May-2017 12:09	1.8M
CSCOec-boss-doc-8.0.16-1.rpm	09-Jun-2017 12:47	1.8M
CSCOec-bsm-8.0.15-1.rpm	18-May-2017 12:09	61K
CSCOec-bsm-8.0.16-1.rpm	09-Jun-2017 12:47	61K
CSCOec-cam-8.0.15-1.rpm	18-May-2017 12:09	573K
[illegible]16-1.rpm	[illegible]2017 12:47	573K
[illegible].rpm	[illegible]:09	434K

10 Refer to one of the following documents to upgrade your software application.

- ***EC 8.0 Upgrade and Migration Guide***
- ***DTACS 5.0 Upgrade and Migration Guide***
- ***Explorer Controller Suite 3.0 Installation and Upgrade Guide***

Index

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

Septemtber 2017

Part Number
TP_00145