



Getting Started Guide for the Videoscape Control Suite

Please Read

Important

Please 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

© 2013 Cisco and/or its affiliates. All rights reserved.

Information in this publication is subject to change without notice. No part of this publication may be reproduced or transmitted in any form, by photocopy, microfilm, xerography, or any other means, or incorporated into any information retrieval system, electronic or mechanical, for any purpose, without the express permission of Cisco Systems, Inc.

Contents

About This Guide	v
Introduction to the Videoscape Control Suite	1
Acronyms Pertinent to the Videoscape Control Suite	2
Cisco UCS Documentation	3
UCS Hardware Requirements.....	4
Obtain This Information	6
Installation Checklist	7
Create the platformConfig.xml File	11
Preparations for Creating the platformConfig.xml File	12
Creating the platformConfig.xml File	14
Create the Virtual Floppy Disk	21
Before You Begin.....	22
Inject Files into the Current Image	23
Install the Videoscape Control Suite Software	27
Open vSphere	28
Download the OVA File.....	29
Deploy the OVA File	31
Mount the ISO and Begin the Videoscape Control Suite Installation	37
Manual Product Deployment Selection.....	43
Videoscape Control Suite Easy Install	57
What's Next?	70
Configure High Availability	71
Configuring High Availability.....	72
Deleting High Availability	75
Upgrading the Videoscape Control Suite	77
Videoscape Control Suite 2.1 to 2.5 Upgrade.....	78
Upgrade the Videoscape Control Suite Software.....	84
Troubleshooting the Videoscape Control Suite	87

Contents

Recover From a Failed Installation of the ISO Image	88
Troubleshooting the Upgrade	90
Installation Log File	93
Miscellaneous Troubleshooting Tips	94
Customer Information	97
Appendix A The cluster.xml Files	99
Overview of the Initial Deployment Configuration	100
Format of the Initial Deployment Configuration File.....	101
Cluster Concepts	102
Cluster File Examples.....	124
Appendix B How to Write an IDC File	155
Prepare the Datasource and the Database Nodes	156
Determine the Zone Configuration.....	158

About This Guide

Purpose

This guide specifies the hardware and software requirements, and the procedures, for installing the Cisco Videoscape Control Suite.

Audience

The audience for this document includes system administrators, operators, and installation engineers who deploy the Videoscape Control Suite.

Document Version

This is the third release of this document. This document has been updated for version 2.5 of the Videoscape Control Suite.

1

Introduction to the Videoscape Control Suite

Introduction

This chapter includes items of interest to installation engineers before they get started installing the Videoscape Control Suite.

In This Chapter

■ Acronyms Pertinent to the Videoscape Control Suite	2
■ Cisco UCS Documentation	3
■ UCS Hardware Requirements	4
■ Obtain This Information	6
■ Installation Checklist.....	7

Acronyms Pertinent to the Videoscape Control Suite

Installation and support engineers will encounter the following acronyms as they read through material necessary for installing and configuring the Videoscape Control Suite.

- Conductor Management Console (CMC)
- Domain Name System (DNS)
- Extensible Communication Platform (XCP)
- Extensible Markup Language (xml)
- Extensible Messaging and Presence Protocol (XMPP)
- International Organization for Standardization (ISO)
- Network Time Protocol (NTP)
- Simple Mail Transfer Protocol (SMTP)
- Unified Computing System (UCS)
- Virtual Storage Operating System (VSOS)
- VMware vSphere Hypervisor (ESXi)

Cisco UCS Documentation

This section lists documentation that pertains to the Cisco Unified Computing System (UCS).

Documentation Roadmaps

- For a complete list of all B-series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL:
<http://www.cisco.com/go/unifiedcomputing/b-series-doc>
- For a complete list of all C-series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL:
<http://www.cisco.com/go/unifiedcomputing/c-series-doc>

Other Documentation Resources

An ISO file containing all B- and C-series documents is available at the following URL:

<http://www.cisco.com/cisco/software/type.html?mdfid=283853163&flowid=25821>

Notes:

- From the link, click **Unified Computing System (UCS) Documentation Roadmap Bundle**. The ISO file is updated after every major documentation release.
- Follow Cisco UCS Docs on Twitter to receive document update notifications.

VMware Installation Documentation

- *Cisco UCS C-Series VMware Installation Guide* (P/N OL-22182-02)
- *Cisco UCS B-Series Blade Series VMware Installation Guide* (part number OL-22763)
- *Cisco UCS C-Series VMware Installation Guide* (P/N OL-21170-02)
- *Cisco UCS B-Series Blade Server Windows Installation Guide* (P/N OL-22764-02)

UCS Hardware Requirements

The Cisco Videoscape Control Suite platform and applications are designed to run on Cisco's Unified Computing System (UCS) B-Series and C-Series M2 and M3 hardware platforms. The following lists show the minimum hardware requirements and the minimal Virtual Machine (VM) configuration necessary for a Videoscape Control Suite installation.

This installation only supports the management node and the database/service node. If you are required to install other features, services, and/or applications, you will need additional nodes. The installation of the Endpoint Manager service requires a minimum of three nodes to support the NOSQLCB database.

UCS B200 Series

Minimum UCS B200 Blade Server Requirements

- Eight (8) B200 blade servers per chassis. Each blade has the following configuration:
 - $12 \times 8 \text{ GB} = 96 \text{ GB RAM}$
 - 2 x X5680 processor (or faster)
 - 2 x 500 GB HD
 - M81KR (Palo Adaptor)

System Requirement

- Dual Fabric Interconnects
- Each FEX has 4 uplinks to Fabric Interconnect (max)
- Single LAN and SAN uplink from each Fabric Interconnect
- Using 8 Gbps Fiber Channel (capable of 4 Gbps)

UCS C200 Series

Minimum UCS C200 Blade Server Requirements

- $12 \times 8 \text{ GB} = 96 \text{ GB RAM}$
- 2 x X5680 processor (or faster)
- 1 or 2 x 500 GB HD (15K SAS HDD)

System Requirement

2 GB Ethernet ports

Management Node VM Requirement

The OVA configuration depends upon the installed hardware and the supported devices. Contact Cisco Services for details.

Minimum VM Installation Requirements

Service Node VM Requirement

- 16 GB RAM
- 55 GB HD

Management Node VM Requirement

- 24 GB RAM
- 160 GB HDD

Important Limitations

Note these important limitations:

- The sum of the disk capacity of all VMs cannot exceed the disk capacity of the UCS server.
- The sum of the memory capacity of all VMs cannot exceed the memory capacity of the UCS server.
- The sum of the CPU capacity of all VMs cannot exceed the CPU capacity of the UCS server.

Required Changes for the UCS C-Series Hardware

- 1 Enable all Intel VT and HT
 - a Enter the BIOS
 - b Enable HyperThreading
 - c Enable all cores (Number of Enabled Cores)
 - d Enable all VT-related features. (Intel Virtualization Tech and all sub-features)
- 2 Enable NUMA
 - a Advanced --> Memory Configuration --> Memory RAS and Perf
 - b Enable NUMA
- 3 Configure the disk
 - a No Soft-Raid

Note: If two SATA disks exist, install them on the second disk.

Obtain This Information

Before installing or upgrading the Videoscape Control Suite software, obtain the following information.

- IP addresses, at least one per node: _____

- Domain name: _____
- Service JSM domain name: _____
- Client JSM domain name: _____
- Hostnames, one per node: _____

- Oracle server IP address: _____
- Oracle server service name: _____
- Oracle Msginfra user name: _____
- Oracle Msginfra user password: _____
- Oracle platform user name: _____
- Oracle platform user password: _____

- Cluster ID: _____
- Cluster secret: _____
- CLI user: _____
- CLI user password: _____
- Managed domain: _____
- Service domain name: _____
- Client JSM name: _____

Installation Checklist

Check Off	Action	Reference
	Rack the servers	<i>Cisco UCS Site Preparation Guide</i> (part number OL-19724-02)
	Cable the servers	<i>Cisco UCS Site Preparation Guide</i> (part number OL-19724-02)
	Install the UCS Servers	Refer to the Documentation Roadmaps section in <i>Cisco UCS Documentation</i> (on page 3) regarding the server you are installing.
	Install the Oracle Database (if needed)	<p>Before beginning the Videoscape Control Suite installation, the database administrator should prepare two Oracle accounts.</p> <ul style="list-style-type: none"> ■ The Videoscape Control Suite installation recommends a dedicated database instance (SID). However, it is the customer's choice to use a dedicated database instance or to share the database instance with other applications. ■ The Videoscape Control Suite installation recommends that you allocate dedicated tablespaces and data files for the Videoscape Control Suite. ■ The Videoscape Control Suite installation must use a dedicated schema and users. A pair of users are required – one for MSGINFRA and one for PLATFORM. <ul style="list-style-type: none"> – The user name must be upper-case. – The password of the user must be set to <i>never expire</i>.
	Install VMware ESXi	<p>This software is available for purchase from VMware. Refer to the VMware Installation Documentation section in <i>Cisco UCS Documentation</i> (on page 3) for instructions on installing ESXi.</p> <p>Note: For information on the types of Users required for the Videoscape Control Suite installation, see <i>Videoscape Control Suite Database User Guide</i> (OL-28290).</p>

Check Off	Action	Reference
	Install Windows server software (Optional. Needed only if a Windows server is not already available.)	This software is available for purchase from Microsoft. This software is used to install VMware vCenter and vSphere. Refer to the VMware Installation Documentation section in <i>Cisco UCS Documentation</i> (on page 3) for instructions on installing the Windows server software.
	Install VMware vCenter	Download this software from the VMware website. This software is licensed for 60-days without a special license. This software allows you to license the ESXi software beyond the standard 90-day period. Refer to the VMware Installation Documentation section in <i>Cisco UCS Documentation</i> (on page 3) for instructions on installing VMware vCenter. Note: There is no vCenter or vSphere requirement for non-production systems.
	Install VMware vSphere	Download the software from the URL of the ESXi instance. This software will be active for 90 days without licensing it with vCenter. Refer to the VMware Installation Documentation section in <i>Cisco UCS Documentation</i> (on page 3) for instructions on installing VMware vSphere.
	Create the cluster.xml file	<i>The cluster.xml Files</i> (on page 99) Note: This one master file represents the entire system.
	Create the platformConfig.xml file	<i>Create the platformConfig.xml File</i> (on page 11) Notes: <ul style="list-style-type: none"> ■ This is an optional file, but without this file platform questions, such as hostname, IP, netmask, DNS, etc., will have to be entered manually during the installation. ■ One platformConfig.xml file is required for each VM/node that is set up.
	Download the WinImage software	Available from this address: http://www.winimage.com/download.htm You need this software to create the virtual floppy disk used during installation of the Videoscape Control Suite.
	Create the virtual floppy disk file	<i>Create the Virtual Floppy Disk</i> (on page 21) Note: This unique *.flp file is required for each node, if you are including the platformConfig.xml file in the flp image.

Installation Checklist

Check Off	Action	Reference
	Download the Videoscape Control Suite Software	Download the Videoscape Control Suite software to an FTP server.
	Open the vSphere client and log on to the ESXi host IP or into vCenter	<i>Open vSphere</i> (on page 28)
	Download the OVA file for the Videoscape Control Suite	<i>Download the OVA File</i> (on page 29)
	Install the Videoscape Control Suite software	<p><i>Install the Videoscape Control Suite Software</i> (on page 27)</p> <p>Three installation methods are available:</p> <ul style="list-style-type: none"> ■ Automated installation using the cluster.xml and platformConfig.xml files. See <i>Install the Videoscape Control Suite Software</i> (on page 27). ■ Manual installation (no cluster.xml and platformConfig.xml files). See <i>Manual product Deployment Selection</i> (on page 43). ■ This is the preferred method. Install the platformConfig.xml file and then go to <i>Videoscape Control Suite Easy Install</i> (on page 57). <p>Important: The database (external Oracle) node must be installed before installing the service or management nodes.</p>
	Install Videoscape Control Suite Management Console	<i>Installing COP Files for the Videoscape Control Suite</i> (part number OL-27753)
	Install services, if needed	<i>Installing COP Files for the Videoscape Control Suite</i> (part number OL-27753)

2

Create the platformConfig.xml File

Introduction

In preparation for the installation of the Videoscape Control Suite software, you need to create a virtual floppy disk. This virtual floppy disk can be created using WinImage software, which can be obtained from the following URL: <http://www.winimage.com/download.htm>.

The contents of the virtual floppy disk are a cluster.xml file and a platformConfig.xml file.

If you are performing the "Easy Installation", skip to *Creating the platformConfig.xml File* (on page 14).

In This Chapter

- Preparations for Creating the platformConfig.xml File 12
- Creating the platformConfig.xml File 14

Preparations for Creating the platformConfig.xml File

Important Limitations

Note these important limitations:

- The sum of the disk capacity of all VMs cannot exceed the disk capacity of the UCS server.
- The sum of the memory capacity of all VMs cannot exceed the memory capacity of the UCS server.
- The sum of the CPU capacity of all VMs cannot exceed the CPU capacity of the UCS server.

The platformConfig.xml File

Important: You must create a unique platformConfig.xml file for each and every node that you deploy.

Note: The following link may be of assistance in helping create the platformConfig.xml file: <http://riker-2.cisco.com/afg/>

You need the following information to create the platformConfig.xml file:

- IP addresses, one for each node you are creating
Note: The Videoscape Control Suite now supports multiple interfaces.
- A hostname for each node you are creating
Note: There must be a matching forward and reverse DNS entry in the DNS server specified for this hostname.
- The subnet mask for this network
- The NTP server IP address
- The DNS server IP (primary) address
- The DNS server IP (secondary) address
- The network gateway
- The domain name
- The timezone
- The city for the node

Preparations for Creating the platformConfig.xml File

- Certificate signing request organization
- Certificate signing request unit
- Certificate signing request location
- Certificate signing request state
- Certificate signing request country
- The SMTP host

Creating the platformConfig.xml File

For the platformConfig.xml file, the entry **Product Deployment** (in the **ParamValue** section) describes what you are installing on the node. You have two options, “rtmbdb” and “rtmb”. All installations will be “rtmb”, in order to install a generic Videoscape Control Suite node.

Note: The option “rtmbdb” will only be used by internal Cisco personnel for lab deployments. This option may be removed in the future. It is used for creating the PostgreSQL database node.

Sample platformConfig2.5.xml File

```
<?xml version="1.0"?>
<PlatformData>
    <Version>2.5</Version>
    <ProductDeployment>
        <ParamNameText>Deployment</ParamNameText>
        <ParamDefaultValue>CallManager</ParamDefaultValue>
        <ParamValue>rtmb</ParamValue>
    </ProductDeployment>
    <PlatformConfigurationDone>
        <ParamNameText>Status of platform configuration</ParamNameText>
        <ParamDefaultValue>no</ParamDefaultValue>
        <ParamValue>no</ParamValue>
    </PlatformConfigurationDone>
    <PreLoadedSoftware>
        <ParamNameText>Create a pre loaded software node</ParamNameText>
        <ParamDefaultValue>no</ParamDefaultValue>
        <ParamValue>yes</ParamValue>
    </PreLoadedSoftware>
    <InstallType>
        <ParamNameText>Install or upgrade type</ParamNameText>
        <ParamDefaultValue>basic</ParamDefaultValue>
        <ParamValue>Basic Install</ParamValue>
    </InstallType>
    <ClusterID>
        <ParamNameText>Cluster ID</ParamNameText>
        <ParamDefaultValue>cluster1</ParamDefaultValue>
        <ParamValue>csoraclus2</ParamValue>
    </ClusterID>
```

Creating the platformConfig.xml File

```
<ClusterSecret>
    <ParamNameText>Cluster Secret</ParamNameText>
    <ParamDefaultValue>cluster_secret</ParamDefaultValue>
    <ParamValue>cisco123</ParamValue>
</ClusterSecret>
<LocalHostNICAuto>
    <ParamNameText>Auto Configure speed and duplex</ParamNameText>
    <ParamDefaultValue>yes</ParamDefaultValue>
    <ParamValue>no</ParamValue>
</LocalHostNICAuto>
<LocalHostNICSpeed>
    <ParamNameText>Auto Configure speed and duplex</ParamNameText>
    <ParamDefaultValue>100</ParamDefaultValue>
    <ParamValue>100</ParamValue>
</LocalHostNICSpeed>
<LocalHostNICDuplex>
    <ParamNameText>Auto Configure speed and duplex</ParamNameText>
    <ParamDefaultValue>Full</ParamDefaultValue>
    <ParamValue>full</ParamValue>
</LocalHostNICDuplex>
<ChangeMTUSize>
    <ParamNameText>MTU Size changed from OS default</ParamNameText>
    <ParamDefaultValue>no</ParamDefaultValue>
    <ParamValue>no</ParamValue>
</ChangeMTUSize>
<LocalHostName>
    <ParamNameText>Host Name for this machine</ParamNameText>
    <ParamDefaultValue>localhost</ParamDefaultValue>
    <ParamValue>csvml185216</ParamValue>
</LocalHostName>
<LocalHostDHCP>
    <ParamNameText>Is DHCP enabled for this machine</ParamNameText>
    <ParamDefaultValue>no</ParamDefaultValue>
    <ParamValue>no</ParamValue>
</LocalHostDHCP>
<LocalHostIP0>
    <ParamNameText>Host IP0 addr for this node</ParamNameText>
    <ParamDefaultValue>127.0.0.1</ParamDefaultValue>
    <ParamValue>10.90.185.216</ParamValue>
```

Chapter 2 Create the platformConfig.xml File

```
</LocalHostIP0>
<LocalHostMask0>
    <ParamNameText>Host IP0 mask for this node</ParamNameText>
    <ParamDefaultValue>255.255.255.0</ParamDefaultValue>
    <ParamValue>255.255.252.0</ParamValue>
</LocalHostMask0>
<LocalHostGW0>
    <ParamNameText>Gateway for this node</ParamNameText>
    <ParamDefaultValue>127.0.0.1</ParamDefaultValue>
    <ParamValue>10.90.184.201</ParamValue>
</LocalHostGW0>
<LocalHostDnsPrimary>
    <ParamNameText>Primary DNS server IP address</ParamNameText>
    <ParamDefaultValue>0.0.0.0</ParamDefaultValue>
    <ParamValue>64.102.6.247</ParamValue>
</LocalHostDnsPrimary>
<LocalHostDnsSecondary>
    <ParamNameText>Secondary DNS server IP address</ParamNameText>
    <ParamDefaultValue>0.0.0.0</ParamDefaultValue>
    <ParamValue>72.163.47.11</ParamValue>
</LocalHostDnsSecondary>
<LocalHostDomain>
    <ParamNameText>Domain name for this machine</ParamNameText>
    <ParamDefaultValue>cisco.com</ParamDefaultValue>
    <ParamValue>cisco.com</ParamValue>
</LocalHostDomain>
<LocalHostTimezone>
    <ParamNameText>Timezone for this node</ParamNameText>
    <ParamDefaultValue>America/Los_Angeles</ParamDefaultValue>
    <ParamValue>America/New_York</ParamValue>
</LocalHostTimezone>
<LocalHostContinent>
    <ParamNameText>Continent for this node</ParamNameText>
    <ParamDefaultValue>America</ParamDefaultValue>
    <ParamValue>America</ParamValue>
</LocalHostContinent>
<LocalHostCity>
    <ParamNameText>City for this node</ParamNameText>
    <ParamDefaultValue>Los_Angeles</ParamDefaultValue>
    <ParamValue>New_York</ParamValue>
```

Creating the platformConfig.xml File

```
</LocalHostCity>
<LocalHostAdminName>
    <ParamNameText>Administrator name for this node</ParamNameText>
    <ParamDefaultValue>administrator</ParamDefaultValue>
    <ParamValue>admin</ParamValue>
</LocalHostAdminName>
<LocalHostAdminPwCrypt>
    <ParamNameText>Admin PW for this node</ParamNameText>
    <ParamDefaultValue>password</ParamDefaultValue>

<ParamValue>97064DD561F94883831812812AB2825C831812812AB2825C831812812AB2825C
</ParamValue>
</LocalHostAdminPwCrypt>
<CertX509>
    <Org>
        <ParamNameText>Certification Signing Request
Organization</ParamNameText>
        <ParamDefaultValue>none</ParamDefaultValue>
        <ParamValue>Cisco</ParamValue>
    </Org>
    <Unit>
        <ParamNameText>Certification Signing Request Unit</ParamNameText>
        <ParamDefaultValue>none</ParamDefaultValue>
        <ParamValue>CS</ParamValue>
    </Unit>
    <Location>
        <ParamNameText>Certification Signing Request Location</ParamNameText>
        <ParamDefaultValue>none</ParamDefaultValue>
        <ParamValue>Lawrenceville</ParamValue>
    </Location>
    <State>
        <ParamNameText>Certification Signing Request State</ParamNameText>
        <ParamDefaultValue>none</ParamDefaultValue>
        <ParamValue>GA</ParamValue>
    </State>
    <Country>
        <ParamNameText>Certification Signing Request Country</ParamNameText>
        <ParamDefaultValue>none</ParamDefaultValue>
        <ParamValue>US</ParamValue>
    </Country>
```

Chapter 2 Create the platformConfig.xml File

```
</CertX509>

<LocaleId>
    <ParamNameText>Microsoft assigned locale identifier
    value</ParamNameText>
    <ParamDefaultValue>00000409</ParamDefaultValue>
    <ParamValue/>
</LocaleId>

<CCMVersion>
    <ParamNameText>CM version on the server backed up</ParamNameText>
    <ParamDefaultValue>CCM ver 5.0</ParamDefaultValue>
    <ParamValue/>
</CCMVersion>

<CcmFirstNode>
    <ParamNameText>First CCM node in the cluster</ParamNameText>
    <ParamDefaultValue>yes</ParamDefaultValue>
    <ParamValue>yes</ParamValue>
</CcmFirstNode>

<SftpPwCrypt>
    <ParamNameText>Security PW for this node</ParamNameText>
    <ParamDefaultValue>password</ParamDefaultValue>
    <ParamValue>694762330078F91752AE5D0C0B01ECDF831812812AB2825C831812812AB2825C
    </ParamValue>
</SftpPwCrypt>

<IPSecFirstNode>
    <ParamNameText>First IPSec node in the cluster</ParamNameText>
    <ParamDefaultValue>yes</ParamDefaultValue>
    <ParamValue>yes</ParamValue>
</IPSecFirstNode>

<IPSecEnabled>
    <ParamNameText>IPSec Configuration for this node</ParamNameText>
    <ParamDefaultValue>no</ParamDefaultValue>
    <ParamValue>no</ParamValue>
</IPSecEnabled>

<IPSecSecurityPwCrypt>
    <ParamNameText>Security PW for this node</ParamNameText>
    <ParamDefaultValue>password</ParamDefaultValue>
    <ParamValue>694762330078F91752AE5D0C0B01ECDF831812812AB2825C831812812AB2825C
    </ParamValue>
</IPSecSecurityPwCrypt>

<NtpServer>
```

Creating the platformConfig.xml File

```
<ParamNameText>Address Range for NTP server</ParamNameText>
<ParamDefaultValue>none</ParamDefaultValue>
<ParamValue>10.90.184.1</ParamValue>
</NtpServer>
<ApplUserUsername>
    <ParamNameText>Application User Username</ParamNameText>
    <ParamDefaultValue>CCMAdministrator</ParamDefaultValue>
    <ParamValue>Default</ParamValue>
</ApplUserUsername>
<ApplUserPwCrypt>
    <ParamNameText>Application User Password</ParamNameText>
    <ParamDefaultValue>password</ParamDefaultValue>
    <ParamValue>694762330078F91752AE5D0C0B01ECDF831812812AB2825C831812812AB2825C
    </ParamValue>
</ApplUserPwCrypt>
<Eth2IPv4Enabled>
    <ParamNameText>Eth2 IPv4 Configuration for this node</ParamNameText>
    <ParamDefaultValue>no</ParamDefaultValue>
    <ParamValue>no</ParamValue>
</Eth2IPv4Enabled>
<Eth2IPv6Enabled>
    <ParamNameText>Eth2 IPv6 Configuration for this node</ParamNameText>
    <ParamDefaultValue>no</ParamDefaultValue>
    <ParamValue>no</ParamValue>
</Eth2IPv6Enabled>
<Eth5IPv4Enabled>
    <ParamNameText>Eth5 IPv4 Configuration for this node</ParamNameText>
    <ParamDefaultValue>no</ParamDefaultValue>
    <ParamValue>no</ParamValue>
</Eth5IPv4Enabled>
<Eth5IPv6Enabled>
    <ParamNameText>Eth5 IPv6 Configuration for this node</ParamNameText>
    <ParamDefaultValue>no</ParamDefaultValue>
    <ParamValue>no</ParamValue>
</Eth5IPv6Enabled>
</PlatformData>
```


3

Create the Virtual Floppy Disk

Introduction

This chapter contains instructions that guide you through the process of creating the virtual floppy disk.

In This Chapter

- Before You Begin..... 22
- Inject Files into the Current Image 23

Before You Begin

- 1 Download and install the free Windows utility, **WinImage**, from the Internet.
- 2 Reference the following topics for information on how the cluster.xml and platformConfig.xml files are constructed:
 - *The cluster.xml Files* (on page 99)
Note: This is optional.
 - *Create the platformConfig.xml File* (on page 11)

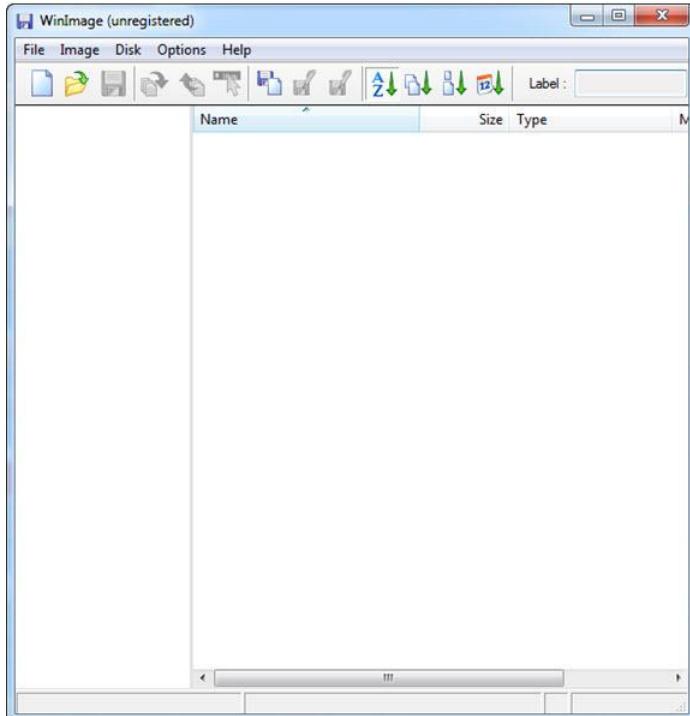
Notes:

- The platformConfig.xml file automates much of the platform configuration during the installation process.
 - The WinImage utility makes use of these file(s) to create a virtual floppy image file (*.flp) for use during the Videoscape Control Suite installation.
- 3 Load a copy of an existing cluster.xml file (if you are using one) and the platformConfig.xml file onto your computer.

Inject Files into the Current Image

The examples used in this procedure assume that a platformConfig.xml file is used to help automate the installation.

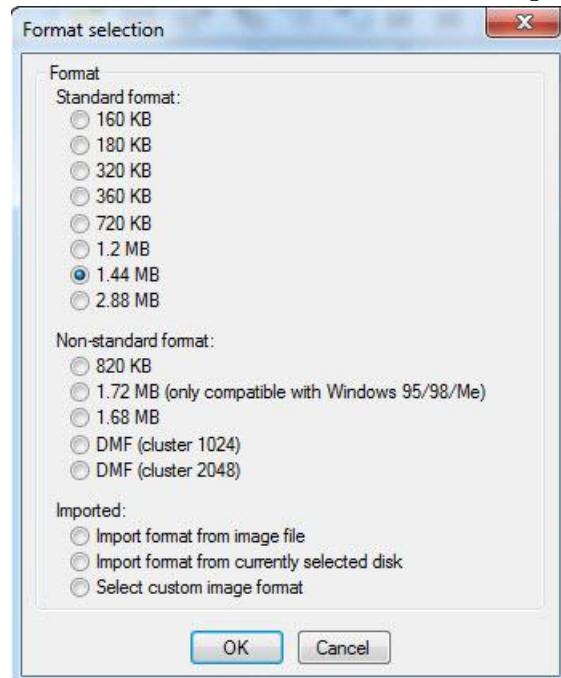
- 1 Launch the WinImage utility.



Chapter 3 Create the Virtual Floppy Disk

- 2 From the WinImage utility, click **File** and select **New**.

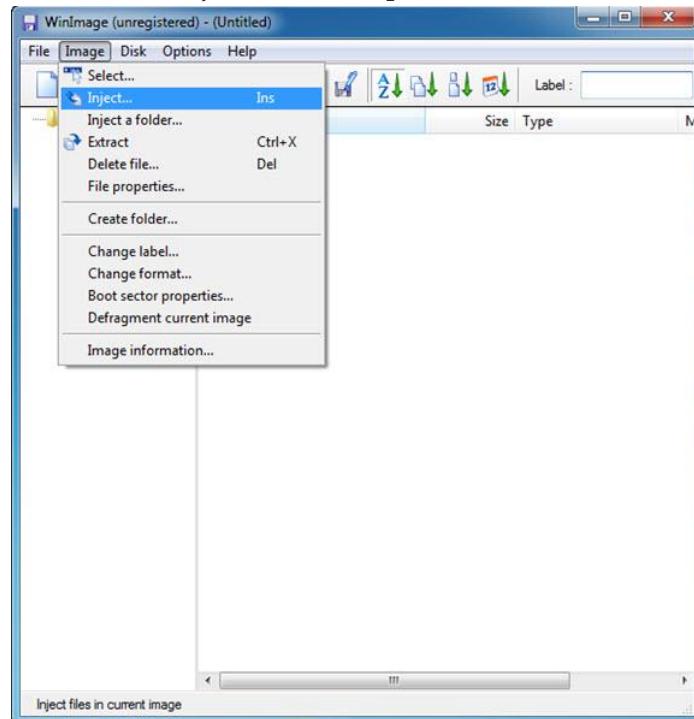
Result: The Format selection window opens.



- 3 Under **Standard format**, be certain that **1.44 MB** is selected. Then, click **OK**.

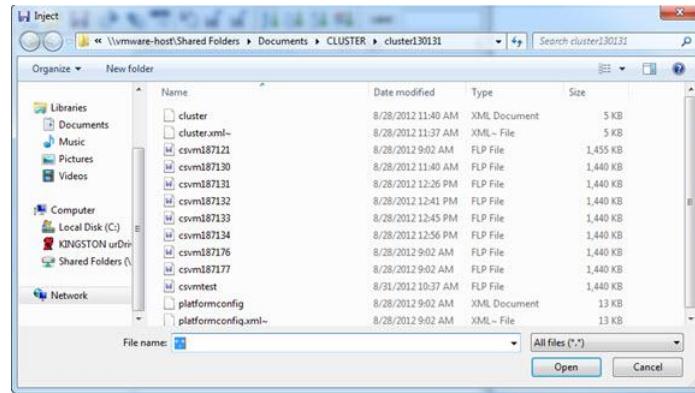
- 4 From the WinImage utility, click **Image** and select **Inject**.

Result: The Inject window opens.



Inject Files into the Current Image

- 5 Navigate to the directory where your cluster.xml and platformConfig.xml (if used) files are stored.

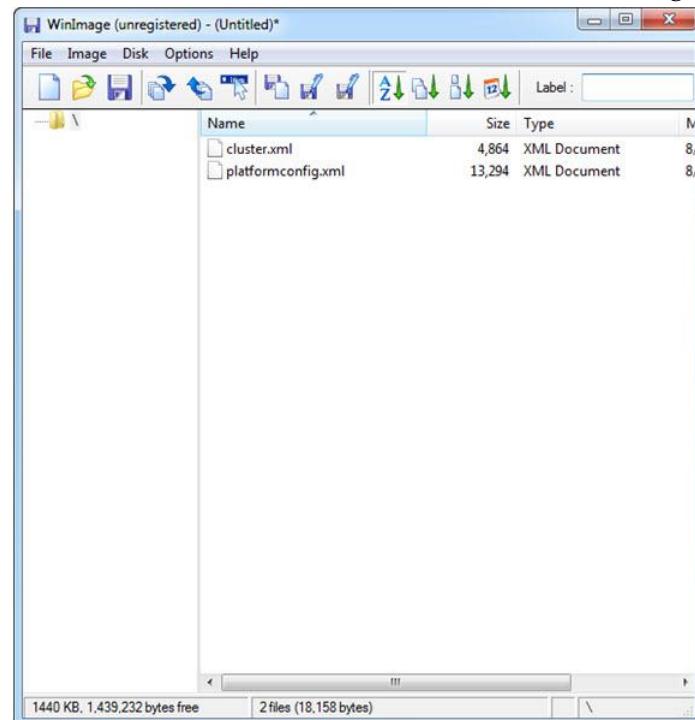


- 6 Highlight the file(s) that you want to inject (select the **cluster.xml** and the **platformConfig.xml** files) and then click **Open**.

Result: A message appears seeking confirmation of your intent to inject file(s).

- 7 Click **Yes**.

Result: You should now have two files in WinImage.

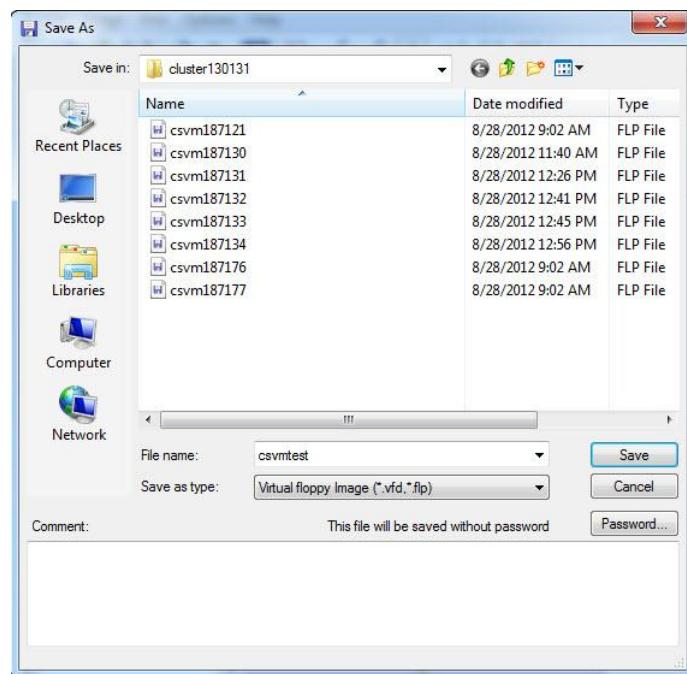


Chapter 3 Create the Virtual Floppy Disk

- 8 Save the file as a virtual floppy file.

Note: The initial, default save will be an .imz file.

- a Change the **Save as type** field to **Virtual floppy Image (*.vfd, *.flp)**.
- b Type in a **File name** (such as, **csvmtest**).
- c Click **Save**.



4

Install the Videoscape Control Suite Software

Introduction

The contents of this chapter guide you through the steps of installing the Videoscape Control Suite.

In This Chapter

■ Open vSphere	28
■ Download the OVA File	29
■ Deploy the OVA File	31
■ Mount the ISO and Begin the Videoscape Control Suite Installation	37
■ Manual Product Deployment Selection.....	43
■ Videoscape Control Suite Easy Install	57
■ What's Next?.....	70

Open vSphere

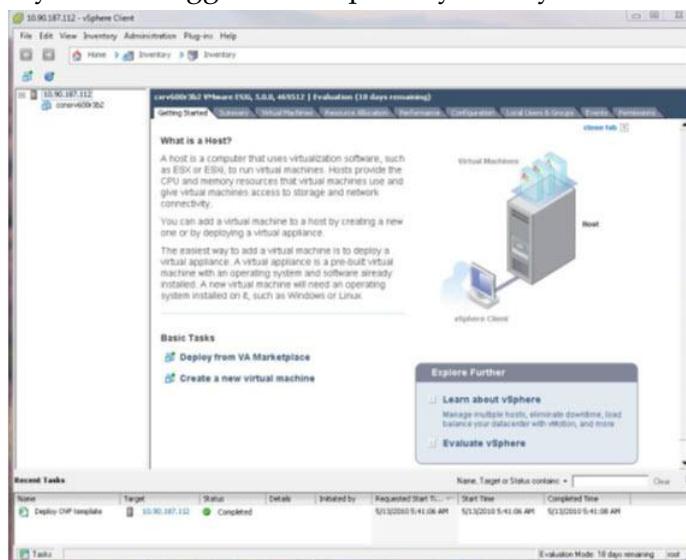
- Double-click on the VMware vSphere icon on your desktop to log into the ESXi host or vCenter server to start the Videoscape Control Suite software installation.

Notes:

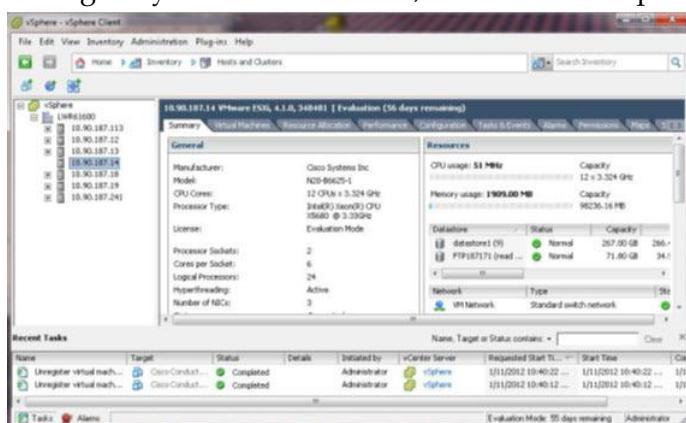
- If ESXi host, enter the ESXi host **IP address**, **User name**, and **Password**.
- If vCenter server, enter the Vcenter server **IP address**, **User name**, and **Password**.

Results:

- If you have logged into vSphere, you only have access to the ESXi host.



- If you have logged into vCenter, you see a list of ESXi hosts that are being managed by the vCenter server, in the left-hand pane.

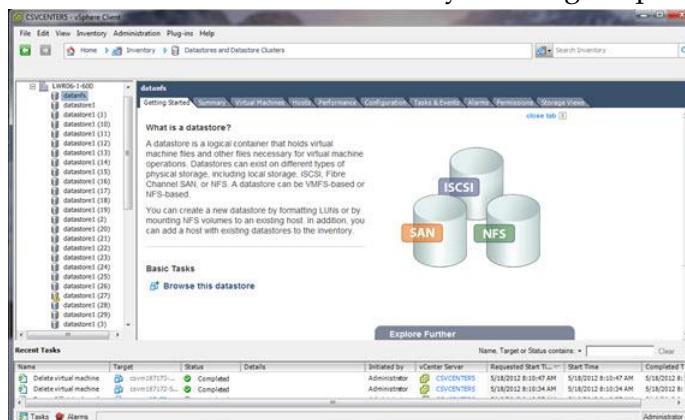


Download the OVA File

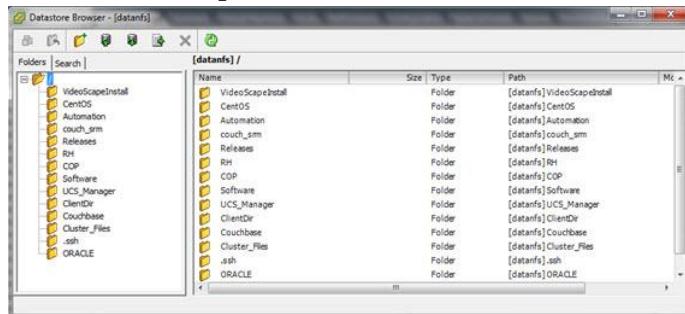
Important: You will only need to perform this procedure if this is not the server you are using for the Image Repository.

1 Select one of the following options:

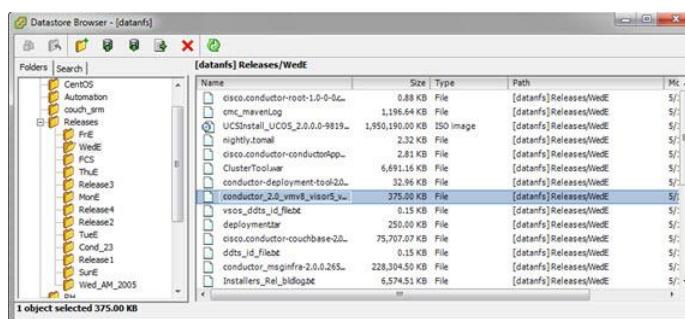
- If you are logging into vSphere, download the OVA file to your desktop.
- If you are logging into vCenter, follow these steps to download the OVA file from the Image Repository.
 - a Select **Inventory**, then, **Datastores and Datastore Cluster**.
 - b Select the Datastore that contains your Image Repository.



- c Select **Browse this Datastore**, then navigate to the OVA file you will use for the Videoscape Control Suite software installation.



- d Select the file to download.



Chapter 4 Install the Videoscape Control Suite Software

- e Right-click on the OVA file and select **Download**.

Result: A window opens that allows you to select the location to which you would like to save the OVA file on your local disk.

- f Navigate to the location and select **OK**.

Result: The following message appears: **If a file or folder in this target location has the same name as the one being copied, it will be replaced. Do you still want to continue?**

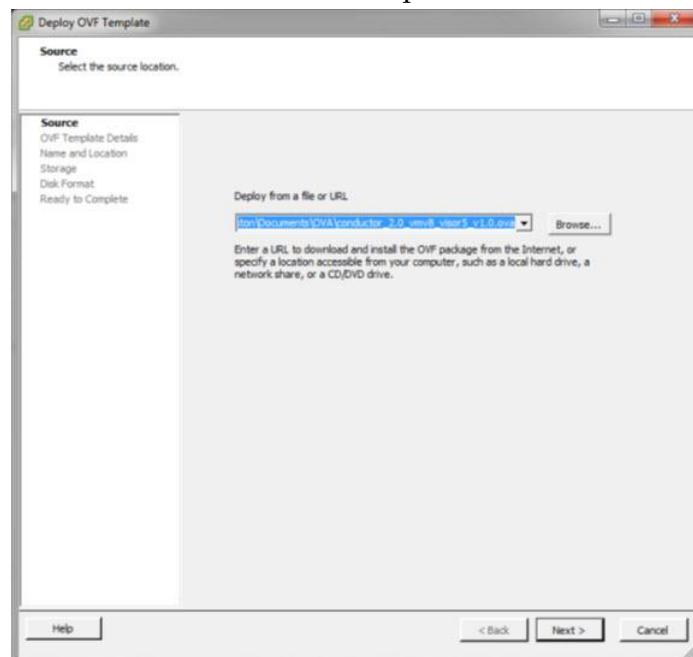
- g Click **Yes**.

Deploy the OVA File

- 1 From vCenter5, click **Home** and then select **Inventory**.
- 2 Click **Hosts and Clusters**.
- 3 Select the ESXi host on which you would like to deploy the OVA template.
- 4 From the vSphere client window, click **File** and then select **Deploy OVF Template**.

Note: The OVA template contains a package of OVF files that specify the configuration of the virtual machine for the Videoscape Control Suite software installation.

Result: The Source window opens.



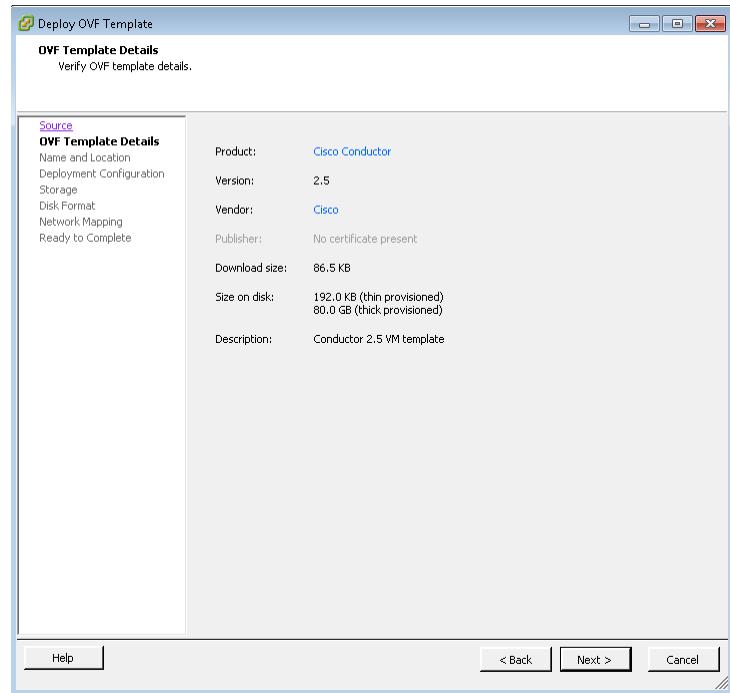
- 5 Click **Browse** on the Source window and navigate to the location of the OVA file.

Chapter 4 Install the Videoscape Control Suite Software

- 6 Highlight the OVA file and click **Open**. Then, click **Next**.

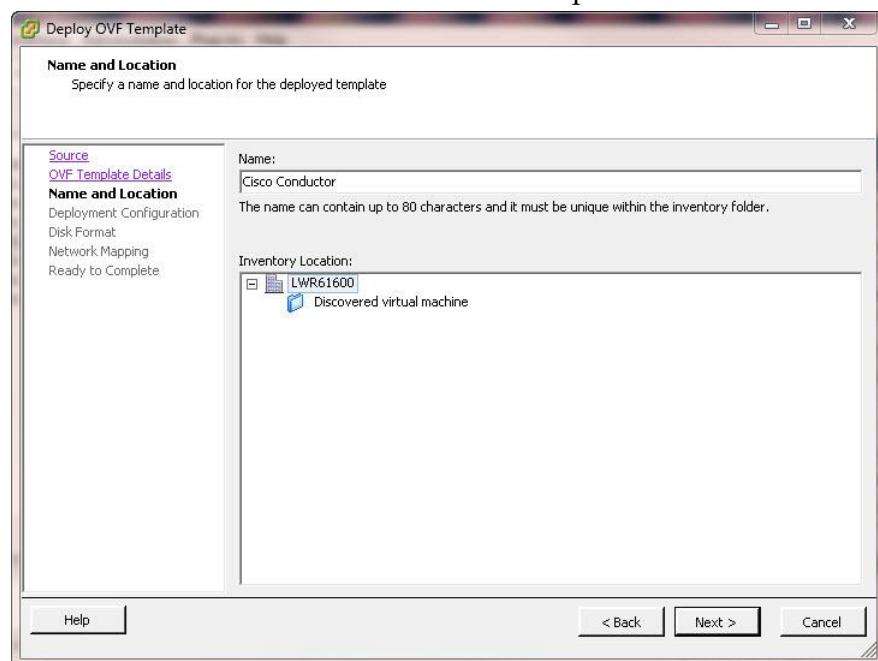
Note: The official Cisco Videoscape Control Suite release comes with three ova files, one for hypervisor 4, one for hypervisor 5, and the third specifically for hypervisor 5 UCS M3 hardware platforms. Currently, only hypervisor 5 is supported.

Result: The OVF Template Details window opens.



- 7 Verify the information on the OVF Template Details window and click **Next**.

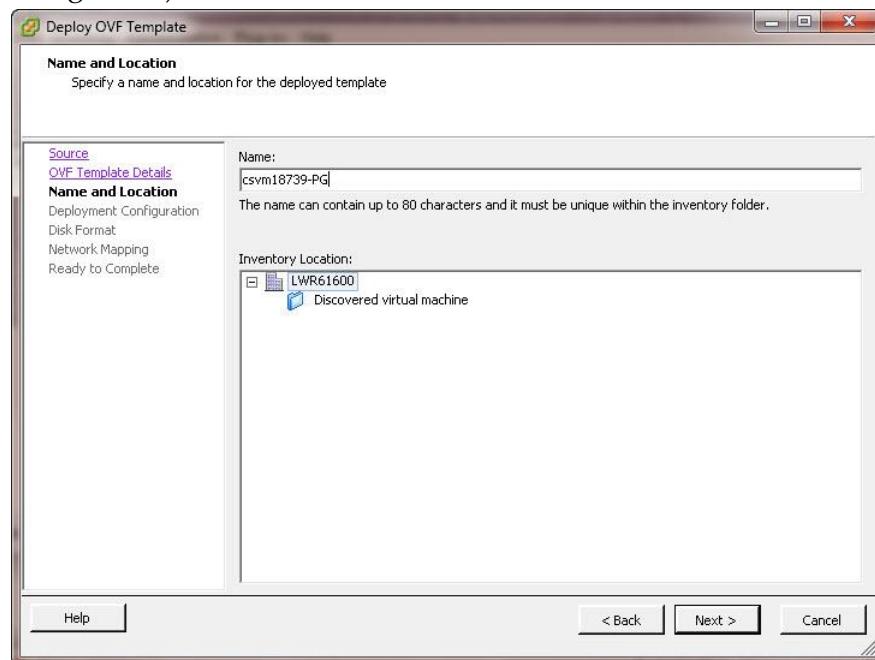
Result: The Name and Location window opens.



Deploy the OVA File

- 8 Click the **Name** field and type a name for your VM.

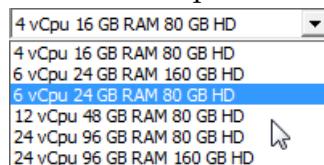
Note: In this example, the name of the VM is **csvm18739--PG** ("PG" for PostgreSQL).



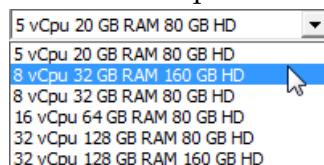
- 9 Click **Next** to begin selecting the number of nodes you are going to install.

Result: The Deployment Configuration window opens.

- M2 hardware platform



- M3 hardware platform



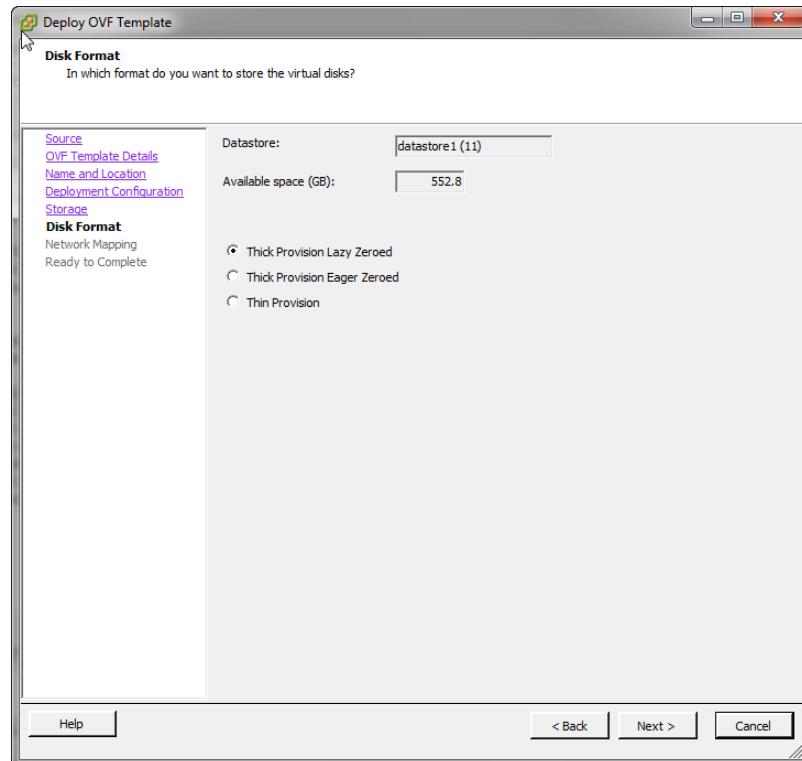
- 10 Click into the **Configuration** field and select the desired deployment configuration concerning the number of virtual machines per blade from the drop-down menu.

Note: Contact Cisco Services for details on the needed OVA configuration to support your devices.

11 Click Next.

Result: The Disk Format window opens.

12 Press **Enter** to select the default format for which you want to store the virtual disks.



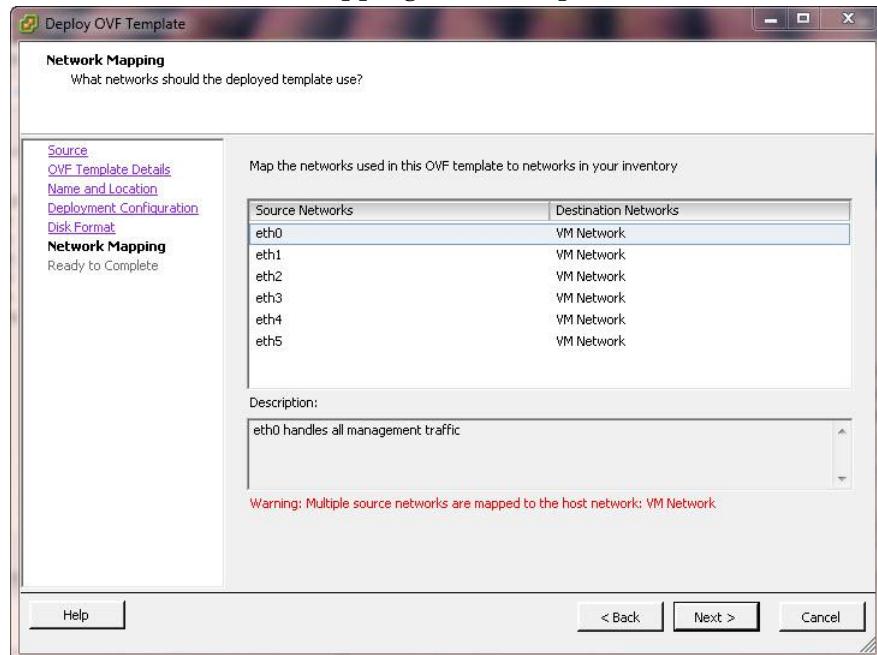
Notes:

- **Thick Provision Lazy Zeroed** format creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out on demand, at a later time, upon first write from the virtual machine.
Using the default flat virtual disk format does not zero out or eliminate the possibility of recovering deleted files or restoring old data that might be present on this allocated space. You cannot convert a flat disk to a thin disk.
- **Thick Provision Eager Zeroed** format is a type of thick virtual disk that supports clustering features, such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create other types of disks.

- **Thin Provision** format is used to save storage space. For the thin disk, you provision as much datastore space as the disk would require based on the value that you enter for the disk size. However, the thin disk starts small and, at first, uses only as much datastore space as the disk needs for its initial operations.
- Notes:**
 - If a virtual disk supports clustering solutions, such as Fault Tolerance, do not make the disk thin.
 - If the thin disk needs more space later, it can grow to its maximum capacity and occupy the entire datastore space provisioned to it. Also, you can manually convert the thin disk into a thick disk.
- For this example, the **Thick Provisioned Lazy Zeroed** disk format is selected.

13 Click Next.

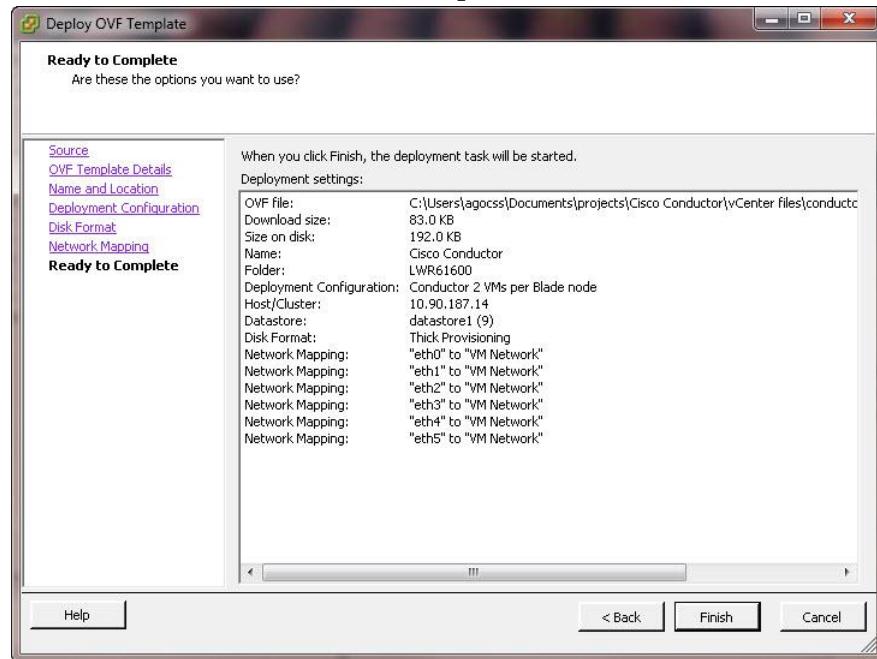
Result: The Network Mapping window opens.



Chapter 4 Install the Videoscape Control Suite Software

- 14 Click Next to accept the default source network.

Result: A confirmation window opens.

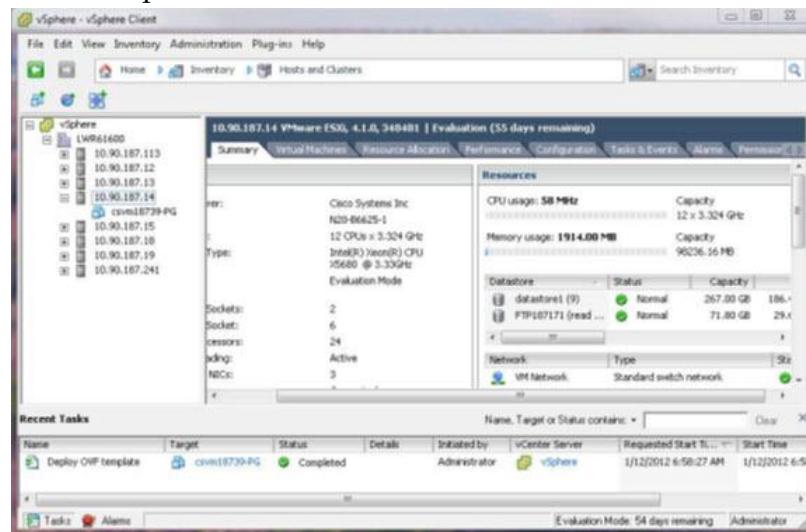


- 15 Click Finish to create the virtual machine.

Result: A Completed Successfully message appears.

- 16 Click Close to close the message.

- 17 Click the + symbol to the left of the highlighted IP address on which you have been working to expand the selection. Confirm that the virtual machine you have created is present.



- 18 Repeat this procedure to create as many VMs as needed.

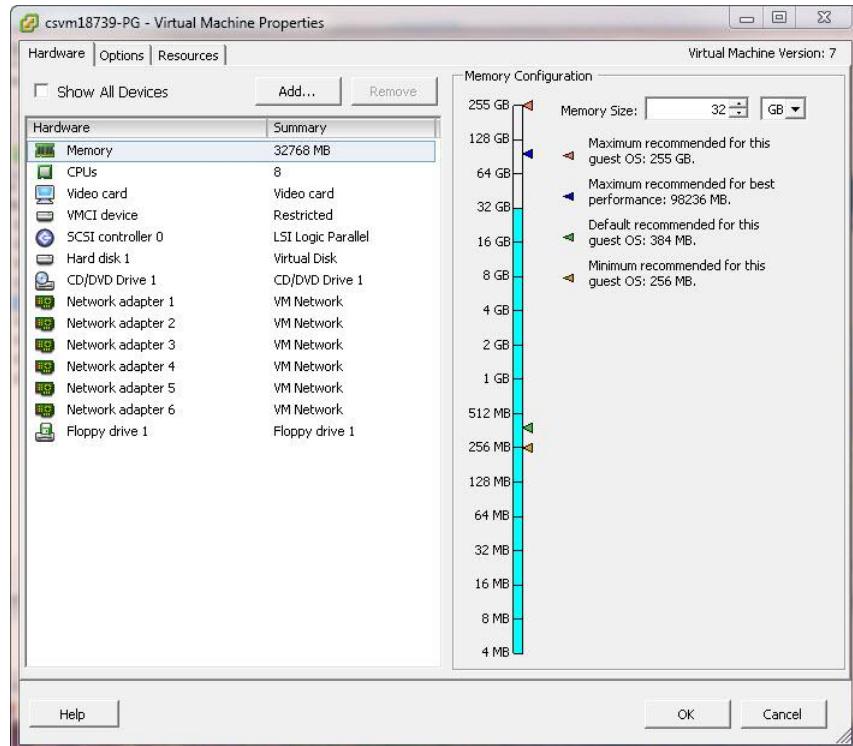
Mount the ISO and Begin the Videoscape Control Suite Installation

Note: If you are performing the Easy Installation for a lab, a demonstration, or for developer use and are using the single Msginfra node, install only the Management and one Service node. Then, deploy the Msginfra. Install the other service nodes if you need them.

Before you begin, be sure the ISO image for the Virtual Storage Operating System (VSOS) has been loaded onto the client machine, hard drive, or datastore. Then, follow these instructions to connect to the ISO image.

- 1 Right-click the virtual machine in the left pane, and select **Edit Settings**.

Result: The Virtual Machine Properties window opens.

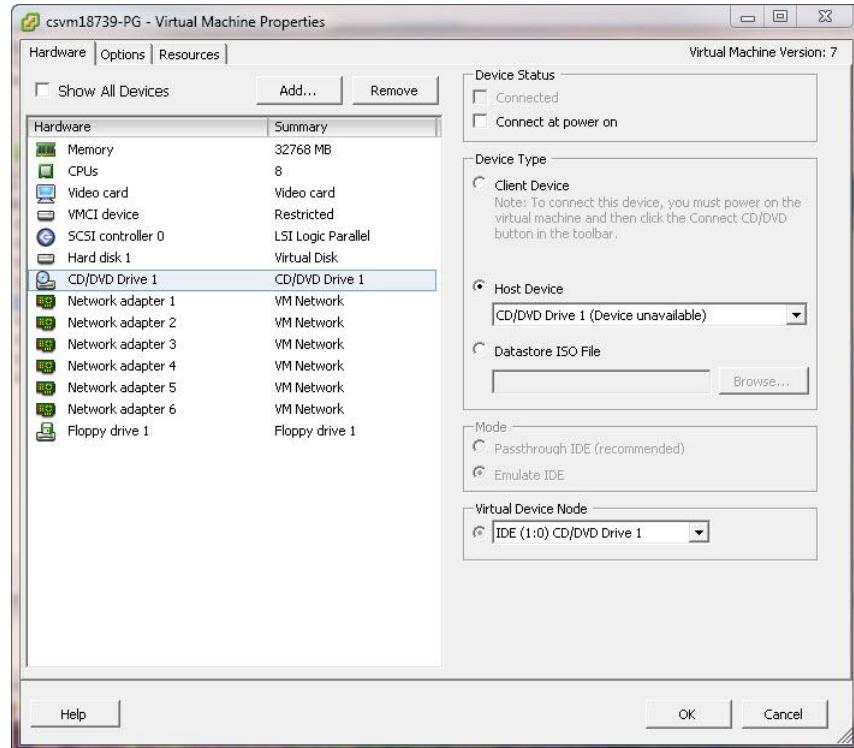


Chapter 4 Install the Videoscape Control Suite Software

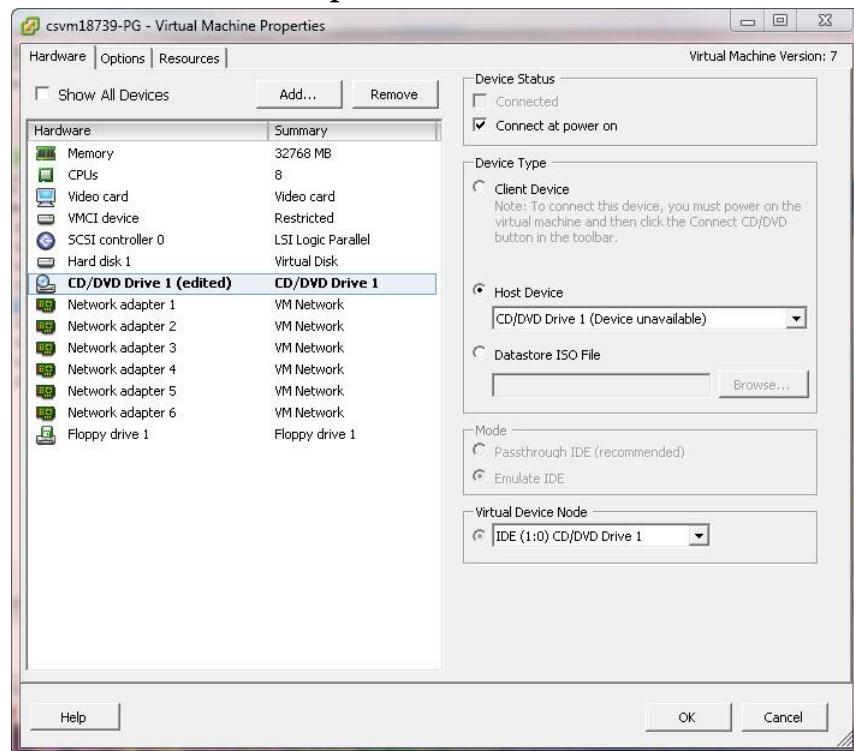
- 2 Click to highlight CD/DVD Drive 1.

Result: The window updates to show various device statuses and device types.

Note: If you are installing the ISO image from the datastore, click to highlight **Datastore ISO File**, then browse to select the file.



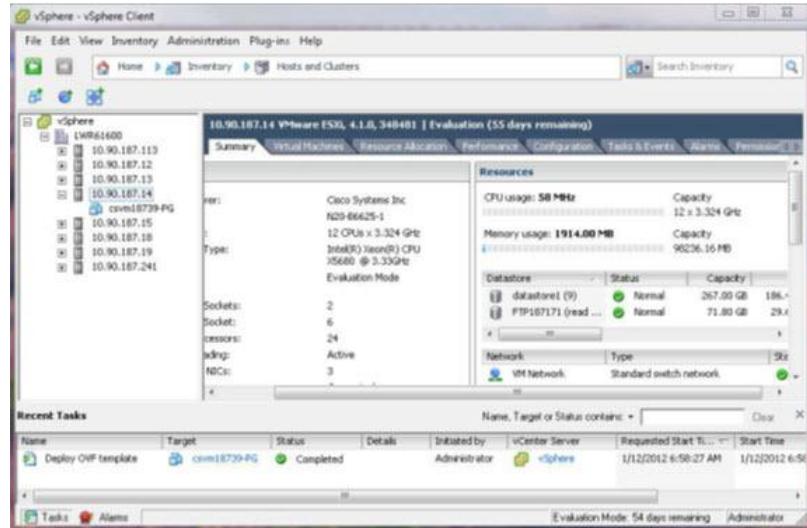
- 3 Click so that **Connect at power on** is checked.



Mount the ISO and Begin the Videoscape Control Suite Installation

- 4 Click OK.

Result: The window reverts to the vSphere Client user interface.



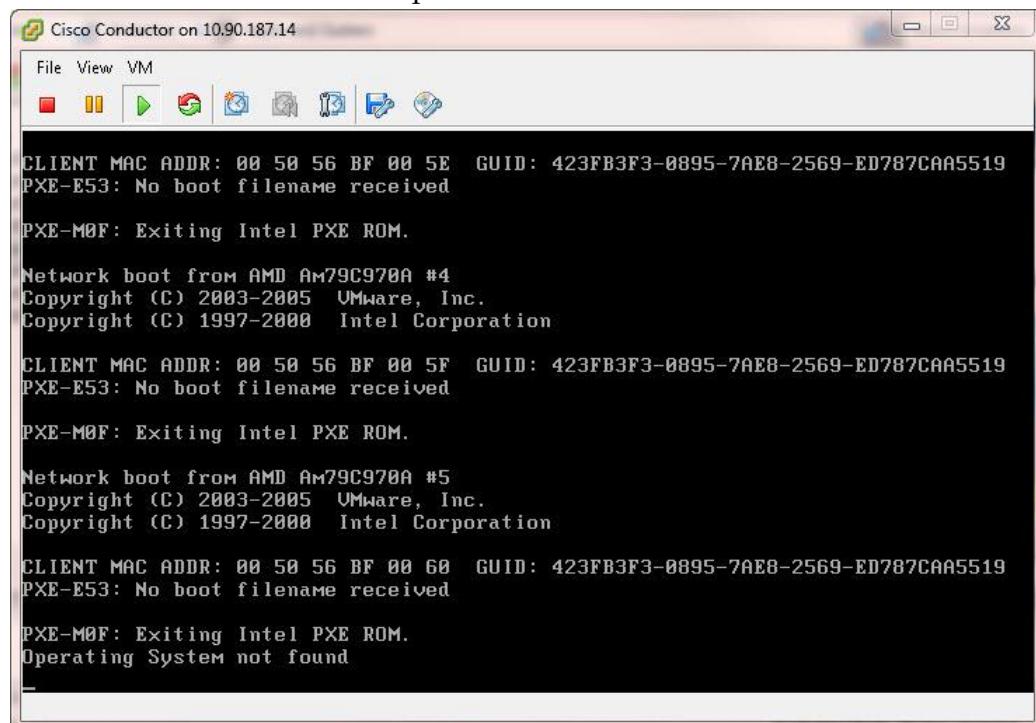
- 5 Click to highlight your newly created virtual machine.

- 6 Right-click, select **Power**, and then select **Power on**.

Result: The VM powers on.

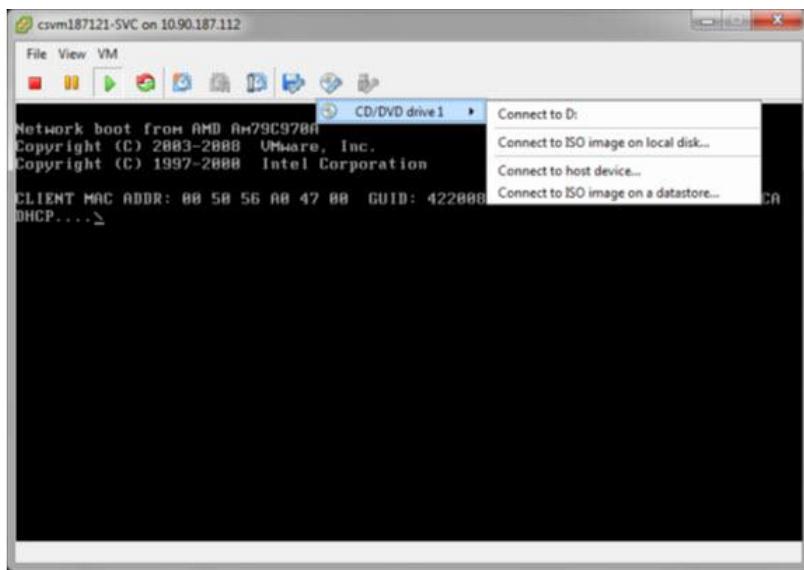
- 7 Right-click the newly created virtual machine and select **Open Console**.

Result: The console window opens.

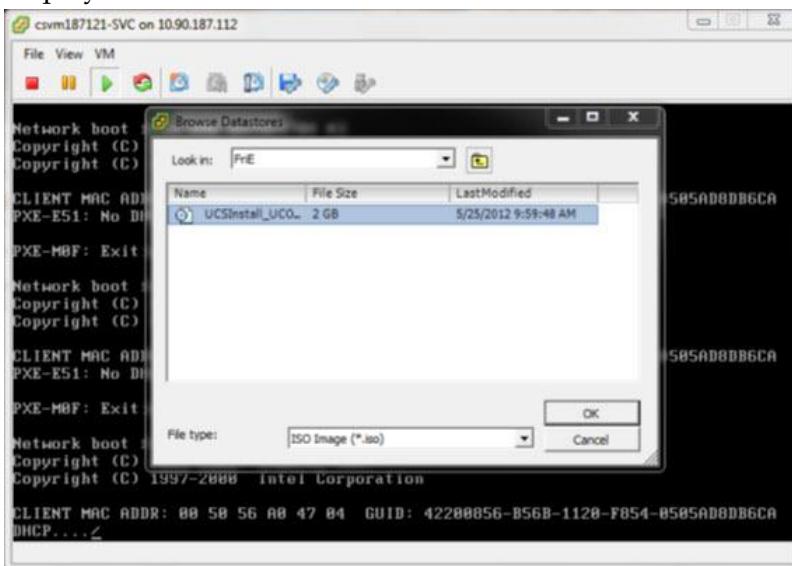


Chapter 4 Install the Videoscape Control Suite Software

- 8 Follow these instructions to attach the ISO file.
 - a Right-click the disk symbol on the console window.
 - i If ISO image is on the local disk, select **Connect to ISO image on local disk**.
 - ii If ISO image is on a datastore, select **Connect to ISO image on datastore**.



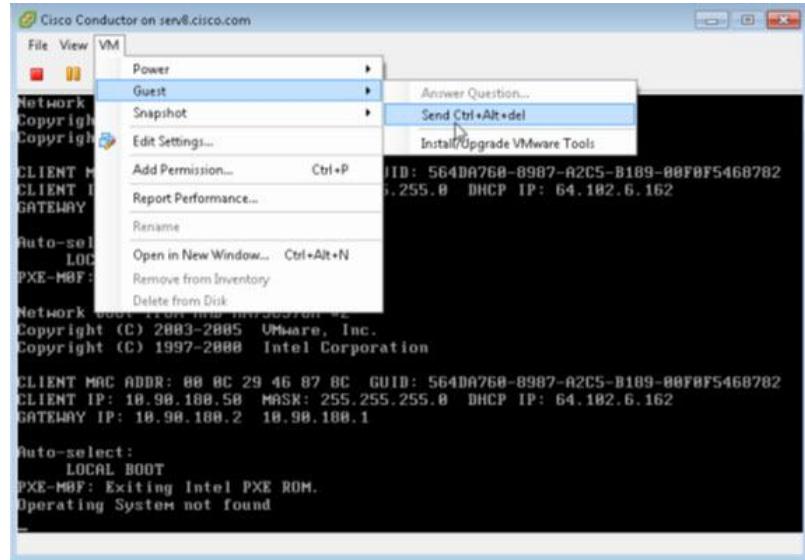
- b Navigate to the directory that contains the ISO file.
 - c Double-click on the ISO file. A pop-up window with the ISO file you selected displays.



- d Select **OK** to attach this ISO image.
- 9 Follow these instructions to restart the virtual machine.
 - a Click **VM** at the top of the console window.
 - b Click to highlight **Guest**.

Mount the ISO and Begin the Videoscape Control Suite Installation

- c Click Send Ctrl+Alt+del.



Results:

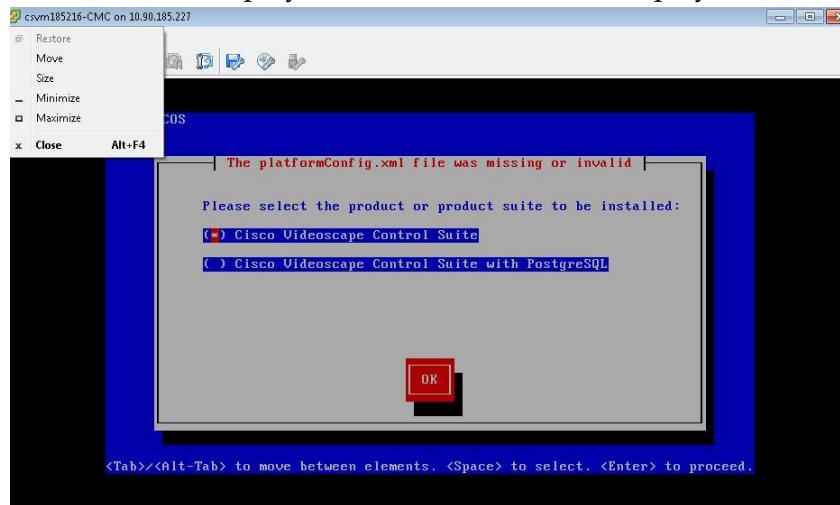
- The virtual machine reboots from the ISO image that you have just connected from the CD/DVD drive.
 - The ISO image begins to install.
- 10 Follow these instructions to connect the virtual floppy disk.
- a Right-click the floppy symbol on the console window.
 - i If ISO image is on the local disk, select **Connect to floppy image on local disk**.
 - ii If ISO image is on a datastore, select **Connect to floppy image on datastore**.
 - b Navigate to the directory that contains the floppy file.
 - c Double-click on the floppy file. A pop-up window with the floppy file you selected displays.
 - d Select **OK** to attach this floppy image.

Notes: Navigating in the VM Console:

- To make changes in the VM Console window, move the mouse cursor over the window and click. This puts the mouse cursor inside the VM console window.
- To move about the window, use the **Tab** and up/down arrow keys.
- To return the mouse cursor to Windows control, simultaneously press the **Ctrl** and **Alt** keys.
- **Important:** Do not simultaneously press **Ctrl**, **Alt**, and **Delete**.

Result: The virtual floppy disk is now mounted for use in the VM console window.

11 Is the Product Deployment Selection window displayed?

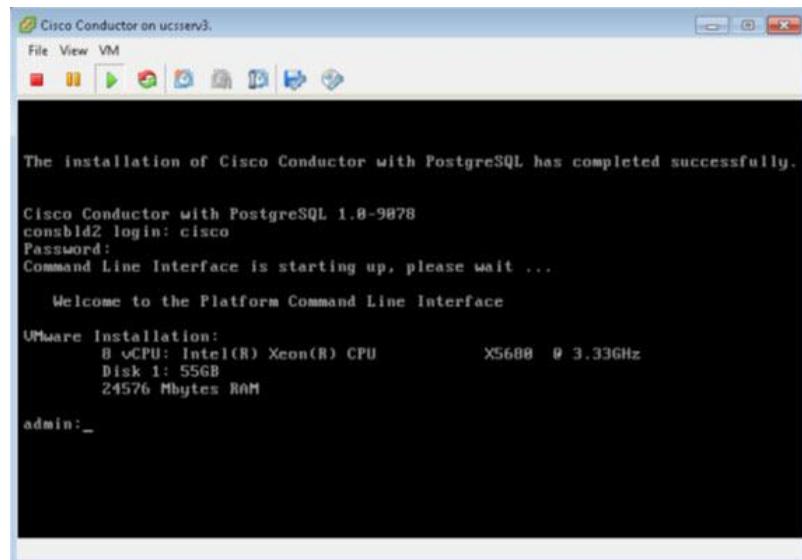


- If **yes**, click **OK** and then go to *Manual Product Deployment Selection* (on page 43) to complete the Videoscape Control Suite installation.

- If **no**, continue with the next step.

12 Click inside the VM console window.

13 Wait for the system login prompt to appear, which indicates that the installation was successful.

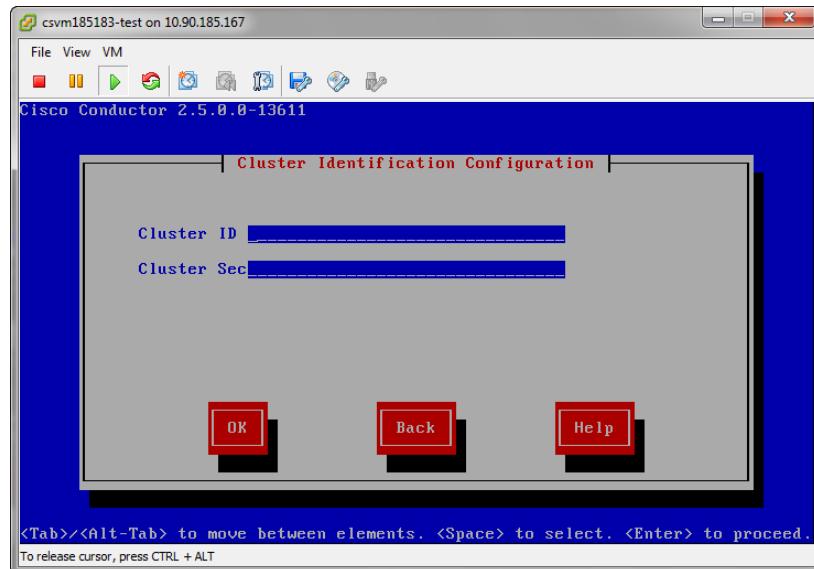


14 Choose one of the following options.

- If your Videoscape Control Suite makes use only of the platformConfig.xml file (no cluster file), go to *Videoscape Control Suite Easy Install* (on page 57).
- Otherwise, go to *What's Next?* (on page 70).

Manual Product Deployment Selection

- When the Cluster Identification Configuration window appears, type in the **Cluster ID** and the **Cluster Secret**. Then, click **OK**.

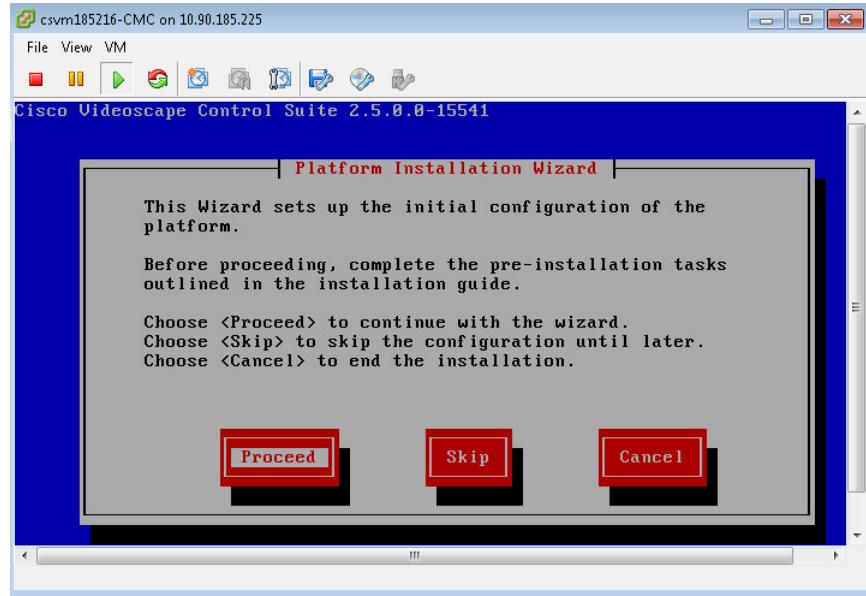


- Select one of the following, based upon the type of node you are installing:
 - If you are installing the database (PostgreSQL) node, select **Cisco Videoscape Control Suite with PostgreSQL**.
Note: Cisco Videoscape Control Suite with PostgreSQL is for Cisco lab use, only.
 - If this is not the database node, select **Cisco Videoscape Control Suite**.

Chapter 4 Install the Videoscape Control Suite Software

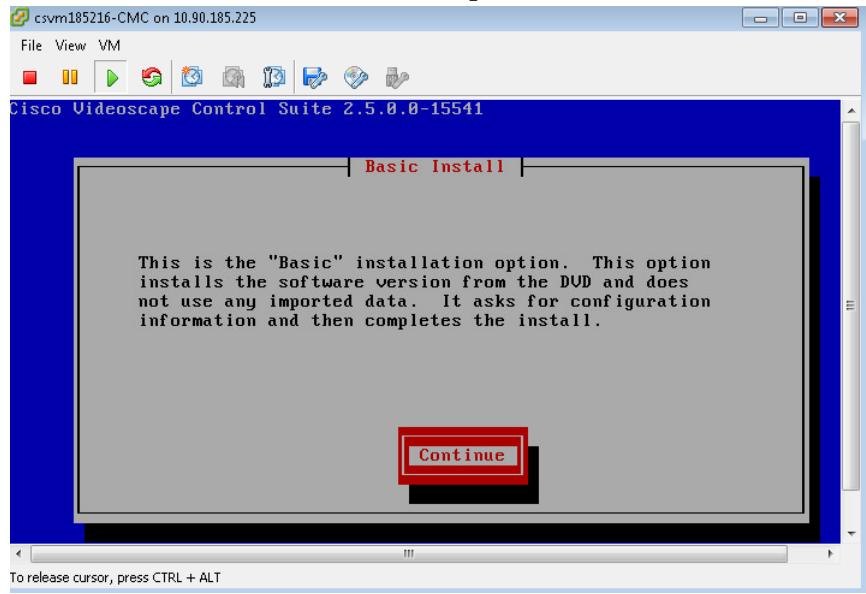
- 3 On the Proceed with Install window, be certain that **Yes** is selected and press **Enter**.

Result: The Platform Installation Wizard window opens.



- 4 The Platform Installation Wizard is required to complete the platform configuration. The screen defaults to **Proceed**. Press **Enter** to proceed.

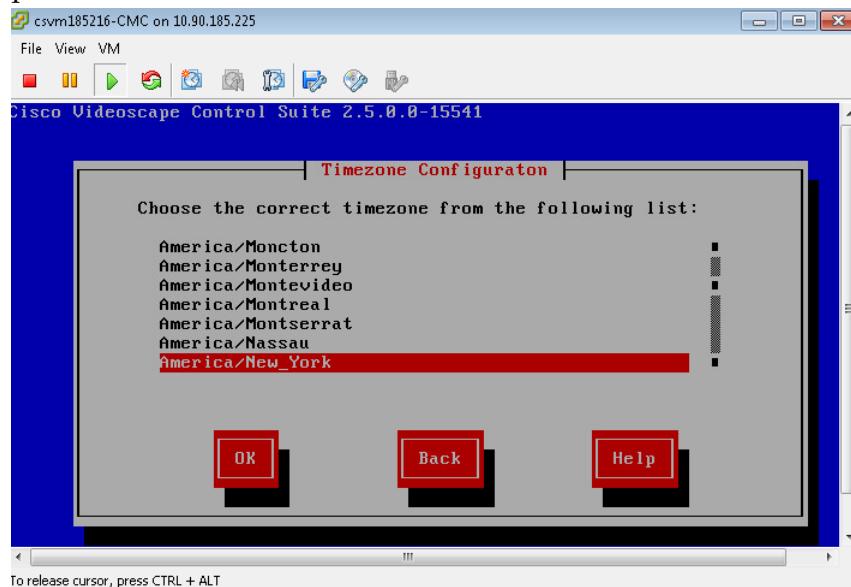
Result: The Basic Install window opens.



- 5 Read the message on the Basic Install window and then press **Enter** to continue.

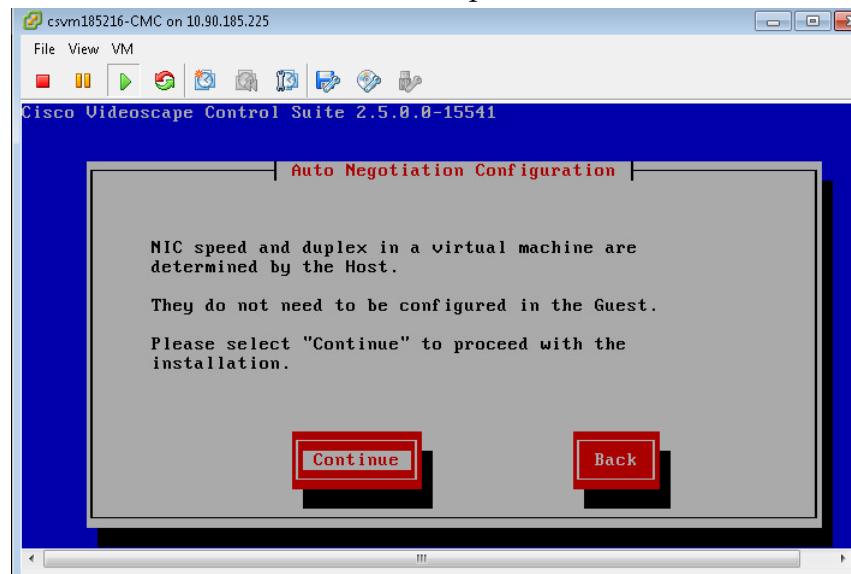
Result: The Timezone Configuration window opens.

- 6 Use the up or down arrow keys to select the correct timezone, which is the timezone where you installed the UCS platform. Then, tab down to **OK** and press **Enter**.



Result: The Auto Negotiation Configuration window opens.

- 7 NIC speeds are determined by the host. The screen defaults to **Continue**, which is the correct choice. Press **Enter** to proceed.

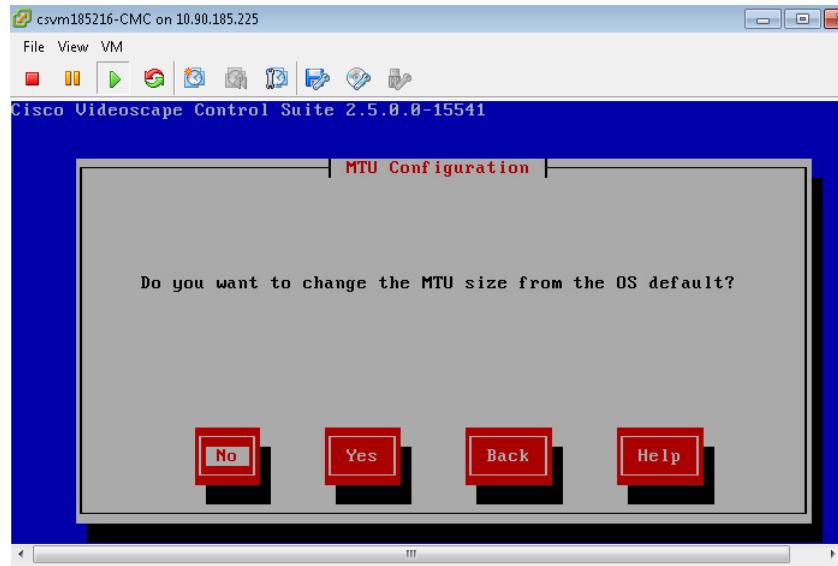


Result: The MTU Configuration window opens.

Note: MTU is an acronym for maximum transmission unit. It refers to the size of the largest packet of data that a network protocol can transmit.

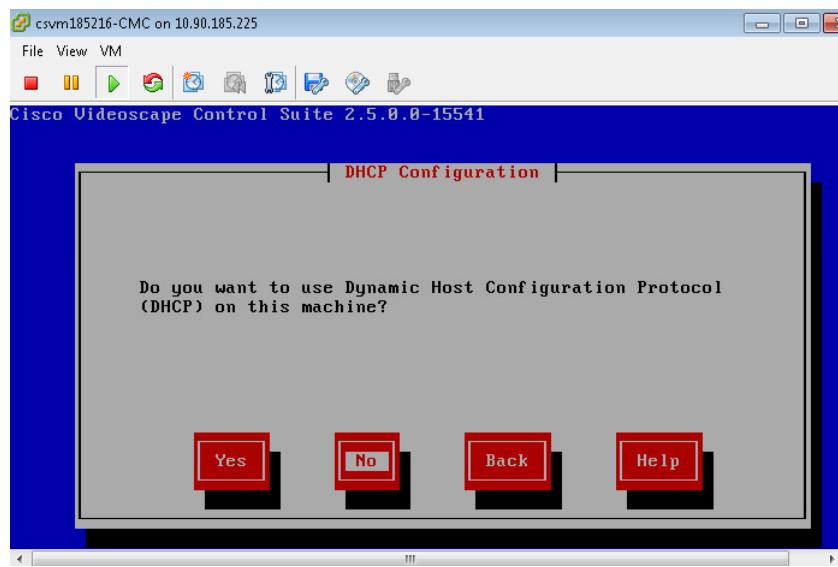
Chapter 4 Install the Videoscape Control Suite Software

- 8 There is no need to change the MTU size from the OS default. The screen defaults to **No**, which is the correct choice. Press **Enter** to proceed.



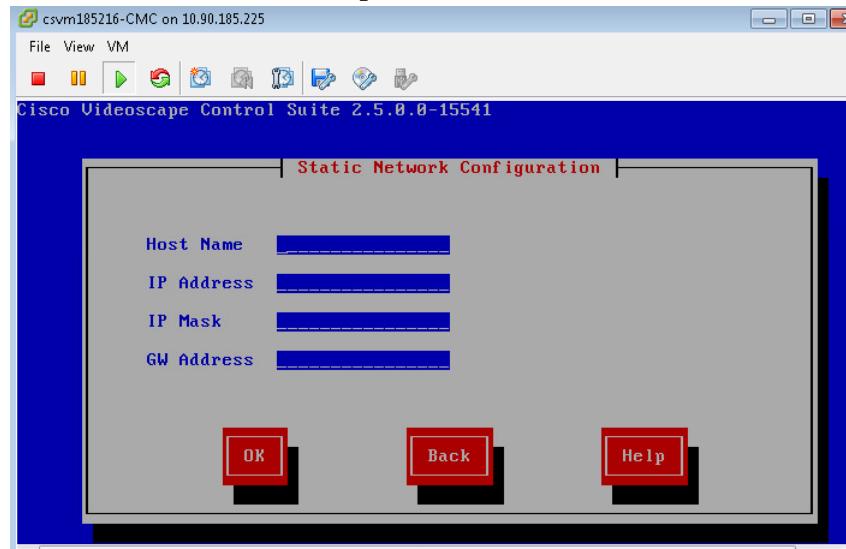
Result: The DHCP Configuration window opens.

- 9 DHCP is not used to assign IP addresses for the Videoscape Control Suite. The screen defaults to **No**, which is the correct choice. Press **Enter** to proceed.



Result: The Static Network Configuration window opens.

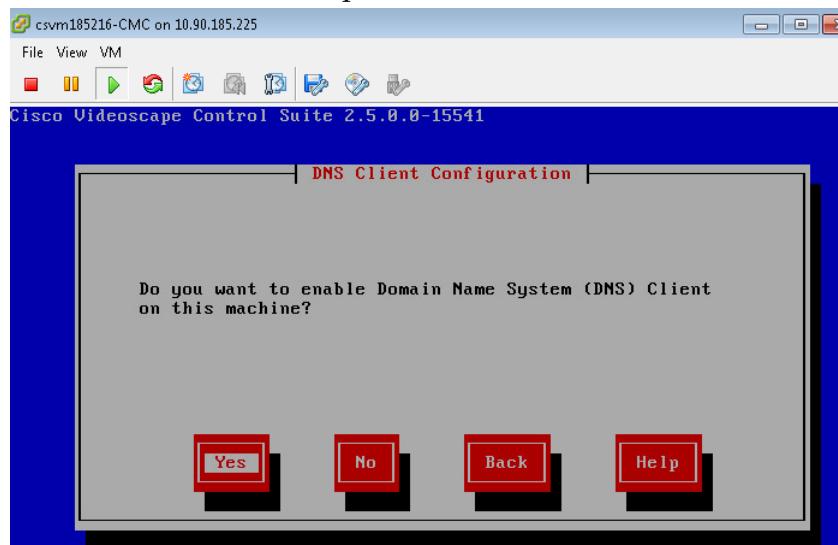
- 10 The Videoscape Control Suite requires a static network configuration. Enter the **Host Name**, **IP Address** (the Management IP address for the blade server), **IP Mask**, and default Gateway (**GW Address**) information in the fields provided. Then tab down to **OK** and press **Enter**.



Result: The DNS Client Configuration window opens.

- 11 Be sure **Yes** is selected and then press **Enter**.

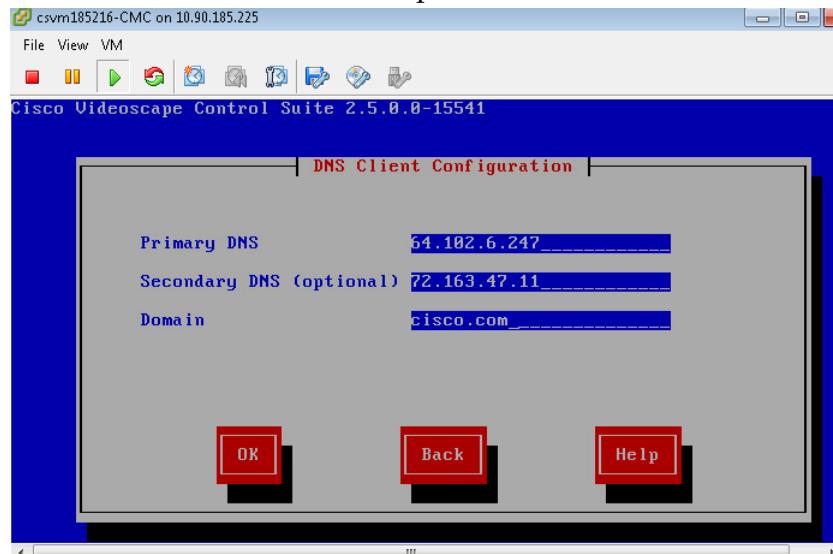
Important: If you are going to add a Domain Name System (DNS), the hosts must be in the DNS table prior to the install.



Result: The DNS Client Configuration window prompts for the **Primary DNS** address and **Domain name**.

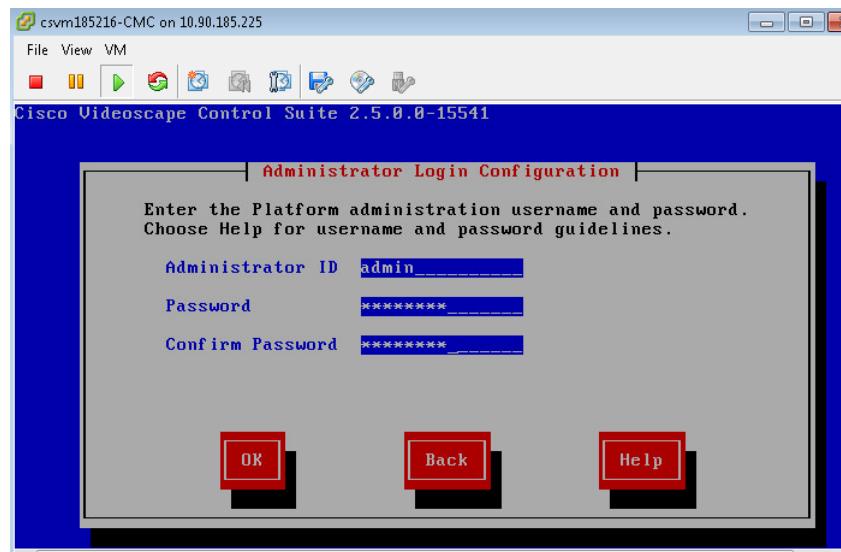
Chapter 4 Install the Videoscape Control Suite Software

- 12 Type the **Primary DNS** address, tab past the **Secondary DNS** field, and then enter the **Domain** name. Then, press **Enter**.



Result: The Administrator Login Configuration window opens.

- 13 The Videoscape Control Suite requires an **Administrator ID** and **Password**. Enter the information in the fields provided, then tab down to **OK** and press **Enter**.

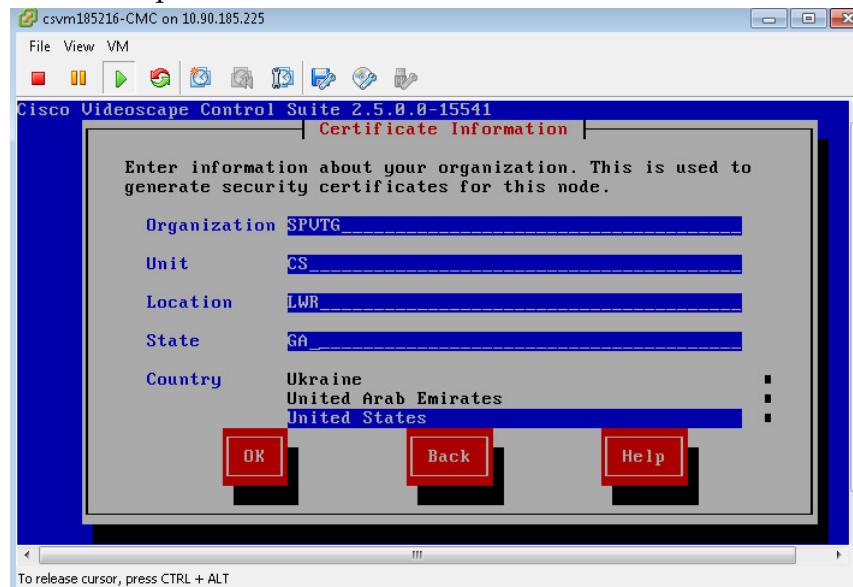


Notes:

- Click **Help** for a list of character restrictions for passwords and administrator IDs.
- The administrator ID cannot be *root*.

Result: The Certificate Information window opens.

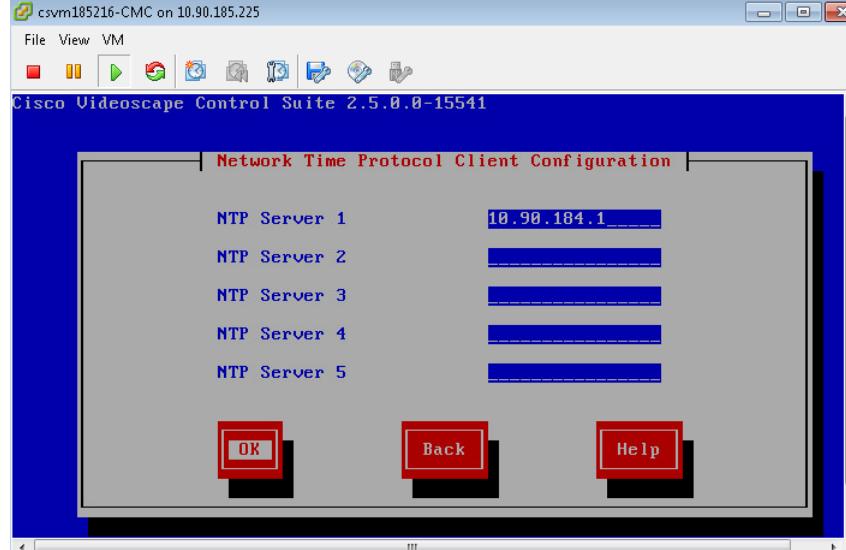
- 14 The Videoscape Control Suite is identified by **Organization**, **Unit**, **Location**, **State**, and **Country**. Enter the information in the fields provided; then, tab down to **OK** and press **Enter**.



To release cursor, press CTRL + ALT

Result: The Network Time Protocol Client Configuration window opens.

- 15 The Videoscape Control Suite needs at least one NTP server address configured to update the NTP client. Enter the information in the fields provided; then, tab down to **Yes** and press **Enter**.

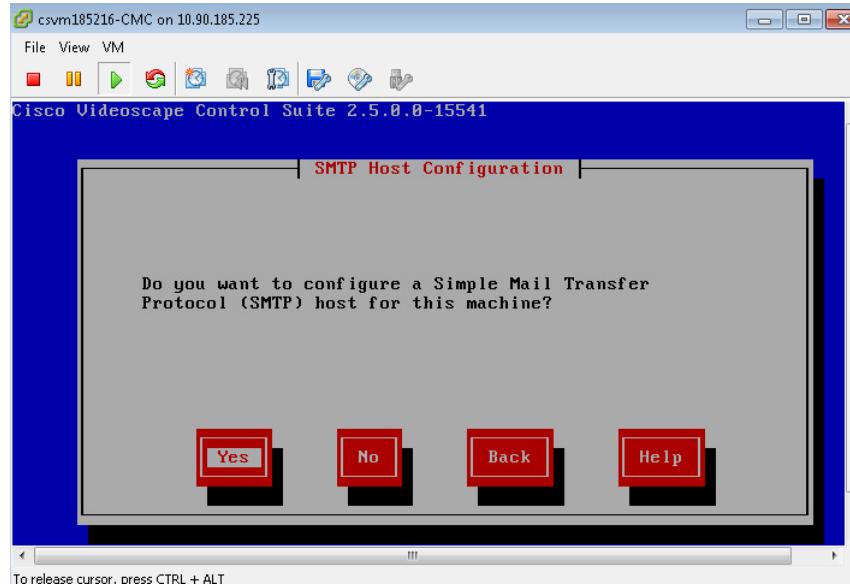


Note: The NTP server identified by the IP address must be accessible or the ISO installation will fail.

Result: The SMPT Host Configuration window opens.

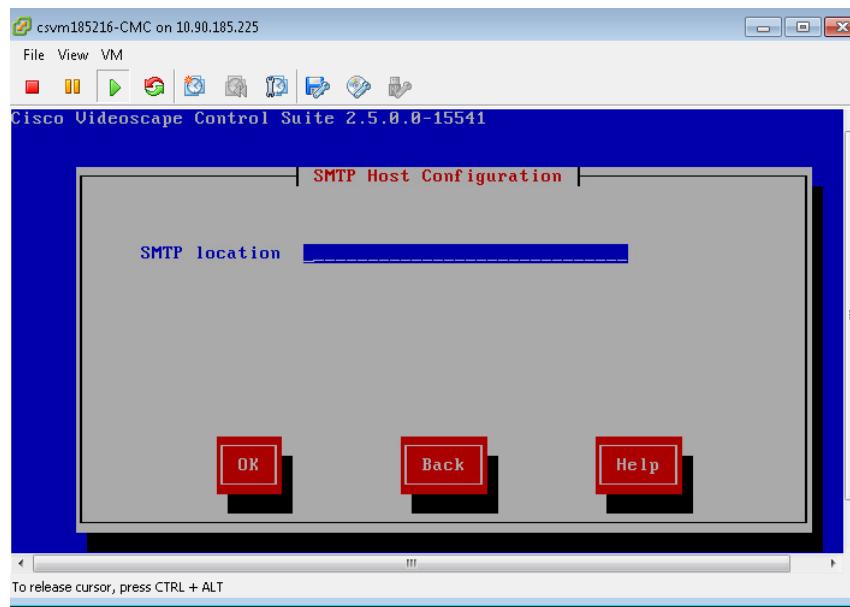
Chapter 4 Install the Videoscape Control Suite Software

- 16 The SMTP host is an option for the Videoscape Control Suite. Tab over to **Yes** or **No** according to your intentions and press **Enter** to proceed.

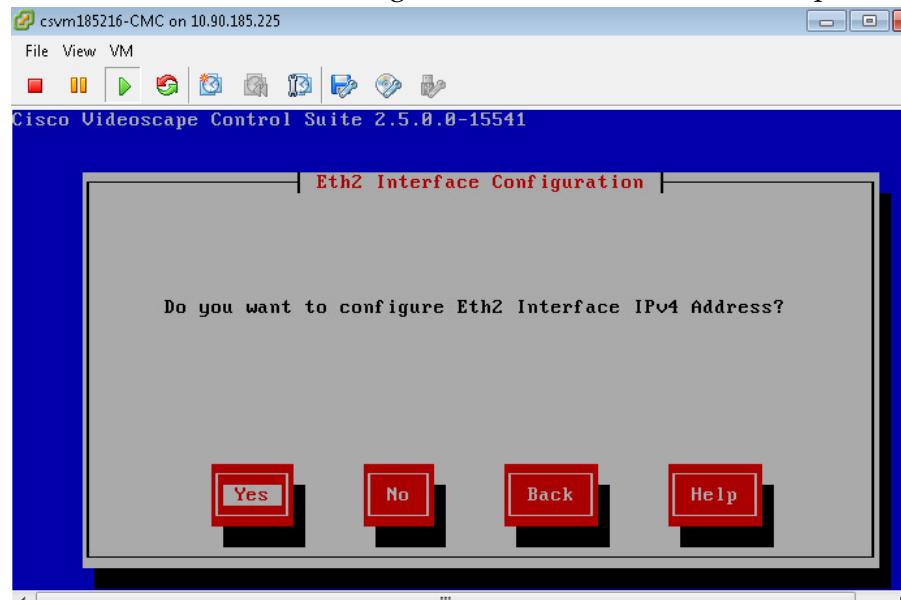


Result: The SMTP Host Configuration window updates to allow for the entry of the SMTP location, if you selected Yes.

- 17 Enter the IP address of the SMTP host. Then, tab down to **OK** and press **Enter**.

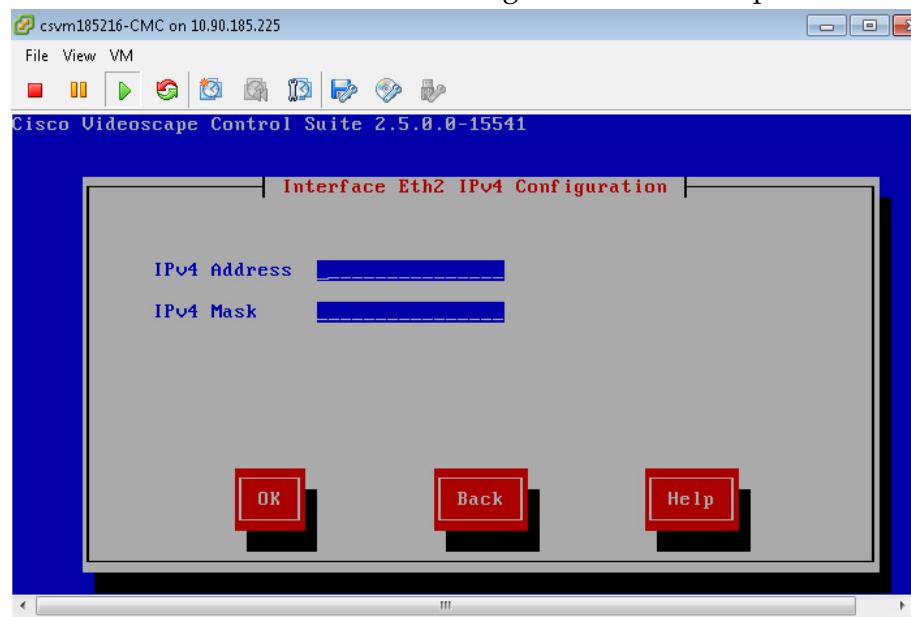


Result: The window to configure the eth2 interface for IPv4 opens.



18 Click Yes.

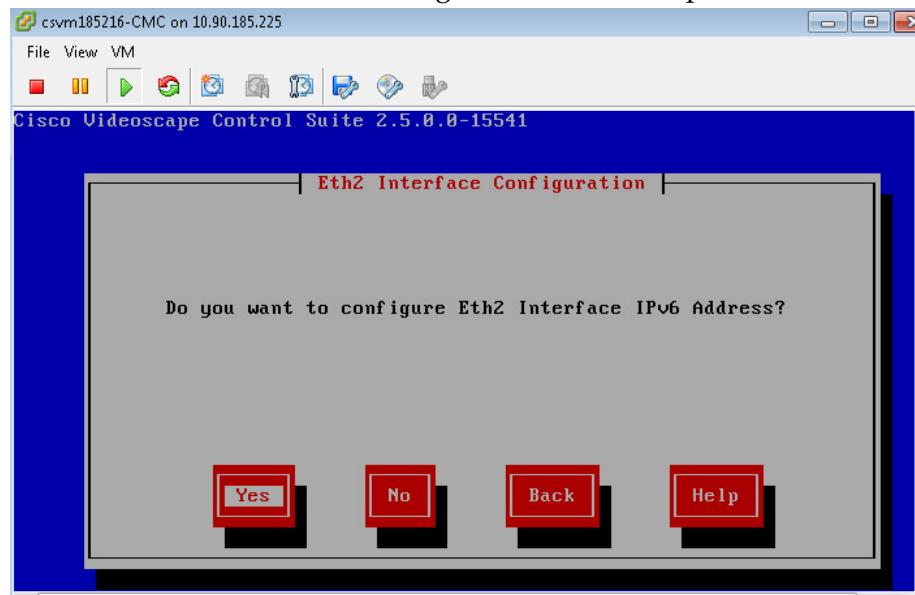
Result: The Interface Eth2 IPv4 Configuration window opens.



Chapter 4 Install the Videoscape Control Suite Software

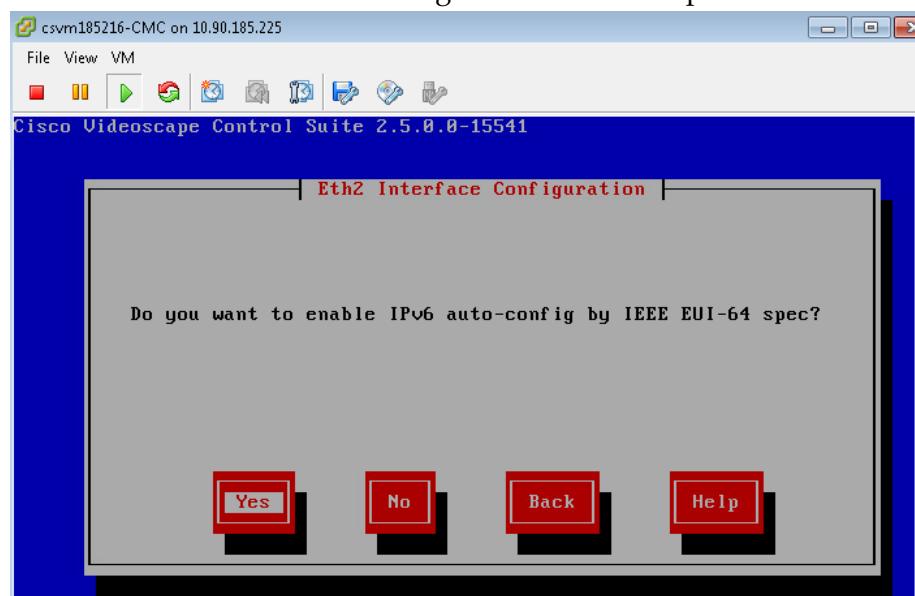
19 Type the IPv4 Address and the IPv4 Mask; then, click OK.

Result: The Eth2 Interface Configuration window opens.



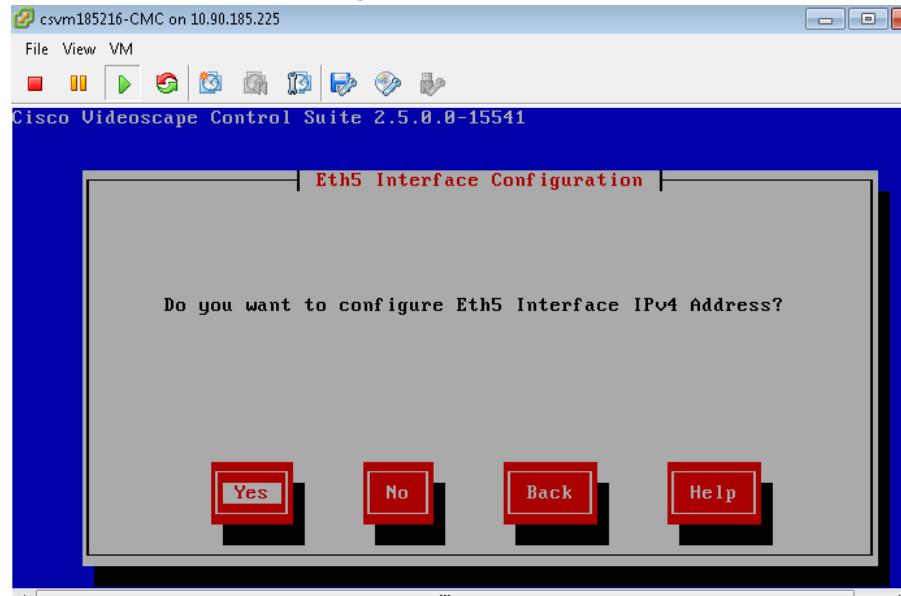
20 Click Yes at the prompt to configure the Eth2 IPv6 address.

Result: The Eth2 Interface Configuration window opens.



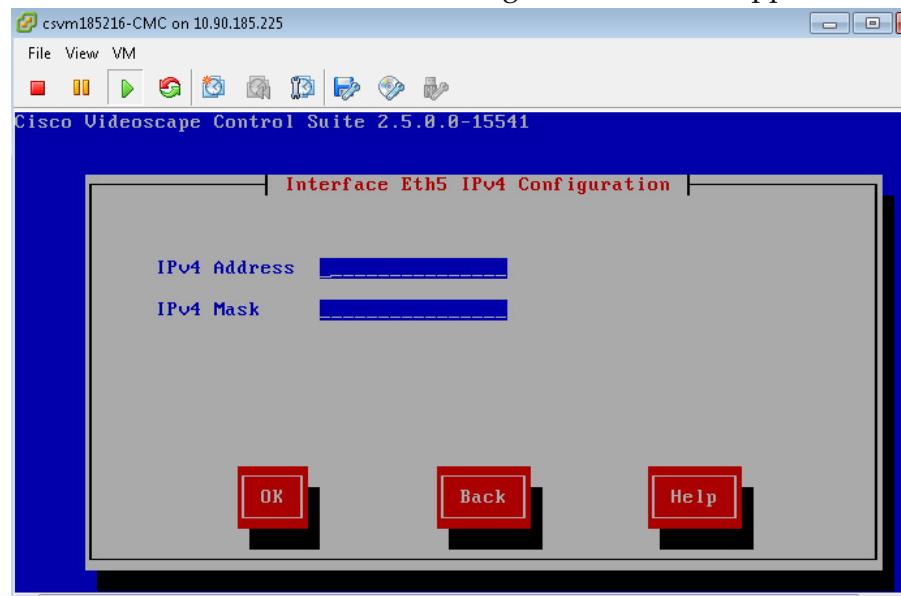
- 21 Click **Yes** at the prompt whether to enable IPv6 auto-config by IEEE EUI-64 spec.

Result: A prompt to configure the Eth5 interface IPv4 address appears.



- 22 Click **Yes** when prompted whether to configure the Eth5 interface IPv4 address.

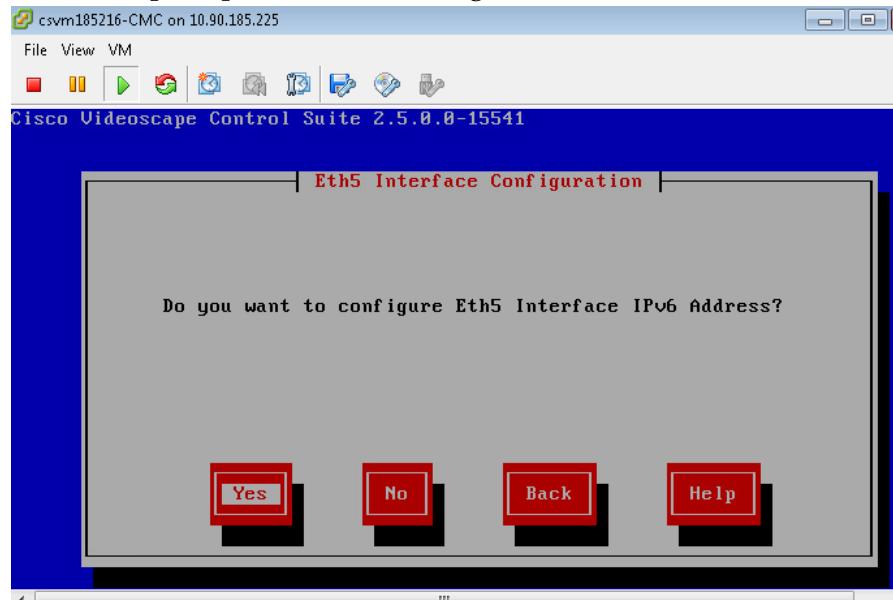
Result: The Interface Eth5 IPv4 Configuration window appears.



Chapter 4 Install the Videoscape Control Suite Software

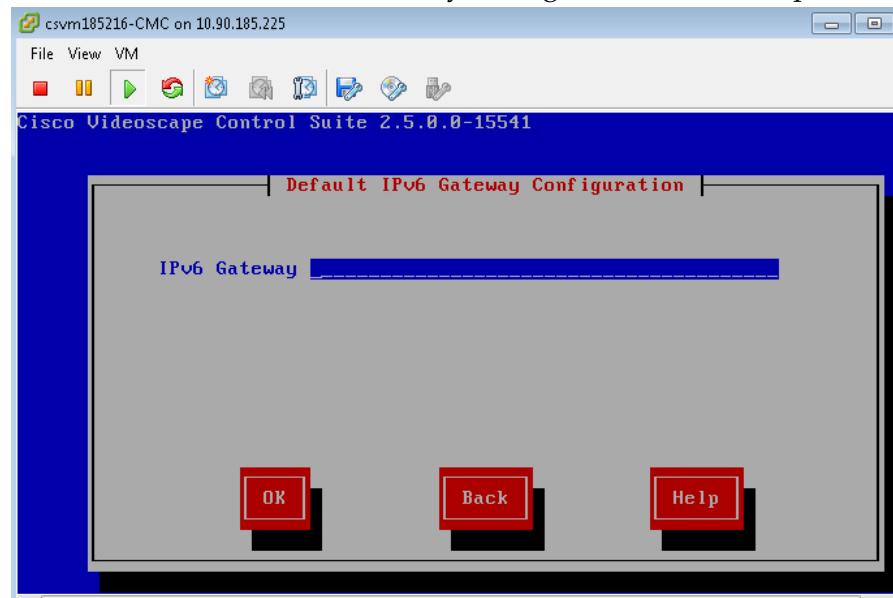
23 Type the IPv4 Address and the IPv4 Mask; then, click OK.

Result: A prompt whether to configure the Eth5 interface IPv6 address appears.



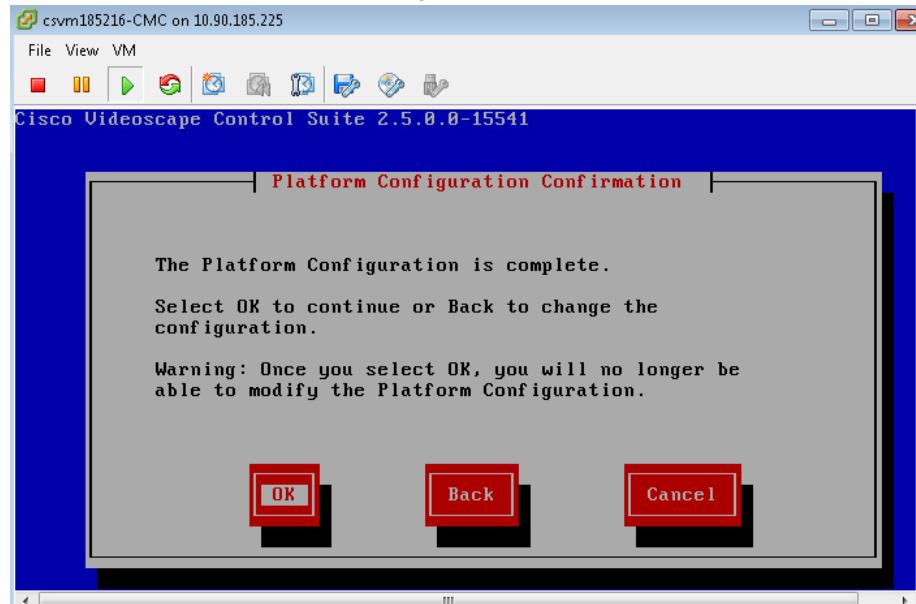
24 Click Yes.

Result: The Default IPv6 Gateway Configuration window opens.

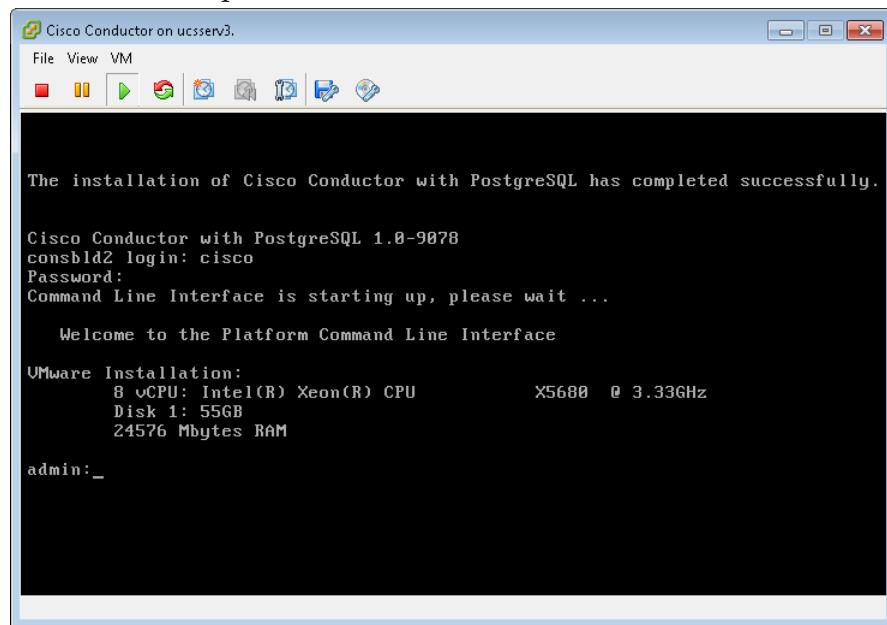


- 25 Type the **IPv6 Gateway** value and then click **OK**.

Result: The ISO installation begins.



Note: Installation can take anywhere from 30 minutes to an hour during which time the virtual machine reboots several times. When installation completes, this text appears in the console window. This is the Command Line Interface (CLI) for the Videoscape Control Suite.



Chapter 4 Install the Videoscape Control Suite Software

- 26** Log in with the platform administrator ID and password. Then, use the CLI as needed.
- 27** Choose one of the following options:
 - If a cluster.xml file was used in your installation, go to *What's Next?* (on page 70).
 - If no floppy file, or only the platformConfig.xml file, was used in your installation, go to *Videoscape Control Suite Easy Install* (on page 57).

Videoscape Control Suite Easy Install

Because of the complexity involved in installing the Videoscape Control Suite, Cisco engineers developed this Easy Install method. The Videoscape Control Suite and the Message Infrastructure (Msginfra) installation can now be performed from the management console.

Important: The Single Msginfra Node of the Easy Install method is designed to install a demo system or a testbed for developers quickly. The Msginfra installation will occur on the first "service node" detected in the Node list. The user cannot select the node to be installed. For a full test environment, it is better to build the Msginfra using the Multiple Node Mode.

This Easy Install method will make use of the platformConfig.xml floppy file. After completing the installation of the ISO image, all nodes default to service nodes. Once you have completed the installation of the service nodes, decide which node will be your Management Node(s). Then, complete the following steps on this node.

Set the Node to be the Management Node

Set the Videoscape Control Suite Database Information

Important: Once the database has been configured, it cannot be changed.

- 1 Log into the CLI with the Platform Administrator ID and password.

Example: `ssh admin@csvm185216`

- 2 Is your database "Oracle"?

- If **yes**, go to step 3.

Important: If the DNS was not set in the platformConfig.xml file, be sure to set the DNS server to the primary DNS server IP address before configuring the database.

- If **no** (it is PostgreSQL), go to step 5.

Note: PostgreSQL is for Cisco internal lab use, only.

Chapter 4 Install the Videoscape Control Suite Software

- 3 Type the following command and press Enter.

```
set vcs database oracle
```

Note: The syntax of this command is as follows:

```
set vcs database oracle hostname port servicename msginfrauser
msginfrausersecret platformuser platformusersecret
hostname      mandatory    oracle hostname
port          mandatory    oracle port
servicename   mandatory    oracle service name
msginfrauser  mandatory    oracle user for msginfra
msginfrausersecret mandatory oracle user secret for
msginfra
platformuser   mandatory    oracle user for platform
platformusersecret mandatory oracle user secret for
platform
```

Example:

```
set vcs database oracle 10.90.184.247 1521 orcl CSVM185169-MSG
Cisco123 CSVM185169-PLAT Cisco123
```

Result: The following messages appear:

The Oracle could be connected successfully

The Oracle DB is set successfully

- 4 Go to *Set the Videoscape Control Suite Node Type* (on page 59).

- 5 Type the following command and press Enter.

```
set vcs database postgresql
```

Notes:

- PostgreSQL is for Cisco internal lab use, only.
- The syntax of this command is as follows:

```
set vcs database postgresql ip port
ip      mandatory    postgresql ip address
port    mandatory    postgresql port
```

Example: set vcs database postgresql 10.90.187.192 5432

Result: The following messages appear:

The PostgreSQL could be connected successfully

The PostgreSQL DB is set successfully

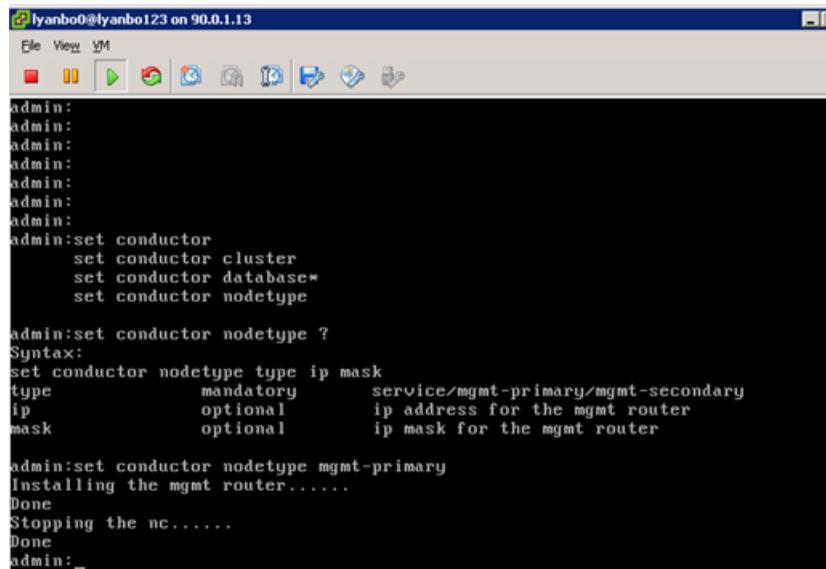
- 6 Go to *Set the Videoscape Control Suite Node Type* (on page 59).

Set the Videoscape Control Suite Node Type

Important: Once the Management Node has been configured, it cannot be changed unless the CMC has not yet been installed.

Type one of the following commands and press **Enter**.

- If you are configuring the first Management Node, type **set vcs nodetype mgmt-primary**.
- If you are configuring the second Management Node, type **set vcs nodetype mgmt-secondary**.



```
lyanbo0@lyanbo123 on 90.0.1.13
File View VM
  ■  □  ▶  ○  ⌂  ⌃  ⌄  ⌅  ⌆  ⌇  ⌈  ⌉
admin:
admin:
admin:
admin:
admin:
admin:
admin:
admin:set conductor
      set conductor cluster
      set conductor database*
      set conductor nodetype

admin:set conductor nodetype ?
Syntax:
set conductor nodetype type ip mask
type      mandatory      service/mgmt-primary/mgmt-secondary
ip       optional        ip address for the mgmt router
mask     optional        ip mask for the mgmt router

admin:set conductor nodetype mgmt-primary
Installing the mgmt router.....Done
Stopping the nc.....Done
admin:_
```

Note: If the Management Router is on a different subnet than the Bootstrap Router, the IP address and netmask is required. This creates the R2R (router-to-router) association for the management and bootstrap routers.

Result: The system sets the node to be the Management Node.

Install the CMC COP File on the Management Node

- 1 To install the Videoscape Control Suite Management Console, see *Installing COP Files for the Videoscape Control Suite* (part number OL-27753).
- 2 When you are finished installing the CMC COP file, return to these instructions and continue with *Deploy the Videoscape Control Suite on Service Nodes* (on page 60).

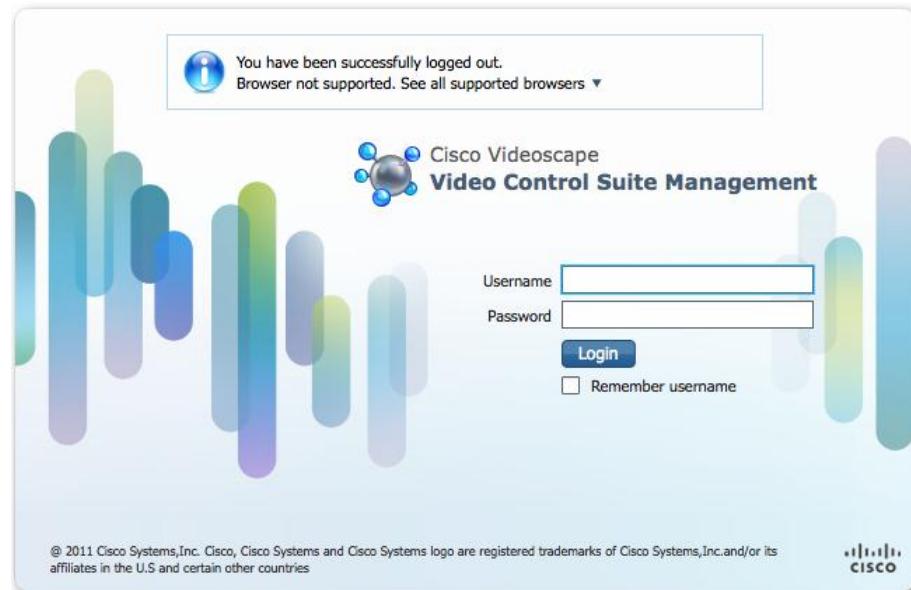
Deploy the Videoscape Control Suite on Service Nodes

The contents of this section guide you through the steps of deploying Videoscape Control Suite on Service Nodes.

Message Infrastructure Deployment

- 1 Open the Firefox version 5 or Internet Explorer version 9 browser and enter the Management Node IP address in the URL text box.

Example: `https://mgmt_node_ip`

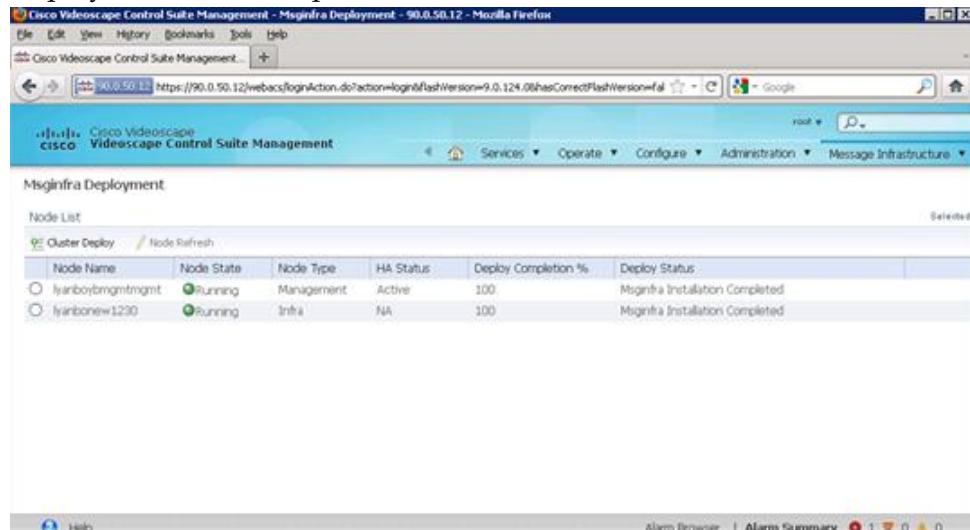


Note: The default **Username** is **root** and the default **Password** is **Public123**. You can change the password after login.

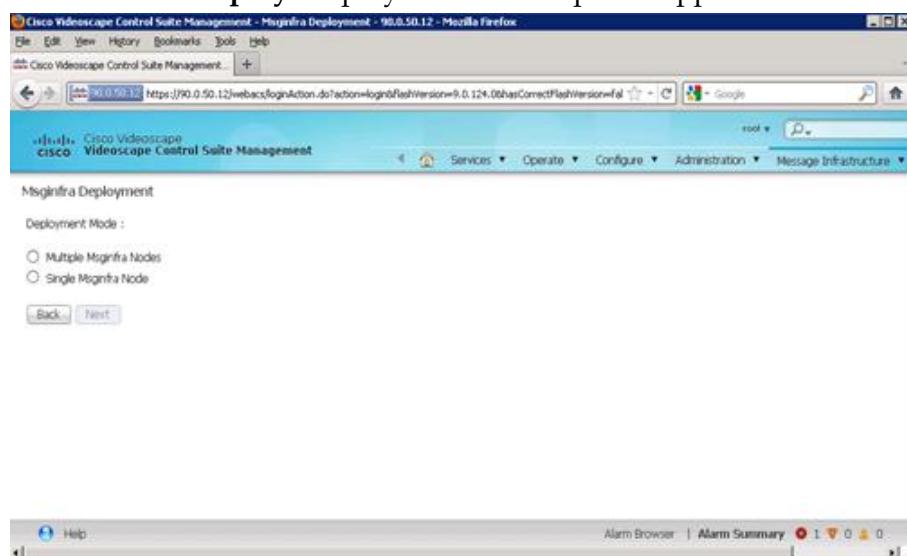
Result: The Conductor Nodes window opens.

Node ID	State	Node Name	IP Address	Memory Usage %	Disk Usage %	CPU Utilization %	RAM Size(kB)	Disk Size(kB)	SysUpTime
1001	●	lyanboybmgt	90.0.50.12	16.4%	16.9%	1.3%	4902672	27101896	19H 30M 50S
1002	●	lyanbonew123	90.0.50.235	1.9%	0.5%	0.0%	345604	6772670	0H 37M 12S

- 2 Click Message Infrastructure --> Msginfra Deployment. The Msginfra Deployment window opens.



- 3 Click Cluster Deploy. Deployment Mode options appear.



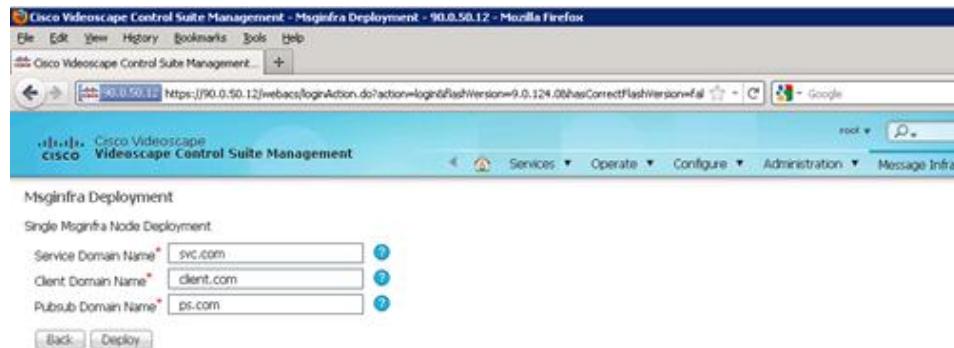
- 4 Choose one of the following deployment options.

- If you want to deploy one Msginfra Node, go to **One Msginfra Node**, which follows.
- If you want to deploy multiple Msginfra Nodes, go to **Multiple Msginfra Nodes** (on page 63).

Chapter 4 Install the Videoscape Control Suite Software

One Msginfra Node

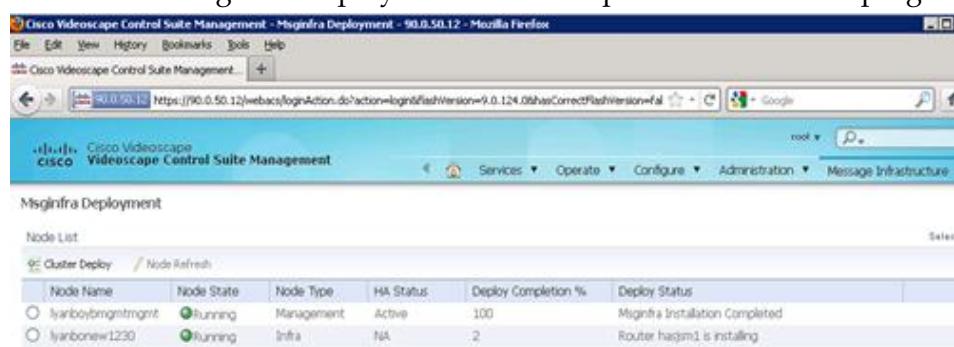
- 1 Click One Msginfra Mode and then click Next.
- 2 Enter the Service Domain Name, the Client Domain Name, and the Pubsub Domain Name. Then, click Deploy.



Notes:

- Valid values for the domain names are alpha-numeric, as well as some special characters: ._-.
- The length should be from 1 to 255 characters.
- The domain name "pubsub.service" and "pubsub.virtual" are reserved for internal usage.
- The first and last character MUST be alpha-numeric.
- The Service Domain Name, Client Domain Name, and Pubsub Domain Name must be unique.
- Reference the online help for additional limitations.

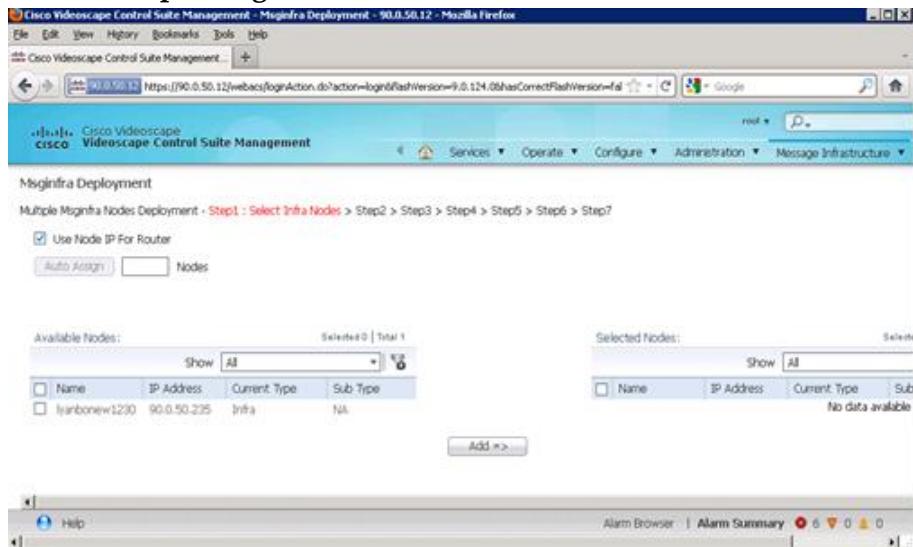
Result: The Msginfra Deployment window opens and tracks the progress.



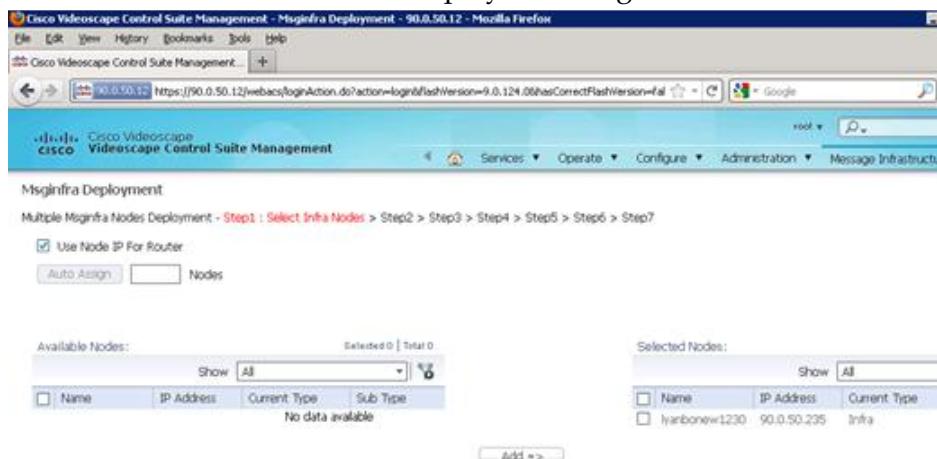
Note: When the Deploy Status changes to **Msginfra Installation Completed**, then the Msginfra has been deployed successfully.

Multiple Msginfra Nodes

- 1 Click Multiple Msginfra Nodes and then click Next.

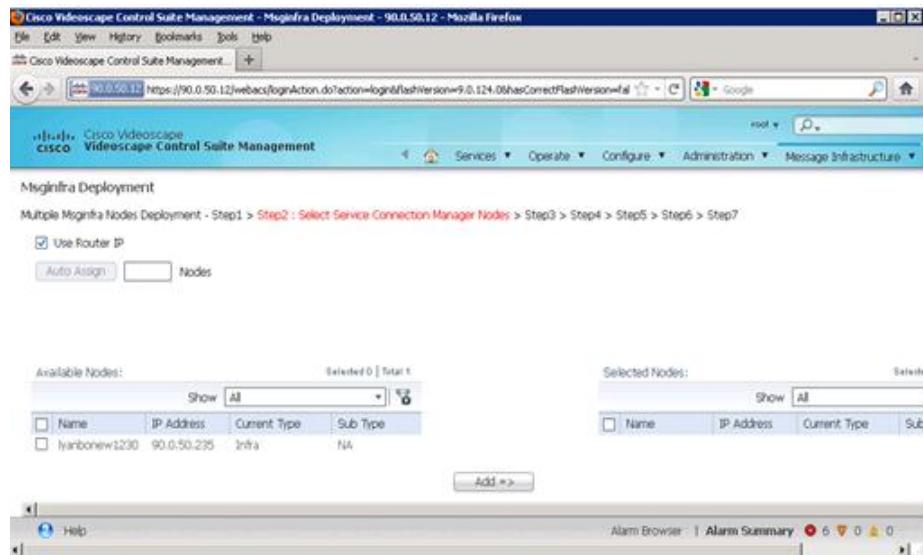


- 2 Do you want to set different IP addresses for the routers?
- If yes, uncheck the **Use Node IP for Router** field.
- Notes:**
- This option is used to separate the traffic from eth0 and to bind it to eth4.
 - You will need to input the IP address range, as well as the Netmask.
- If no, be sure that the **Use Node IP for Router** field has a check-mark beside it.
- 3 In the **Available Nodes** list, select the nodes that you want to deploy, and then click **Add**. These nodes will be deployed as Msginfra Nodes.



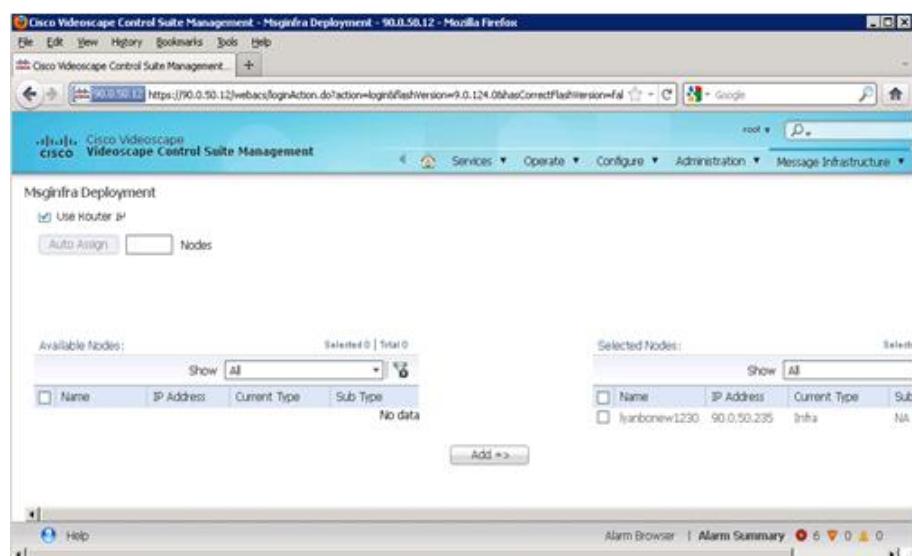
Chapter 4 Install the Videoscape Control Suite Software

- 4 Click Next to select the Service Connection Manager Nodes.



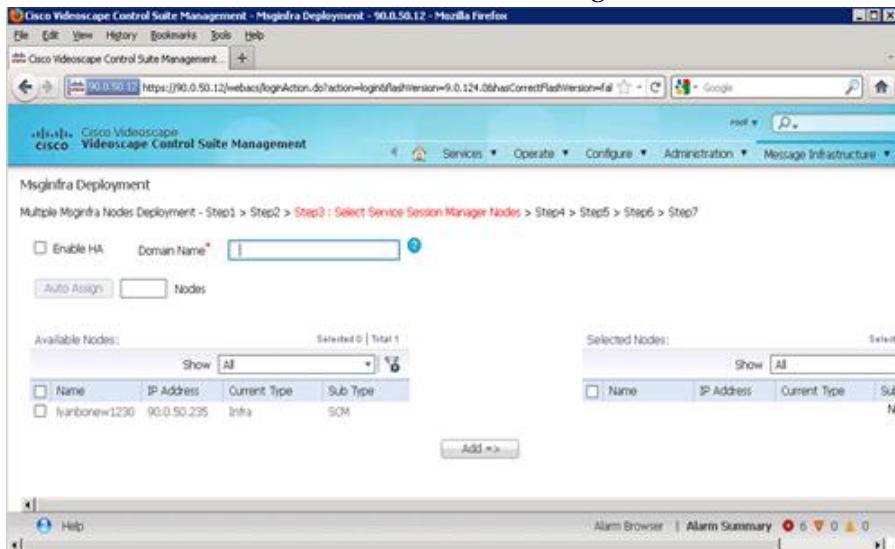
Notes:

- If you want to use a different IP address for the Connection Manager than the router IP address, uncheck **Use Router IP**.
 - This option is used to separate the SCM from eth0, and to bind it to eth1.
- 5 In the **Available Nodes** list, select the nodes that you want to deploy, and then click **Add**.



Note: You can use the GUI to modify the number of CMs.

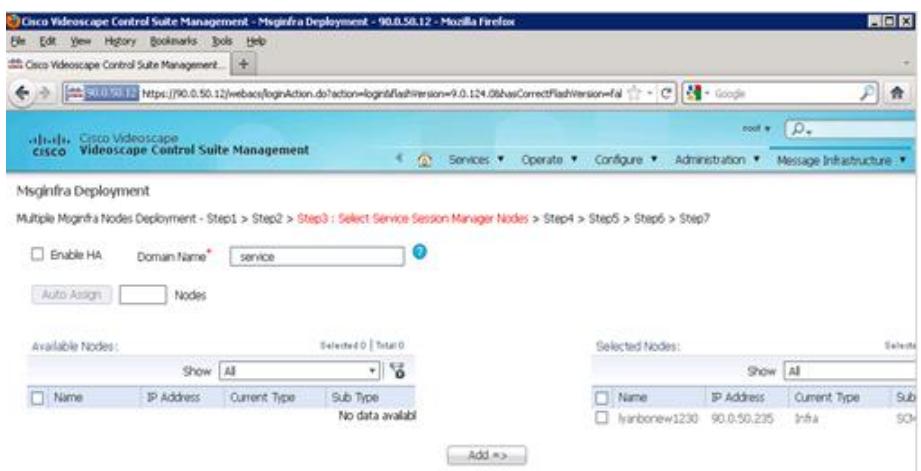
- 6 Click Next to select the Service Session Manager Nodes.



- 7 Enter the **Domain Name**.

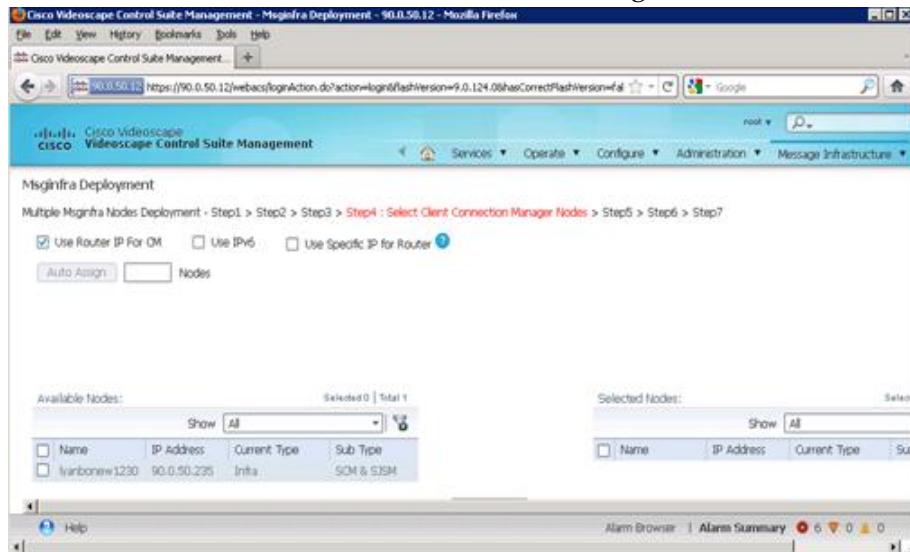
- 8 In the **Available Nodes** list, select the nodes that you want to deploy, and then click **Add**.

Note: If you check **Enable HA**, the number of nodes you select must be an even number.



Chapter 4 Install the Videoscape Control Suite Software

- 9 Click Next to select the Client Connection Manager Nodes.



- 10 Uncheck **Use Router IP for CM** if you want to use a different IP address for the Connection Manager than the IP address of the router.

Notes:

- **Use Router IP for CM** to separate the SCM from eth0.
- **Use IPv6** is similar to IPv4, but with a different protocol.
- **Use Specific IP for Router** when some nodes are outside of the firewall. It establishes an S2S connection between the CCM and the SCM.

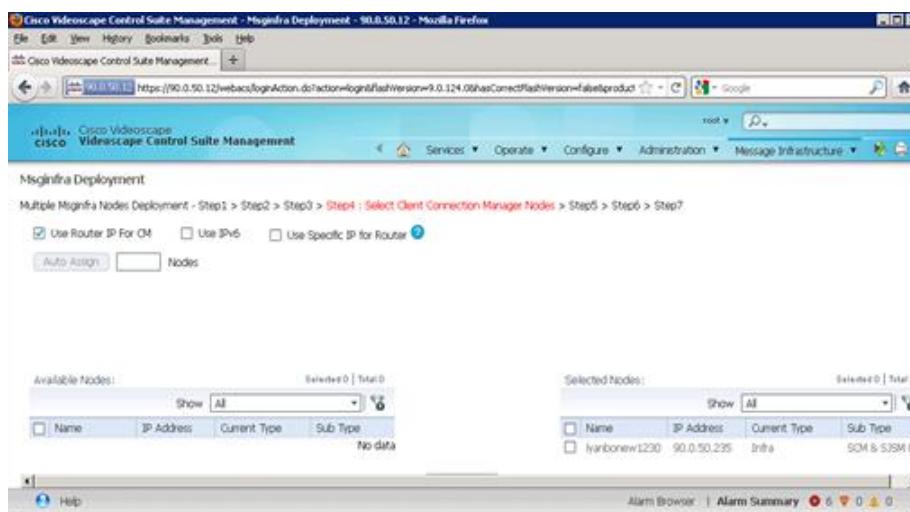
- 11 If you want to use the IPv6 protocol, check **Use IPv6**.

Note: IPv4 is the default protocol.

- 12 If you want to use a specific IP address for the Client Connection Manager, check **Use Specific IP for Router**.

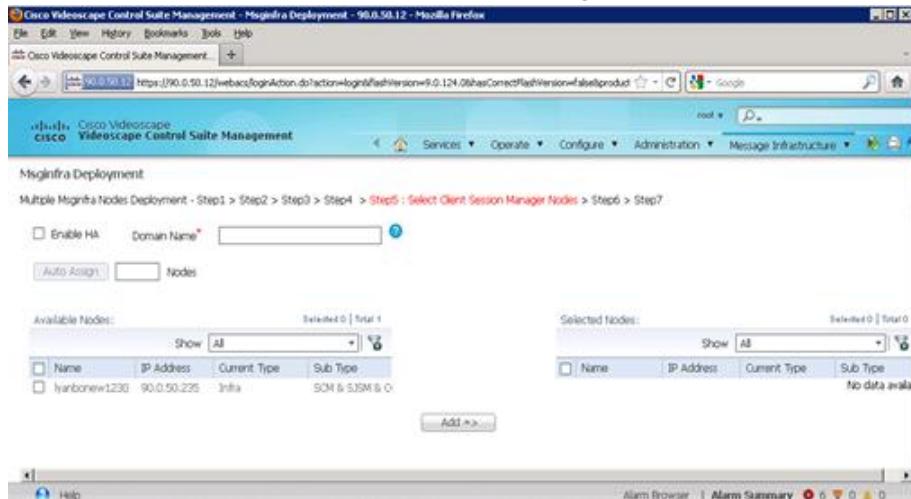
Note: The router IP address is only supported in the IPv4 protocol.

- 13 In the **Available Nodes** list, select the nodes that you want to deploy, and then click **Add**.



Videoscape Control Suite Easy Install

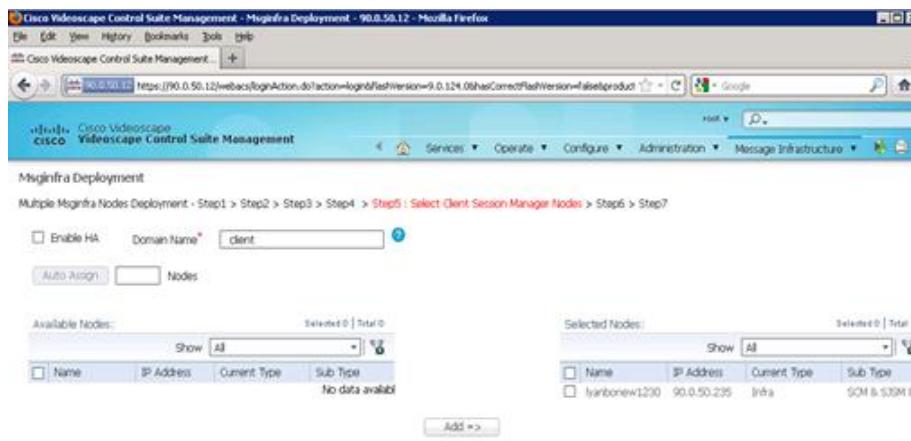
- 14 Click Next to select the Client Session Manager Nodes.



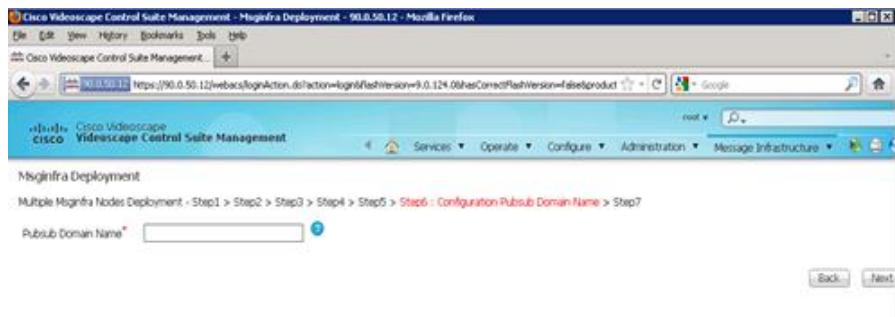
- 15 Enter the Domain Name.

- 16 In the Available Nodes list, select the nodes that you want to deploy, and then click Add.

Note: If you check **Enable HA**, the number of nodes you select must be an even number.



- 17 Click Next to set the Pubsub Domain Name.



Chapter 4 Install the Videoscape Control Suite Software

- 18 Enter the **Pubsub Domain Name** and click **Next** to display an overview of the Msginfra nodes.

This screenshot shows the 'Msginfra Deployment' section of the Cisco Videoscape Control Suite Management interface. It displays two nodes: 'lyanboymgrmt' (IP 90.0.50.12) and 'lyanbonew1230' (IP 90.0.50.235). The table provides details such as IP Address, Current Type, Sub Type, CPU, and Memory.

Name	IP Address	Current Type	Sub Type	CPU	Memory
lyanboymgrmt	90.0.50.12	Management	N/A	8 X 2930 MHz	24GB
lyanbonew1230	90.0.50.235	Infra	SOM 6, SSM 6, COM 6, CSM	4 X 2930 MHz	16GB

- 19 Click **Deploy**. The Msginfra Deployment window appears, which shows deployment progress.

This screenshot shows the 'Node List' section of the 'Msginfra Deployment' window. It lists two nodes: 'lyanboymgrmt' (Status: Running, Deploy Completion %: 100) and 'lyanbonew1230' (Status: Running, Deploy Status: Router hagent is installing).

Node Name	Node State	Node Type	HA Status	Deploy Completion %	Deploy Status
lyanboymgrmt	Running	Management	Active	100	Msginfra Installation Completed
lyanbonew1230	Running	Infra	N/A	1	Router hagent is installing

Node Refresh -- Reinstall the Msginfra on the Node

- 1 Open a Firefox version 5 or Internet Explorer version 9 browser.
- 2 In the URL text box, enter the Management Node IP address.

Note: The default Username is root and the default Password is Public123, which you can change over logging in.

Result: The Videoscape Control Suite Nodes window appears.

This screenshot shows the 'Videoscape Control Suite Nodes' window. It displays two nodes: Node ID 1001 (lyanboymgrmt) and Node ID 1002 (lyanbonew1230). The table provides real-time monitoring data including State, Node Name, IP Address, Memory Usage %, Disk Usage %, CPU Utilization %, RAM Size(kB), Disk Size(kB), and SyncUpTime.

Node ID	State	Node Name	IP Address	Memory Usage %	Disk Usage %	CPU Utilization %	RAM Size(kB)	Disk Size(kB)	SynchUpTime
1001	●	lyanboymgrmt	90.0.50.12	18.4%	16.9%	1.3%	4902572	27101886	19H 30M 50S
1002	●	lyanbonew1230	90.0.50.235	1.9%	0.5%	0.0%	345604	6772670	0H 37M 12S

- 3 Click **Message Infrastructure** and then click **Deployment**. Then, click **Msginfra Deployment**.

The screenshot shows the 'Msginfra Deployment' page. At the top, there's a navigation bar with tabs like 'Services', 'Operate', 'Configure', 'Administration', and 'Message Infrastructure'. Below the navigation bar is a 'Node List' table with two rows:

Node Name	Node State	Node Type	HA Status	Deploy Completion %	Deploy Status
Iyanboribmgmtmngt	Running	Management	Active	100	Msginfra Installation Completed
Iyanborinew1230	Running	Infra	NA	100	Msginfra Installation Completed

- 4 Select an infra node from the **Node List** and then click **Node Refresh**. The window updates to show progress.

The screenshot shows the same 'Msginfra Deployment' page after refreshing. The 'Deploy Status' column now includes a progress bar and text indicating the status of each node:

Node Name	Node State	Node Type	HA Status	Deploy Completion %	Deploy Status
Iyanboribmgmtmngt	Running	Management	Active	100	Msginfra Installation Completed
Iyanborinew1230	Running	Infra	NA	1	Router hagpm1 is installing

What's Next?

Important: Cisco engineers recommend that you now take a snapshot of your VMs from vSphere.

- 1 Right-click on a VM.
- 2 Select **Snapshot**.
- 3 Select **Take Snapshot**.
- 4 Save your snapshots so that you can refer to them in the event of an issue with a VM.

At this point, you should refer to the following two guides to complete the installation of the Videoscape Control Suite:

- *Cisco Conductor Management Console User Guide* (part number OL-26324)
- *Installing COP Files for the Videoscape Control Suite* (part number OL-27753)

5

Configure High Availability

Introduction

Use the information in this chapter to help you configure High Availability (HA) for the Videoscape Control Suite.

In This Chapter

- Configuring High Availability 72
- Deleting High Availability 75

Configuring High Availability

- 1 Select **Operate --> High Availability --> Setup**. The High Availability Configuration window opens.
- 2 Use the following information to configure the High Availability Configuration window.
 - **Management IP Address** – Enter the IP address of the Virtual IP you would like to use for management of HA.
 - **Peer Hostname** – Enter the hostname for the other configured Management node.
 - **Enable Peer HA** – Check this box.
- 3 Click **Save**.

Example: The completed High Availability Configuration window should look similar to this example when you are finished and the **High Availability has been initiated** message will appear.

High Availability Configuration

Local Hostname : **csvm18570**

Management IP Address :

Subnet Mask :

Peer Hostname : **csvm18571**

Enable Peer HA :

Save

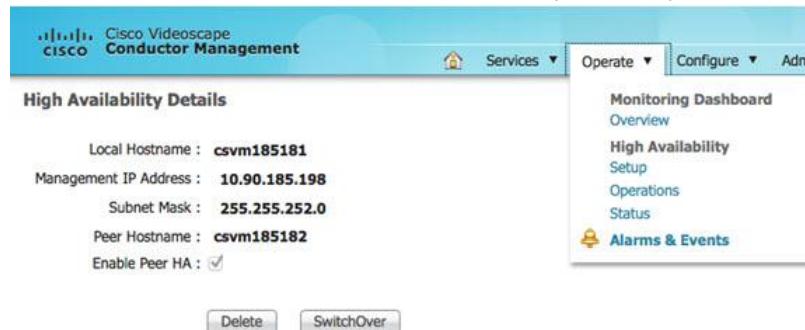
Note: This operation may take as long as 30 minutes on a C210 server or a B210 M2 server, and about an hour on a B200 M3 server.

- 4 Log into the CMC using the Virtual IP address you configured for the Management IP Address in step 2.
- Note:** The username is **root**; the password is **Public123**.
- 5 After logging in, click **Operate --> High Availability --> Status** to verify that the databases have synchronized with one another. The High Availability Status window should look similar to this example.

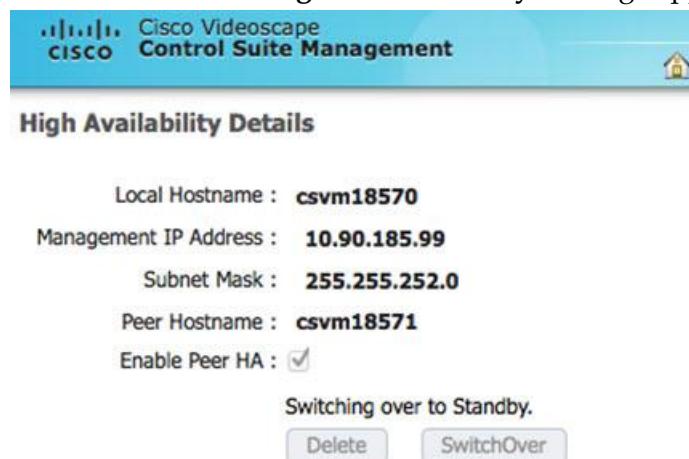
High Availability Status

Node ID	State	Node Name	HA State	HA Node Type	Database Sync Status	Last Switchover Time
1002		csvm18571	standby	secondary	synced	N/A
1005		csvm18570	active	primary	synced	2013-May-07, 02:05:36 EDT

- 6 Click **Operate --> High Availability --> Operations**, and then click **Switchover** to perform the switchover to the secondary-standby mode.



Result: The **Switching over to Standby** message appears.



Notes:

- This operation usually takes between 10 and 30 minutes to complete.
- The Delete and SwitchOver buttons are grayed out during this operation.
- The CMC is unavailable during this operation.

- 7 After the switchover is complete, click **Operate > High Availability > Status** to confirm that the databases are synchronized and that the status of the secondary node is active.

Node ID	State	Node Name	HA State	HA Node Type	Database Sync Status	Last Switchover Time
1002	●	csvm18571	active	secondary	synced	2013-May-07, 16:21:14 EDT
1005	●	csvm18570	standby	primary	synced	N/A

Note: The High Availability mode can be deleted only when the primary node is in an active state. The **Delete** option is grayed out when the secondary node is active.

HA Status Descriptions

- **Active** — All conditions are good. The active node is backed up by the standby node and there are no errors.
- **Standby** — The standby node is good and the HA feature is working normally and reports no errors.
- **Active-No_peer** — This status appears only when the standby node has a problem and is not reachable. With this status, the HA Status table has only one row for the active node. The peer node is not displayed.

HA Node Type Descriptions

- **Primary** — Preferred Primary node.
- **Secondary** — Preferred Secondary node.

Deleting High Availability

- 1 Click **Operate --> High Availability --> Operations**, and then click **Switchover**. A confirmation message appears.
- 2 Click **OK**. The message **Switching over to Standby** appears.



Note: This operation takes between 10 and 30 minutes to complete. The CMC is unavailable during this operation.

- 3 After the switchover has completed, click **Operate --> High Availability --> Status** to confirm that the databases are synchronized and that the secondary node is **active**.

High Availability Status						
Node ID	State	Node Name	HA State	HA Node Type	Database Sync Status	Last Switchover Time
1002	●	csvm18571	active	secondary	synced	2013-May-07, 16:21:14 EDT
1005	●	csvm18570	standby	primary	synced	N/A

- 4 Click **Operate --> High Availability --> Operations**, and then select **Delete** to delete the HA configuration. A confirmation message appears.
- 5 Click **OK**. The **High Availability configuration removal initiated** message appears.



Chapter 5 Configure High Availability

- 6 Click **Operate --> High Availability --> Status** to confirm that the HA configuration has been removed. Only the primary node should be listed.

The screenshot shows a table titled "High Availability Status". The table has columns: Node ID, State, Node Name, HA State, and HA Node Type. There is one row with data: Node ID 1005, State green dot, Node Name csvm18570, HA State NA, and HA Node Type primary.

Node ID	State	Node Name	HA State	HA Node Type
1005	●	csvm18570	NA	primary

- 7 To further confirm, click **Operate --> High Availability --> Setup**. All fields, except **Local Hostname**, should be blank.

High Availability Configuration

The screenshot shows a form titled "High Availability Configuration". It includes fields for Local Hostname (set to "csvm185172"), Management IP Address (empty), Subnet Mask (empty), Peer Hostname (empty), and Enable Peer HA (unchecked). A "Save" button is at the bottom.

Local Hostname : **csvm185172**

Management IP Address :

Subnet Mask :

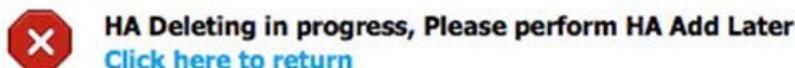
Peer Hostname :

Enable Peer HA :

Save

The Cleanup Process

The cleanup process removes all HA entries and reverts the system back to standalone mode. If someone attempts to configure HA while the cleanup process is still underway, the following message appears.



6

Upgrading the Videoscape Control Suite

Introduction

This chapter includes these procedures.

- **Videoscape Control Suite 2.1 to 2.5 Upgrade** contains the procedures necessary to upgrade an existing Videoscape Control Suite system, currently at version 2.1, to version 2.5 software.
- **Upgrade the Videoscape Control Suite Software** contains procedures necessary to upgrade an existing system at version 2.1 or version 2.5 to a more current version of the same release.

In This Chapter

- Videoscape Control Suite 2.1 to 2.5 Upgrade 78
- Upgrade the Videoscape Control Suite Software..... 84

Videoscape Control Suite 2.1 to 2.5 Upgrade

The purpose of this section is to provide the steps to upgrade the Videoscape Control Suite from Release 2.1 to Release 2.5. This section details the upgrade procedures for the major components of the Videoscape Control Suite platform.

Pre-Upgrade Checklist

Be sure the site you are upgrading meets these requirements:

- Be sure that you have sufficient disk space to perform the upgrade.
Note: More than 50 percent of disk space needs to be available.
- No critical alarms or system errors can exist prior to upgrading. Any errors or alarms must be resolved.
- The CMC needs to be installed and running.
- Full HA must be enabled.
- The upgrade from Release 2.1 to 2.5 does not support the upgrade path from "R2.1 Oracle RAC A-S mode" to "R2.5 Oracle RAC A-A mode". In other words, if the customer has already deployed R2.1 and wants to use R2.5, is to continue to use "Oracle RAC A-S mode" after upgrade to R2.5.

Notes:

- "A-S" is Active-Standby; "A-A" is Active-Active.
- R2.1 Does not support Oracle RAC A-A mode for the production environment.

Pre-Upgrade Preparation Tasks

Complete these tasks prior to upgrading.

- Make a backup snapshot of your virtual machines.
- Back up the NOSQLCB database. FTP the back up files to another server.
Note: See *Videoscape Control Suite Database User Guide* (OL-28290) for instructions on backing up the NOSQLCB database.
- Download the needed images (*.iso, *.cop.sgn, etc) to the CMC Management Node.
- Validate that the entire system is in a healthy state. See the previous section, **Pre-Upgrade Checklist**.
- For a graceful upgrade, check for Standby Peer Readiness.

Platform Upgrade with CMC

Preferred Method

- 1 Download the Release 2.5 signed CMC COP file to the Release 2.1 CMC using the CMC UI. Refer to *Installing COP Files for the Videoscape Control Suite* (part number OL-27753) for instructions on downloading the COP files to the CMC.
- 2 Upgrade the CMC on the secondary-standby node.
 - a Select the secondary-standby node from the Conductor nodes.
 - b Select the **2.5 CMC** from the **COP Images to Install** list.
 - c Select **COP Upgrade** to initiate the COP upgrade to the version 2.5 release of the CMC.
 - d Select **OK** for any confirmation messages.

COP Install

Conductor Nodes

Node ID	Node Name	IP Address	COP Install Completion %	COP Install Status	COP File	Last Updated
<input type="checkbox"/> 1000	csvm18773	10.90.187.73	100	SUCCESS	cisco.conductor-couchbase-2.1-1...	Mon Apr 8 13:11:17 EDT 2013
<input type="checkbox"/> 1001	csvm18772	10.90.187.72	100	SUCCESS	cisco.conductor-couchbase-2.1-1...	Mon Apr 8 13:07:50 EDT 2013
<input type="checkbox"/> 1002	csvm18770	10.90.187.70	100	SUCCESS	cisco.conductor-edn-2.1-1-37%.co...	Thu Apr 11 16:34:10 EDT 2013
<input type="checkbox"/> 1003	csvm18790	10.90.187.90	100	SUCCESS	cisco.conductor-couchbase-2.1-1...	Mon Apr 8 13:11:20 EDT 2013
<input checked="" type="checkbox"/> 1004	csvm18771	10.90.187.71	100	SUCCESS	cisco.conductor-cmc-2.1-1-635.c...	Thu Apr 11 13:06:17 EDT 2013

COP Images to install

COP Install COP Upgrade COP Uninstall

File Name	Image Type	Version	Size	Updated On
<input type="radio"/> cisco.conductor-alertManager-2.1-1-8.cop.sgn	COP	2.1-1-8	16.97 MB (17793548 bytes)	April 11, 2013 4:18:00 PM EDT
<input type="radio"/> cisco.conductor-edn-2.1-1-378.cop.sgn	COP	2.1-1-378	33.28 MB (34900886 bytes)	April 11, 2013 4:21:49 PM EDT
<input checked="" type="radio"/> cisco.conductor-cmc-2.5-0-1122.cop.sgn	COP	2.5-0-1122	3530 MB (3701661532 bytes)	April 12, 2013 11:53:20 AM EDT
<input type="radio"/> cisco.conductor-couchbase-2.1-1-0.cop.sgn	COP	2.1-1-0	119.6 MB (125358344 bytes)	April 11, 2013 4:19:44 PM EDT

Results:

- A message appears that states that the upgrade was successfully initiated.
- Continuing status messages appear until the CMC has actually started the installation.

Note: Once the upgrade begins, the CMC will not be accessible until the upgrade completes.

- 3 After upgrading the CMC on the secondary-standby node, upgrade the CMC on the primary-active node.

Chapter 6 Upgrading the Videoscape Control Suite

- 4 Perform the HA switchover to make the primary-active node the primary-standby node.
 - a Select **Operate --> High Availability --> Operation.**

The screenshot shows the Cisco Videoscape Conductor Management interface. The top navigation bar includes icons for Home, Services, Operate (selected), Configure, and Admin. The main content area is titled "High Availability Details". It displays the following information:

- Local Hostname : **csvm185181**
- Management IP Address : **10.90.185.198**
- Subnet Mask : **255.255.252.0**
- Peer Hostname : **csvm185182**
- Enable Peer HA :

At the bottom are two buttons: "Delete" and "SwitchOver". On the right side of the interface, there is a sidebar with links: Monitoring Dashboard Overview, High Availability Setup, Operations, Status, and Alarms & Events (highlighted).

- b Click **Switchover** to switch to the Standby node.

The screenshot shows the Cisco Videoscape Conductor Management interface after a switchover. The top navigation bar includes icons for Home, Services, Operate (selected), Configure, and Admin. The main content area is titled "High Availability Details". It displays the following information:

- Local Hostname : **csvm185181**
- Management IP Address : **10.90.185.198**
- Subnet Mask : **255.255.252.0**
- Peer Hostname : **csvm185182**
- Enable Peer HA :

At the bottom are two buttons: "Delete" and "SwitchOver". The "SwitchOver" button is now grayed out. On the right side of the interface, there is a sidebar with links: Monitoring Dashboard Overview, High Availability Setup, Operations, Status, and Alarms & Events (highlighted).

Note: This operation may take between 20 and 40 minutes to complete.

- c To check for completion of the switchover select **Operate --> High Availability --> Status**. Once the **Database Sync Status** has changed to **synced**, the switchover operation has completed.

The screenshot shows the Cisco Videoscape Conductor Management interface displaying the "High Availability Status" table. The table has the following columns: Node ID, State, Node Name, HA State, HA Node Type, Database Sync Status, and Last Switchover Time. The data is as follows:

Node ID	State	Node Name	HA State	HA Node Type	Database Sync Status	Last Switchover Time
1005	●	csvm185182	standby	secondary	synced	NA
1006	●	csvm185181	active	primary	synced	NA

- 5 Perform the HA switchover to make the current primary-standby node the primary-active node.

- a Select **Operate --> High Availability --> Operation.**

High Availability Details

Local Hostname : **csvm185181**
Management IP Address : **10.90.185.198**
Subnet Mask : **255.255.252.0**
Peer Hostname : **csvm185182**
Enable Peer HA :

Delete **SwitchOver**

- b Click **Switchover** to switch to the Standby node.

Note: This operation may take between 20 and 40 minutes to complete.

- 6 Perform the ISO upgrade on the current secondary-standby node.
- a Select the secondary-standby node from the Videoscape Control Suite nodes.
- b Select **2.5 ISO** from the **Images to Upgrade** list.
- c Select **Upgrade Image** to initiate the image upgrade to the version 2.5 ISO release.

Image Upgrade

Videoscape Control Suite Nodes

Node ...	State	Node Name	IP Address	Memory Usage ...	Disk Usage %	CPU Utilization %	RAM Size(KB)	Disk Size(KB)	SysUpTime	Platform \
<input type="checkbox"/>	●	csvm18773	10.90.187.73	3.7%	6.6%	1.6%	989152	5269791	9Days 19H 18M 30S	2.1.1.0-1
<input type="checkbox"/>	●	csvm18772	10.90.187.72	3.7%	6.3%	1.3%	978760	4953803	9Days 19H 18M 26S	2.1.1.0-1
<input type="checkbox"/>	●	csvm18770	10.90.187.70	9.5%	6.1%	1.0%	2535048	4835524	9Days 19H 24M 54S	2.1.1.0-1
<input type="checkbox"/>	●	csvm18790	10.90.187.90	3.7%	6.6%	1.5%	978012	5262211	9Days 19H 42M 21S	2.1.1.0-1
<input checked="" type="checkbox"/>	●	csvm18771	10.90.187.71	19.9%	20.7%	2.2%	5287484	33273659	2H 43M 7S	2.1.1.0-1

Software Images to install

Upgrade Node

File Name	Image Type	Version	Size	Updated On
UCInstall_UCOS_2.5.0.0-15163.iso	ISO	2.5.0.0-15163	2115 MB (2217318400 bytes)	April 15, 2013 11:03:49 AM EDT

Note: This node will reboot during the process. Then, the ISO will be launched on this node.

Chapter 6 Upgrading the Videoscape Control Suite

- 7 Perform the HA switchover to make the current secondary-standby node the secondary-active node.
 - a Select **Operate --> High Availability --> Operation.**

The screenshot shows the Cisco Videoscape Conductor Management interface. The top navigation bar includes icons for Home, Services, Operate, Configure, and Admin. The 'Operate' menu is currently selected. On the left, a sidebar menu lists 'Monitoring Dashboard', 'Overview', 'High Availability' (which is selected and highlighted in blue), 'Setup', 'Operations', 'Status', and 'Alarms & Events'. The main content area is titled 'High Availability Details' and displays the following information:

- Local Hostname : **csvm185181**
- Management IP Address : **10.90.185.198**
- Subnet Mask : **255.255.252.0**
- Peer Hostname : **csvm185182**
- Enable Peer HA :

At the bottom of the content area are two buttons: 'Delete' and 'SwitchOver'.

- b Click **Switchover** to switch to the Standby node.
Note: This operation may take between 20 and 40 minutes to complete.
- 8 Perform the ISO upgrade on the current primary-standby node.
 - a Select the secondary-standby node from the Videoscape Control Suite nodes.
 - b Select **2.5 ISO** from the **Images to Upgrade** list.
 - c Select **Upgrade Image** to initiate the image upgrade to the version 2.5 ISO release.

Note: This node will reboot during the process. Then, the ISO will be launched on this node.
- 9 Perform the HA switchover to make the current primary-standby node the primary-active node.
 - a Select **Operate --> High Availability --> Operation.**

The screenshot shows the Cisco Videoscape Conductor Management interface, identical to the previous one but with updated information. The main content area is titled 'High Availability Details' and displays the following information:

- Local Hostname : **csvm185181**
- Management IP Address : **10.90.185.198**
- Subnet Mask : **255.255.252.0**
- Peer Hostname : **csvm185182**
- Enable Peer HA :

At the bottom of the content area are two buttons: 'Delete' and 'SwitchOver'.

- b Click **Switchover** to switch to the Standby node.
Note: This operation may take between 20 and 40 minutes to complete.

Videoscape Control Suite 2.1 to 2.5 Upgrade

- 10 Upgrade the other Msginfra nodes one by one from the CMC.

The screenshot shows the Cisco Videoscape Control Suite Management interface. At the top, there's a navigation bar with tabs for Services, Operate, Configure, Administration, and Message Infrastructure. Below the navigation bar, the title "Image Upgrade" is displayed, followed by "Videoscape Control Suite Nodes". A table lists six nodes (1000-1005) with their status, IP addresses, and various system metrics. Node 1004 is selected, indicated by a checked checkbox. Below the table, a section titled "Software Images to install" shows a single entry: "UCSInstall_UCOS_2.5.0.0-15163.iso" (ISO type, version 2.5.0.0-15163, size 2115 MB, updated on April 15, 2013).

Node ...	State	Node Name	IP Address	Memory Usage ...	Disk Usage %	CPU Utilization %	RAM Size(KB)	Disk Size(KB)	SysUpTime	Platform \
<input type="checkbox"/> 1000	●	csvm18773	10.90.187.73	3.7%	6.6%	1.6%	989152	5269791	9Days 19H 18M 30S	2.1.1.0-1
<input type="checkbox"/> 1001	●	csvm18772	10.90.187.72	3.7%	6.3%	1.3%	978760	4953803	9Days 19H 18M 26S	2.1.1.0-1
<input type="checkbox"/> 1002	●	csvm18770	10.90.187.70	9.5%	6.1%	1.0%	2535048	4835524	9Days 19H 24M 54S	2.1.1.0-1
<input type="checkbox"/> 1003	●	csvm18790	10.90.187.90	3.7%	6.6%	1.5%	978012	5262211	9Days 19H 42M 21S	2.1.1.0-1
<input checked="" type="checkbox"/> 1004	●	csvm18771	10.90.187.71	19.9%	20.7%	2.2%	5287484	33273659	2H 43M 7S	2.1.1.0-1

Software Images to install

File Name	Image Type	Version	Size	Updated On
UCSInstall_UCOS_2.5.0.0-15163.iso	ISO	2.5.0.0-15163	2115 MB (2217318400 bytes)	April 15, 2013 11:03:49 AM EDT

Upgrade the Videoscape Control Suite Software

Use this procedure to upgrade a system, currently at version 2.1 or 2.5, to the same version, albeit one with a more current build.

Important: Always upgrade your database node first.

- 1 At the CMC main GUI, click **Operate** and then select **Software**.
- 2 Click **Download**. The Image Repository window opens.
- 3 From the Image Repository, select **Import**. The Import Images window opens.
- 4 Click **SFTP**. The window expands to show Collection Options.
- 5 Enter the following information:
 - **Server** – This is the IP address of the server which holds the image repository.
 - **User Name** – This is the user name associated with the server containing the image repository.
 - **User Password** – This is the password associated with the server containing the image repository.
 - **Directory** (full path) – This is the full directory path to the COP file.
 - **Image Name** – This is the actual name of the COP file you want to download.

Example: The window should look similar to the following example when you are finished.

The screenshot shows the 'Import Images' window with the 'Source' tab selected (radio button for 'SFTP' is checked). The 'Collection Options' section is expanded, displaying the following fields:

Server	10.90.187.251
User Name	ftpuser
User Password	*****
Directory	/home/ftpuser/Releases/TueE
Image Name	conductor-couchbase-2.0-0-0.cop

At the bottom right of the window are 'Submit' and 'Cancel' buttons.

- 6 Click **Submit**. A confirmation message appears.

Upgrade the Videoscape Control Suite Software

- 7 Click OK on the confirmation message.

Result: The **UCSInstall_UCOS_2.x.x.x-xxxxxx.iso** ISO image is now listed in the Image Repository.

Image Repository

<input type="checkbox"/>	File Name	Image Family	Image Type	Version	Size	Updated On
<input type="checkbox"/>	UCSInstall_UCOS_2.0.0.0-10240.iso	UCOS	ISO	2.0.0.0-10240	1905 MB (1997019136 bytes)	June 18, 2012 11:51:48 AM EDT
<input type="checkbox"/>	cisco.conductor-alertManager-2.0...	alertManager	COP	2.0-0-9	16.89 MB (17713134 bytes)	June 18, 2012 11:55:26 AM EDT
<input type="checkbox"/>	cisco.conductor-alertManager-2.0...	alertManager	TEMPLATE	2.0-0-9	0.0009575 MB (1004 bytes)	June 18, 2012 11:54:35 AM EDT
<input type="checkbox"/>	cisco.conductor-cdr-2.0.0.213.cop	cdr	COP	2.0.0.213	30.69 MB (32185321 bytes)	June 18, 2012 11:50:20 AM EDT
<input type="checkbox"/>	cisco.conductor-cdr-2.0.0.213.tm...	cdr	TEMPLATE	2.0.0.213	0.0006933 MB (727 bytes)	June 18, 2012 11:49:45 AM EDT
<input type="checkbox"/>	cisco.conductor-endpointManager-...	endpointManager	COP	2.0-0-13	13.61 MB (14269658 bytes)	June 18, 2012 11:57:55 AM EDT
<input type="checkbox"/>	cisco.conductor-endpointManager-...	endpointManager	TEMPLATE	2.0-0-13	0.001930 MB (2024 bytes)	June 18, 2012 11:57:25 AM EDT
<input type="checkbox"/>	cisco.conductor-wfe-2.0-0-0.cop	wfe	COP	2.0-0-0	191.4 MB (200688133 bytes)	June 18, 2012 11:52:51 AM EDT
<input type="checkbox"/>	cisco.conductor-wfe-2.0-0-0.tmpx...	wfe	TEMPLATE	2.0-0-0	0.0007076 MB (742 bytes)	June 18, 2012 11:53:43 AM EDT

- 8 On the CMC main GUI, click **Operate** and then select **Software**.

- 9 Click **Image Upgrade** and then select the node or nodes that you want to upgrade. The Software Images to Install section of the Image Upgrade window appears.

Image Upgrade

Conductor Nodes

Node ...	State	Node Name	IP Address	Memory Usage ...	Disk Usage %	CPU Utilization %	RAM Size(KB)	Disk Size(KB)	SysUpTime	Platform Version
<input checked="" type="checkbox"/>	1000	csmv185171	10.90.185.171	5.0%	9.8%	0.8%	1333740	7792857	8Days 20h 58m 15s	2.0.0.0-10136
<input type="checkbox"/>	1001	csmv185182	10.90.185.182	6.7%	10.3%	0.8%	3466286	8183469	19h 30m 195s	2.0.0.0-10240
<input checked="" type="checkbox"/>	1002	csmv185181	10.90.185.181	69.2%	41.6%	1.4%	35585832	32937965	8Days 23h 58m 435s	2.0.0.0-10136
<input type="checkbox"/>	1003	csmv185178	10.90.185.178	9.1%	9.7%	0.9%	2429558	7681589	19h 24m 235s	2.0.0.0-10240
<input type="checkbox"/>	1004	csmv185176	10.90.185.176	9.3%	9.7%	1.0%	2472026	7666833	19h 31m 555s	2.0.0.0-10240
<input type="checkbox"/>	1005	csmv185179	10.90.185.179	9.1%	9.7%	0.8%	2417960	7674541	19h 34m 335s	2.0.0.0-10240
<input type="checkbox"/>	1006	csmv185179	10.90.185.179	10.5%	9.7%	0.8%	2789844	7674493	19h 27m 65s	2.0.0.0-10240
<input type="checkbox"/>	1007	csmv185180	10.90.185.180	10.5%	9.7%	1.1%	2795776	7677269	19h 24m 35s	2.0.0.0-10240
<input type="checkbox"/>	1008	csmv185175	10.90.185.175	9.1%	9.2%	0.8%	2409976	7701789	19h 32m 15s	2.0.0.0-10240
<input checked="" type="checkbox"/>	1009	csmv185173	10.90.185.173	5.3%	9.8%	1.0%	1412388	7799145	8Days 22h 33m 105s	2.0.0.0-10136
<input type="checkbox"/>	1010	csmv185177	10.90.185.177	17.7%	14.2%	1.1%	4719404	11261201	19h 25m 55s	2.0.0.0-10240

Software Images to Install

Upgrade Node

File Name	Image Type	Version	Size	Updated On
UCSInstall_UCOS_2.0.0.0-10240.iso	ISO	2.0.0.0-10240	1905 MB (1997019136 bytes)	June 18, 2012 11:51:48 AM EDT

- 10 Select the image that you want to use for the upgrade and then click **Upgrade Node**. The upgrade begins.

Result: The system will show no indication that anything has occurred until after the upgrade has completed. Once the upgrade is complete, the **SysUpTime**, **Platform Version**, and **Message Infra Version** fields on the Nodes window change to reflect the successful upgrade.

Conductor Nodes										
Node ...	Status	Node Name	IP Address	Memory Usage ...	Disk Usage %	CPU Utilization %	RAM Size(KB)	Disk Size(KB)	SysUpTime	Platform Version
<input type="checkbox"/>	1000	csmv185171	10.90.185.171	8.2%	9.7%	0.6%	274532	7660933	0H 31m 245s	2.0.0.0-10240
<input type="checkbox"/>	1001	csmv185182	10.90.185.182	6.9%	10.3%	0.5%	2932468	8184921	20h 34m 395s	2.0.0.0-10240
<input checked="" type="checkbox"/>	1002	csmv185181	10.90.185.181	27.5%	39.0%	2.1%	14134388	30946905	0H 31m 155s	2.0.0.0-10240
<input type="checkbox"/>	1003	csmv185178	10.90.185.178	9.3%	9.7%	0.6%	2466988	7681557	20h 19m 435s	2.0.0.0-10240
<input type="checkbox"/>	1004	csmv185176	10.90.185.176	9.5%	9.7%	0.6%	2530820	7664941	20h 27m 355s	2.0.0.0-10240
<input type="checkbox"/>	1005	csmv185179	10.90.185.179	9.3%	9.7%	0.7%	2429720	7674536	20h 39m 535s	2.0.0.0-10240
<input type="checkbox"/>	1006	csmv185179	10.90.185.179	11.0%	9.7%	0.8%	2927794	7674865	20h 19m 265s	2.0.0.0-10240
<input type="checkbox"/>	1007	csmv185180	10.90.185.180	11.0%	9.7%	1.2%	2932216	7679277	20h 19m 235s	2.0.0.0-10240
<input type="checkbox"/>	1008	csmv185175	10.90.185.175	9.3%	9.7%	1.0%	2474028	7703473	20h 27m 215s	2.0.0.0-10240
<input type="checkbox"/>	1009	csmv185173	10.90.185.173	8.2%	9.7%	0.8%	2185344	7668097	0H 30m 435s	2.0.0.0-10240
<input type="checkbox"/>	1010	csmv185177	10.90.185.177	18.2%	14.2%	1.0%	4843604	11264073	20h 29m 255s	2.0.0.0-10240
<input type="checkbox"/>	1011	csmv185172	10.90.185.172	8.4%	9.7%	1.2%	2510948	7673257	20h 26m 425s	2.0.0.0-10240
<input type="checkbox"/>	1012	csmv185174	10.90.185.174	9.2%	9.7%	1.1%	2451188	7672289	20h 29h 45s	2.0.0.0-10240
<input type="checkbox"/>	1013	csmv185169	10.90.185.169	9.5%	9.7%	1.0%	2524908	7677085	20h 26m 395s	2.0.0.0-10240
<input type="checkbox"/>	1014	csmv185184	10.90.185.184	1.2%	5.7%	0.4%	1220432	9173274	19h 31m 545s	2.0.0.0-10136
<input type="checkbox"/>	1015	csmv185183	10.90.185.183	3.1%	5.3%	0.1%	3101392	8505461	20h 34m 495s	2.0.0.0-10240
<input type="checkbox"/>	1016	csmv185165	10.90.185.185	8.9%	17.3%	0.4%	4579332	13747845	20h 28m 505s	2.0.0.0-10240
<input type="checkbox"/>	1017	csmv185186	10.90.185.186	4.8%	9.5%	0.5%	2464172	7506129	20h 28m 255s	2.0.0.0-10240

Note: If you are upgrading the CMC node, it will not be accessible until the upgrade has completed. Once you can log in again, log in and confirm that the three parameters have changed.

7

Troubleshooting the Videoscape Control Suite

Introduction

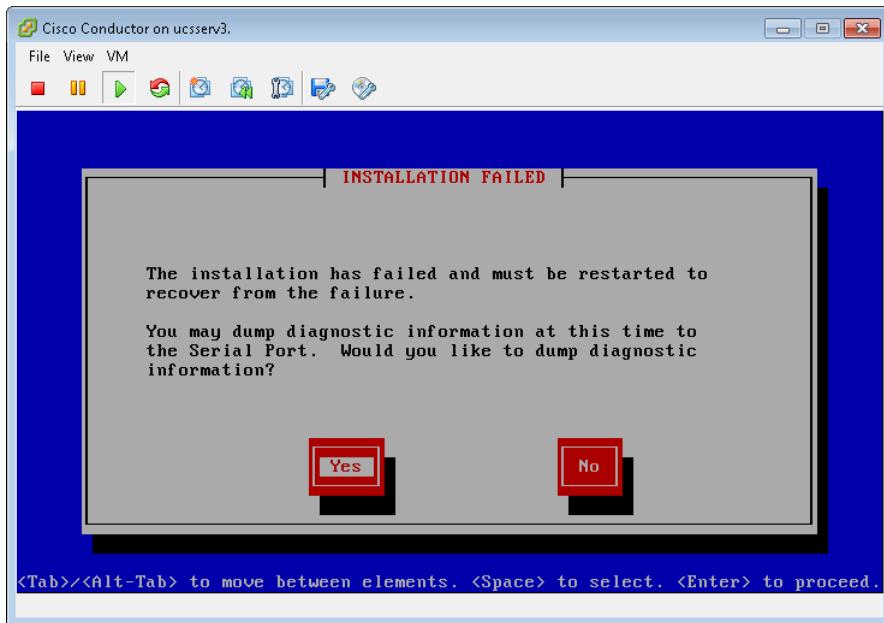
This chapter contains information that system operators might find useful when troubleshooting their Cisco Videoscape Control Suite installation.

In This Chapter

■ Recover From a Failed Installation of the ISO Image	88
■ Troubleshooting the Upgrade.....	90
■ Installation Log File	93
■ Miscellaneous Troubleshooting Tips	94

Recover From a Failed Installation of the ISO Image

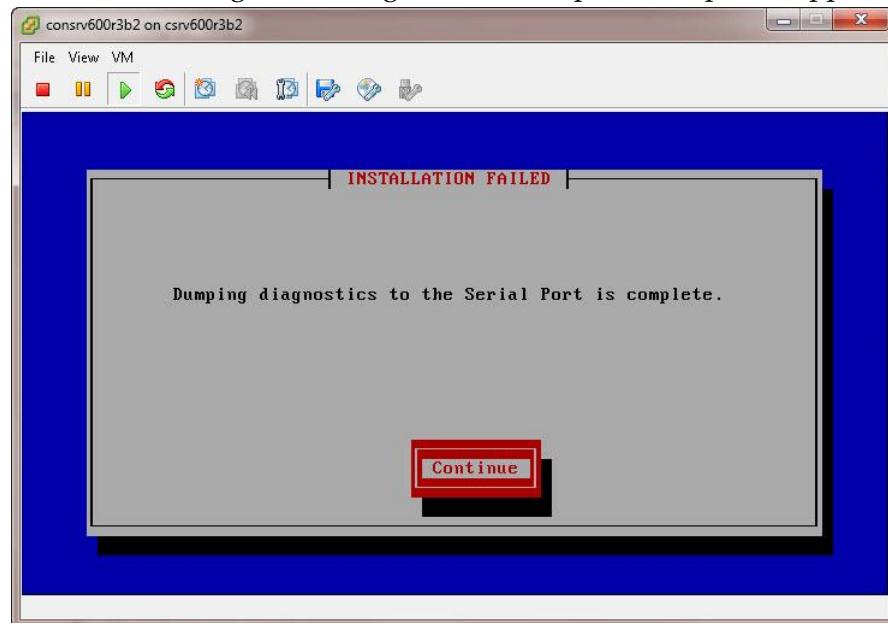
Occasionally, your installation of the ISO Image will fail. This usually occurs because of an issue with the DVD connection. Follow these instructions to recover.



- 1 Make sure **Yes** is selected and press **Enter** to produce a diagnostic information dump.

Note: This can take a few minutes to complete.

Result: A message indicating that the dump has completed appears.



Recover From a Failed Installation of the ISO Image

- 2 Press **Enter** to continue.
Result: The message **Restart install to recover from failure** appears.
- 3 In vCenter, right-click the virtual machine on which you are working, click **Power**, and then click **Shut Down Guest**. A confirmation message appears.
- 4 Click **Yes** on the confirmation message.
Note: A message appears that states that the remote device is disconnected.
- 5 Right-click the virtual machine and click **Delete from Disk**.
- 6 Go back to *Deploy the OVA File* (on page 31) and start over.

Troubleshooting the Upgrade

The following is information that might be useful if the upgrade from version 2.1 to 2.5 fails.

Note: The upgrade can be initiated from the CLI without all of the checks that are performed when using the CMC.

```
admin@csvm185216's password:  
Command Line Interface is starting up, please wait ...  
Welcome to the Platform Command Line Interface  
VMware Installation:  
  8 vCPU:           Intel(R) Xeon(R) CPU E5-2690 0 @ 2.90GHz  
  Disk 1: 80GB  
  Disk 2: 80GB  
  32768 Mbytes RAM  
  
admin:utils system upgrade initiate  
Warning: Do not close this window without first canceling the upgrade.  
Source:  
  1) Remote Filesystem via SFTP  
  2) Remote Filesystem via FTP  
  3) Local Upload Directory  
  q) quit  
Please select an option (1 - 3 or "q" ): 1  
Directory: /home/ftpuser/Releases/2013-04-30-05:01  
Server: 10.90.187.251  
User Name: ftpuser  
Password: *****  
Please enter SMTP Host Server (optional):  
Checking for valid upgrades. Please wait...  
Available options and upgrades in  
"10.90.187.251:/home/ftpuser/Releases/2013-04-30-05:01":  
  1) UCSInstall_UCOS_3.0.0.0-14950.iso  
  q) quit  
Please select an option (1 - 1 or "q" ): 1  
Accessing the file. Please wait...  
Downloaded 1985 MB.  
Checksumming the file...  
Validating the file...  
A system reboot is required when the upgrade process completes or is  
canceled. This will ensure services affected by the upgrade process are  
functioning properly.
```

```
Downloaded: UCSInstall_UCOS_3.0.0.0-14950.iso
File version: 3.0.0.0-14950
File checksum: f2:2a:b6:ea:08:95:3f:56:c4:2d:b1:4d:5c:ea:d7:ed

Automatically switch versions if the upgrade is successful (yes/no):
Automatically switch versions if the upgrade is successful (yes/no): yes

Start installation (yes/no): yes
The upgrade log is install_log_2013-04-30.11.59.24.log
Upgrading the system. Please wait...
04/30/2013 11:59:26 file_list.sh|Starting file_list.sh|<LVL::Info>
04/30/2013 11:59:26 file_list.sh|Parse argument
method=remote_sftp|<LVL::Debug>
04/30/2013 11:59:26 file_list.sh|Parse argument
source_dir=/home/ftpuser/Releases/2013-04-30-05:01|<LVL::Debug>
04/30/2013 11:59:26 file_list.sh|Parse argument
dest_file=/var/log/install/downloaded_versions|<LVL::Debug>
04/30/2013 11:59:26 file_list.sh|Parse argument
remote_host=10.90.187.251|<LVL::Debug>
04/30/2013 11:59:26 file_list.sh|Parse argument
user_name=ftpuser|<LVL::Debug>
04/30/2013 11:59:26 file_list.sh|is_upgrade_lock_available: Upgrade lock is
available.|<LVL::Debug>
04/30/2013 11:59:26 file_list.sh|is_upgrade_result_available: Result is not
available|<LVL::Debug>
04/30/2013 11:59:26 file_list.sh|acquire_upgrade_lock: Lock is free,
creating lock (pid: 19822)|<LVL::Debug>
04/30/2013 11:59:26 file_list.sh|Process remote SFTP request|<LVL::Info>
04/30/2013 11:59:26 file_list.sh|Calling SFTP command with metering
off|<LVL::Debug>
04/30/2013 11:59:26 file_list.sh|SFTP command complete (0)|<LVL::Debug>
04/30/2013 11:59:26 file_list.sh|List file (pre-filtered):|<LVL::Debug>
04/30/2013 11:59:26 file_list.sh|(CAPTURE) ClusterTool30.war|<LVL::Debug>
04/30/2013 11:59:26 file_list.sh|(CAPTURE)
Installers_Rel_bldlog.txt|<LVL::Debug>
04/30/2013 11:59:26 file_list.sh|(CAPTURE) UCSInstall_UCOS_3.0.0.0-
14950.iso|<LVL::Debug>
04/30/2013 11:59:26 file_list.sh|(CAPTURE) cisco.conductor-
DeviceProfileServices-1.5-0-1499.cop|<LVL::Debug>
04/30/2013 11:59:26 file_list.sh|(CAPTURE) cisco.conductor-
DeviceProfileServices-1.5-0-1499.tmp.xml|<LVL::Debug>
04/30/2013 11:59:26 file_list.sh|(CAPTURE) cisco.conductor-ECS-
CpeManagement-1.0-5-35.cop|<LVL::Debug>
```

Chapter 7 Troubleshooting the Videoscape Control Suite

```
04/30/2013 11:59:26 file_list.sh| (CAPTURE) cisco.conductor-ECS-
CpeManagement-1.0-5-35.tmp.xml|<LVL::Debug>

04/30/2013 11:59:26 file_list.sh| (CAPTURE) cisco.conductor-ECS-
DBAccessService-1.0-5-40.cop|<LVL::Debug>

04/30/2013 11:59:26 file_list.sh| (CAPTURE) cisco.conductor-ECS-
DBAccessService-1.0-5-40.tmp.xml|<LVL::Debug>

04/30/2013 11:59:26 file_list.sh| (CAPTURE) cisco.conductor-ECS-
LoadPIMSService-1.0-5-35.cop|<LVL::Debug>

04/30/2013 11:59:26 file_list.sh| (CAPTURE) cisco.conductor-ECS-
LoadPIMSService-1.0-5-35.tmp.xml|<LVL::Debug>

04/30/2013 11:59:26 file_list.sh| (CAPTURE) cisco.conductor-ECS-OAMService-
1.0-5-41.cop|<LVL::Debug>

04/30/2013 11:59:26 file_list.sh| (CAPTURE) cisco.conductor-ECS-OAMService-
1.0-5-41.tmp.xml|<LVL::Debug>

04/30/2013 11:59:26 file_list.sh| (CAPTURE) cisco.conductor-ECS-RPSService-
1.0-5-51.cop|<LVL::Debug>

04/30/2013 11:59:26 file_list.sh| (CAPTURE) cisco.conductor-ECS-RPSService-
1.0-5-51.tmp.xml|<LVL::Debug>

04/30/2013 11:59:26 file_list.sh| (CAPTURE) cisco.conductor-ECS-RPS_XSD-1.0-
5-35.cop|<LVL::Debug>

04/30/2013 11:59:26 file_list.sh| (CAPTURE) cisco.conductor-ECS-
RegisterService-1.0-5-48.cop|<LVL::Debug>

04/30/2013 11:59:26 file_list.sh| (CAPTURE) cisco.conductor-ECS-
RegisterService-1.0-5-48.tmp.xml|<LVL::Debug>
```

Installation Log File

From the command line interface (CLI), you can examine the installation log file to determine what caused an installation failure.

- 1 When you receive an XCP *Installation* error, type the following command and press **Enter** to log into the CLI as the *admin* user to examine the logs.

```
ssh admin@<hostname>
```

Result: The system prompts for the password of the admin user.

- 2 Type the password and press **Enter**.
- 3 At the prompt, type the following commands and press **Enter**:

- To list the installation log files:

```
file list activelog install
```

Sample output:

```
top-xcp-install.log  
dir count = 0, file count = 1
```

- To dump the install.log file:

```
file dump activelog install/top-xcp-install.log
```

Sample output:

```
answerfile.upgrade.default  
answerfile.upgrade.template  
answerfile.upgrade.template.oracle  
answerfile.upgrade.template.postgresql
```

- To view the install.log file:

```
file view activelog install/top-xcp-install.log
```

Sample contents:

```
answerfile.upgrade.default  
answerfile.upgrade.template  
answerfile.upgrade.template.oracle  
answerfile.upgrade.template.postgresql  
cleannode.sh
```

Miscellaneous Troubleshooting Tips

- When creating the floppy file, the file names you inject must be *cluster.xml* and *platformConfig.xml*. No customization of these file names are allowed.
- If the Videoscape Control Suite does not install as expected, examine the following log files:
 - /common/xcp-install/conductor_install.log – Log of python installation script, related to cluster.xml
 - /common/xcp-install/conductor_msinfra-installer.log – Log of Videoscape Control Suite msinfra installer
 - /common/xcp-install/failure.log – Only exists when a python installation script error occurs
 - /common/xcp-install/top-xcp-install.log – I/O redirection file
- XCP installation failure message:
 - The XCP installation failed because of:
Error, Invalid XML configuration file format!
Fatal error when parsing the config file, exit.
Please change the cluster.xml file and then press OK to retry.
Possible solution: Verify the cluster.xml file, and make all necessary changes. Save the changed file to the .flp file. Reconnect the floppy file and select **OK**.
 - The XCP installation failed because of:
Blank adminjid secret
Errors, when parsing zone section, config
Errors, when parsing cluster section, config
Fatal error when parsing the config file, exit.
Please change the cluster.xml file and then press OK to retry.
Possible solution:
 - 1) Disconnect the floppy. Edit the cluster file to add the admin jid entry:

```
<adminjid> admin@mgmt.conductor.cisco.com</adminjid>
<secret>pa$$w0rd</secret>
```
 - 2) Open the floppy with winimage, delete the current cluster file, inject the new cluster, and save the file. Connect the new floppy and select **OK**.

- The XCP installation failed because of:

Can't install msginfra with current configuration.

Please change the cluster.xml file and then press OK to retry.

Possible reasons for this error:

- You did not install a Postgres database node, or the platformConfig.xml file did not contain the **rtmbdb** entry to create the database node.
- The floppy image did not contain the default file names *cluster.xml* and/or *platformConfig.xml*.

Possible solution:

Verify the cluster.xml file and/or platformConfig.xml file and make all the necessary changes. Save the changed file to the .flp file. Reconnect the floppy file and select **OK**.

8

Customer Information

If You Have Questions

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Access your company's extranet site to view or order additional technical publications. For accessing instructions, contact the representative who handles your account. Check your extranet site often as the information is updated frequently.

A

The cluster.xml Files

Introduction

This appendix provides an overview of the initial deployment configuration of the Videoscape Control Suite product.

The Videoscape Control Suite uses a pre-configured file, cluster.xml, to enable initial automated deployment when installing the VSOS. This configuration file is a standard Extensible Markup Language (XML) file, which contains the configuration of the initial deployment of the whole cluster. Users can predefined such a file to set up full functional services for the deployment of VSOS.

In This Appendix

■ Overview of the Initial Deployment Configuration	100
■ Format of the Initial Deployment Configuration File.....	101
■ Cluster Concepts.....	102
■ Cluster File Examples.....	124

Overview of the Initial Deployment Configuration

The initial deployment configuration (IDC) file, cluster.xml, uses the following key concepts to set up a Videoscape Control Suite service:

- **Cluster** – A cluster is a group of servers or virtual servers that place multiple services and software components into nodes. All services and components together build an organized product.
- **Zone** – A zone is a group of servers or virtual servers that provide the same functionality or service within a cluster. A cluster has one or more zones which provide different functionalities. All servers within a zone have identical configuration. The load balance (or HA) is based on zone.
- **Node** – A node is a server or virtual server which combines one or more Videoscape Control Suite message infrastructure (infra) realms and corresponding components. A zone may have one or more nodes.
- **Defaultsvc** – A defaultsvc is a service configuration based on Videoscape Control Suite Msginfra. A node may have only one defaultsvc.
- **Realm** – A realm is a message infra installation of the Videoscape Control Suite service. Within a realm, there is one message infra core router (Jabberd) and one or more components connected to the router. A node may have one or more realms.
- **Component** – A component is a software process or a plug-in of the router that provides a specific service other than a routing service, such as XMPP Connection Manager (CM), Jabber Session Manager (JSM), etc. A realm may have one or more components.

Format of the Initial Deployment Configuration File

The format of the initial deployment configuration file should be similar to the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration version='xxxx'>
    <clusters>
        <cluster attribute_1='xxx'... attribute_n='xxx' >
            <zones>
                <zone attribute_1='xxx'... attribute_n='xxx' >
                    <adminjid>
                        <jid>admin@sample.com</jid>
                        <secret>xxx</secret>
                    </adminjid>
                    <nodes>
                        <node attribute_1='xxx'... attribute_n='xxx' >
                            <defaultsvc attribute_1='xxx'... attribute_n='xxx' />
                            <realms>
                                <realm attribute_1='xxx'... attribute_n='xxx' >
                                    <component attribute_1='xxx'... attribute_n='xxx' >
                                        <sub-key-1>value1</sub-key-1>
                                        <!---->
                                    </component>
                                    <component attribute_1='xxx'... attribute_n='xxx' />
                                </realm>
                            </realms>
                        </node>
                    </nodes>
                </zone>
            </zones>
        </cluster>
    </clusters>
    <datasource>
        <data attribute_1='xxx'... attribute_n='xxx' />
    </datasource>
</configuration>
```

Cluster Concepts

Data Types

Some of the values used in the cluster.xml file are standardized according to the following requirements.

- **USERID** – Must be a combination of numbers, alphabetical characters, '_', and '-'. Must be from 4 to 32 characters in length.
- **PASSWORD** – Must be a combination of numbers, alphabetical characters, and some special characters (1-9, a-z, A-Z, ~!@#\$%^* _+=[]{}?.?). Must be from 4 to 32 characters in length.
- **CLUSTERID** – Must be a combination of numbers and alphabetical characters. Must be from 4 to 32 characters in length.
- **COMPONENTID** – Must be a combination of numbers, alphabetical characters, '_', and '-'. Must be from 4 to 32 characters in length, and all lower-case.
- **REALMID** – Must be a combination of numbers, alphabetical characters, and '-'. Must be from 4 to 32 characters in length.
Note: The REALMID data type must not contain the following values: "cm-", "tc-", "jsm-", and "sasl-". In addition, the REALMID data type must not begin or end with the character "-".
- **HOSTNAME** – Must be a combination of numbers, alphabetical characters, '_', and '-', and a period. The HOSTNAME must be from 1 to 255 characters long, and each part must be divided by a period. No individual part can be longer than 63 characters, and must not begin or end with a "-".

Configuration

The Configuration section is the root element for the whole cluster.xml file. It contains only cluster and datasource sub-elements. The attribute “version” should match the Videoscape Control Suite Msginfra image version.

Attributes	Meaning	Values	Optional?
version	The cluster.xml file version. The cluster.xml file checks the version to detect backward-compatibility.	A number matching the Videoscape Control Suite Msginfra image version	Optional

Data Source

The datasource section defines the database configuration information. The datasource may be the server where the Msginfra and the PostgreSQL are installed, or it may be an external database. This datasource must be installed before any realms that rely on this datasource are installed.

If the datasource is part of a cluster, a database zone should be installed with a minimum Msginfra.

Attributes	Definition	Values	Optional?
name	The name of the datasource	A value of the USERID type	Must have
dbtype	The database type	A valid name. Must be one of the following values: <ul style="list-style-type: none">■ postgresql-odbc■ oracle-oci The default is "postgresql-odbc".	Optional
msginfradb	The name of the PostgreSQL database used for the message infra service. If no such database exists, the installer must create a new one	A value of the USERID type. All characters must be lower-case. The default is "msginfra".	Must have
conductordb	The name of the PostgreSQL database used for the Videoscape Control Suite platform service. If no such database exists, the installer must create a new one	A value of the USERID type. All characters must be lower-case. The default is "platform".	Must have
dbsvrsuperps	The password of the "root" account at the database server	A value of the PASSWORD type. Use the XML escape, if necessary.	Must have
dbuser	The name of the account that owns the two databases within the PostgreSQL server. If no such database exists, the installer must create a new one	A value of the USERID type. All characters must be lower-case.	Must have
dbsecret	The password of the "dbuser" account	A value of the PASSWORD type. Use the XML escape, if necessary.	Must have
ip	The database server IP address	A valid IP address	Must have
port	The database server port	A valid port number	Must have

Appendix A

The cluster.xml Files

Attributes	Definition	Values	Optional?
msginfrauser	The username of msginfra db instance	A value of the USERID type. All characters should be upper-case.	Must have when dbtype is set to "oracle-oci"
msginfrauser secret	The password of the msginfra db instance	A value of the PASSWORD type	Must have when dbtype is set to "oracle-oci"
platformuser	The username of the platform db instance	A value of the USERID type. All characters should be upper-case.	Must have when dbtype is set to "oracle-oci"
platformuser secret	The password of the platform db instance	A value of the PASSWORD type.	Must have when dbtype is set to "oracle-oci"
service	The service name of the external oracle database	A valid name of the HOSTNAME type	Must have when dbtype is set to "oracle-oci"

Cluster

The MSGINFRA cluster is the only kind of cluster that can be defined in this release. This cluster provides the message infrastructure and add-on services.

Note: The DATABASE cluster, with which some operators may be familiar, is now replaced with a *database tag*.

The MSGINFRA cluster has the following attributes:

Attribute	Definition	Values	Optional?
type	The type of cluster	Must be MSGINFRA (upper-case, only)	Must have
clusterid	The name of the MSGINFRA cluster	A value of the CLUSTERID type	Must have

Attribute	Definition	Values	Optional?
clustersecret	The password used for router/component authentication within the MSGINFRA cluster. All components use the same authentication password.	A value of the PASSWORD type. Use the XML escape, if necessary.	Must have
admin	The name that the Jabber XCP administrator will use to log onto the Web Controller	A value of the USERID type. Must have All characters must be lower-case.	
adminsecret	The password used for admin authentication within the MSGINFRA cluster	A value of the PASSWORD type. Use the XML escape, if necessary.	Must have

Zone

A zone has one or more nodes in which one or more realms are installed with the same configuration. The zone key has the following attributes:

Attribute	Description	Value	Optional?
name	The name of the zone	A value of the USERID type	Must have
datasource	The name of the datasource defined in the DATASOURCE entry. This datasource is shared by all the realms within the same zone.	A value of the USERID type	Must have

- A Zone has a "adminjid" stanza, which defines the administration account for all components within the zone. The key of "adminjid" has one or more sub-keys, "jid", whose value is a valid bare JID, and must be named similarly to "555@example.com".
- A Zone has one or more node sub-keys, which are defined in the *Node* (on page 106) section.

Node

A node is a virtual machine server with a VSOS running on it. The node has the following attributes:

Attribute	Definition	Value	Optional?
name	The node name of the server that installs the message infra realms	A valid node name of the server. This name must match the target server's configuration. All characters must be lowercase.	Must have
type	The type of node	Must be one of the following values (uppercase only): <ul style="list-style-type: none"> ■ MGMT ■ SERVICE 	Must have
hrestartperiod	When the realm (either the router or some component) fails, the Node Controller (NC) will try to restart the realm for several times within "hrestartperiod" seconds. If it still fails, the NC will fail this realm.	Must be an integer (represents seconds): [120,2400] Default: 1200	Optional
hrestartcount	When the realm (either the router or some component) fails, the NC will try to restart the realm for "hrestartcount" times within "hrestartperiod" seconds. If it still fails, the NC will fail this realm.	Must be an integer: [1,40] Default: 10	Optional
hahlthckintrlv	When HA (defined with router type) is enabled, the NC will check the service (JSM, router) every "hahlthckintrlv" seconds. This parameter is rounded up to an integer.	Must be an integer (represents 0.1 seconds): [30,1000] Default: 30	Optional

Attribute	Definition	Value	Optional?
hahlthchkcnt	When HA (defined with router type) is enabled, the NC believes the service (JSM) is down if “hahlthchkcnt” successive health checks fail. Then, the NC will restart the service.	Must be an integer: [3,10] Default: 3	Optional
hahlthchkigncnt	When the realm starts, the NC waits for “hahlthchkigncnt*hahlthinter val” seconds to start the health check in order to avoid a component-presence message burst.	Must be an integer: [0,10] Default: 3	Optional
cfgchkintrvl	When the NC starts, it starts a single thread that monitors the component configuration for each realm. When the component configuration is changed, the NC detects the change at most cfgchkintrvl intervals. Note: The cfgchkintrvl field is mainly used in polling the Jabber configuration.	Must be an integer: [5,15] Default: 10	Optional
pref	When the management type realm starts, the Videoscape Control Suite platform regards the pref attribute as a PRIMARY/SECONDARY node to set up.	Must be of the following value: 1. SECONDARY	Optional

A node has one or more realm keys, defined in the *Realm* (on page 108) section.

Defaultsvc

A defaultsvc is a service configuration based upon the Videoscape Control Suite Msginfra. A node may have only one defaultsvc. The defaultsvc key has the following attributes.

Attribute	Definition	Value	Optional?
cmip	The service based upon the Videoscape Control Suite Msginfra connects to the system with this IP address.	A valid IP address of a node with the Connection Manager	Must have

Appendix A

The cluster.xml Files

Attribute	Definition	Value	Optional?
cport	The service based upon the Videoscape Control Suite Msginfra connects to the system on this port.	A valid port of a node with the Connection Manager	Must have
jsmdomain	The service based upon the Videoscape Control Suite Msginfra connects to the system with this domain name.	A valid hostname	Must have
jsmid	The service based upon the Videoscape Control Suite Msginfra connects to the system with this jsm component ID.	A valid hostname	Must have

Realm

A realm is a combination of a router and one or more specific components. The realm key has the following attributes.

Attribute	Meaning	Value	Optional?
realmid	The ID of the realm, which should be unique within the whole cluster.	A value of the REALMID type. All characters must be lowercase.	Must have
ip	The IP address to which the router listens.	A valid IP address of the node	Must have
ipmask	The network mask of the router IP address	A valid IP mask of the router. If the router IP address is not equal to the admin IP address, the value is mandatory.	Optional
port	The port to which the router listens	A valid port of the node	Must have
adminip	The IP address to which the Web Controller or other management components listen.	A valid IP address of the node. If not specified, the default value is the IP address of the node.	Optional

Attribute	Meaning	Value	Optional?
adminport	The port to which the Web Controller listens.	A valid port of the node	Must have
mdns	Enable or disable the MultiCast DNS feature. <ul style="list-style-type: none"> ■ If enabled, the realm/routers within the same cluster will be connected with full mesh topology. ■ If disabled, the connections between realms and routers must be manually configured. 	Must be one of the following options: 1 – on 2 – off	Must have
type	The type of router	Must be one of the following values (upper-case, only): 1 – BOOTSTRAP 2 – HAENABLED 3 – HADISABLED Important: In a single node configuration, the router must be of the BOOTSTRAP type.	Must have

A realm has one or more component sub-keys, defined in the *Component* (on page 110) section.

Component

A component provides a specific service, such as the XMPP connection, Jabber Session management, or Management Console.

Attribute	Description	Value	Optional?
type	The type of service/component	Must be one of the following: 1 – CM 2 – CMW 3 – JSM 4 – PS 5 – SDNS 6 – MC 7 – MCC 8 – SASL 9 – SVM 10 – SMM 11 – SVCVIEWER 12 – HTTPGW 13 – R2R The value must be upper-case.	Must have: All
subtype	If the type is SDNS, the subtype is the type of component behind the SDNS.	Must be one of the following: 1 – JSM 2 – PS 3 – SVM 4 – SASL 5 – CD 6 – OTHERS The values must be upper-case.	Must have: SDNS Optional: None No need: CM, CMW, JSM, PS, MC, MCC, SASL, SVM, SMM, SVCVIEWER, HTTPGW, R2R
name	The ID of the component	A value of the COMPONENTID type. All characters must be lower-case. Cannot be the same as the router realmid.	Must have: All

Attribute	Description	Value	Optional?
svcip	The IP address to which the service listens. If specified, a virtual IP address is configured.	A valid IP address. If not specified, the default value is the IP address of the router. When CM/CMW is configured with this attribute, if the value is not equal to either the "adminip" or "ip" value within local node, a new eth1 is created with this attribute value.	Must have: None Optional: CM, CMW, MCC, SVCVIEWER, HTTPGW No need: JSM, SDNS, PS, MC, SASL, SVM, SMM, R2R
svcipmask	The IP mask for the service IP address	A valid IP mask address. If not specified, the default value is the IP mask of the node.	Must have: None Optional: CM, CMW No need: JSM, PS, SDNS, MC, MCC, SASL, SVM, SMM, SVCVIEWER, HTTPGW, R2R
ip	The IP address to which the service listens	A valid IP address	Must have: R2R Optional: None No need: CM, CMW, JSM, SDNS, PS, MC, MCC, SASL, SVM, SMM, SVCVIEWER, HTTPGW
port	The port to which the service listens	A valid port. If not specified, the default value is 5222 (CM), 5280 (CMW), 8100 (HTTPGW), 8200 (MCC), or 8300 (SVCVIEWER).	Must have: R2R Optional: CM, CMW, MCC, SVCVIEWER, HTTPGW No need: JSM, SDNS, PS, MCC, SASL, SVM, SMM
compport	The port to which the compatible service listens. This is only valid for the CM service. If specified, an old CM SSL service is created that listens to this port.	A valid port. If not specified, the compatible port-related XMPP director is removed.	Must have: None Optional: CM No need: CMW, JSM, PS, SDNS, MC, MCC, SASL, SVM, SMM, SVCVIEWER, HTTPGW, R2R

Appendix A

The cluster.xml Files

Attribute	Description	Value	Optional?
hostname	A hostname that addresses the service within the XMPP addressing space	A valid hostname Important: The string <i>pubsub.service</i> is reserved for internal trap transmission. User components MUST not use this string.	Must have: SDNS(JSM, PS,SVM, OTHERS), SMM, MC, MCC Optional: JSM, PS, SDNS(SASL, CD), SVM No need: CM, CMW, SASL, SVCVIEWER, HTTPGW, R2R
cmip	The Connection Manager IP address to which the MCC connects	A valid IP address. The value is the service IP address of the Connection Manager on the Management node.	Must have: MCC, HTTPGW Optional: None No need: CM, CMW, JSM, PS, SDNS, MC, SASL, SVM, SMM, SVCVIEWER, R2R
cmport	The Connection Manager port to which the MCC connects	A valid port. The value is the service port of CM on the Management node.	Must have: MCC, HTTPGW Optional: None No need: CM, CMW, JSM, PS, SDNS, MC, SASL, SVM, SMM, SVCVIEWER, R2R
snmpport	The SNMP port to which the trap is sent	A valid port. If not specified, the default value is 11162.	Must have: None Optional: MCC No need: CM, CMW, JSM, PS, SDNS, MC, SASL, SVM, SMM, SVCVIEWER, HTTPGW, R2R
maxsession	The maximum session number for a single JID	A valid number, [1,100]. The default value is 10.	Must have: None Optional: JSM No need: CM, CMW, PS, SDNS, MC, MCC, SASL, SVM, SMM, SVCVIEWER, HTTPGW, R2R

Attribute	Description	Value	Optional?
bcc	The component hostname to which the JSM sends the client presence	A valid hostname. The value is the component from which the client presence is obtained from the JSM type.	Must have: None Optional: JSM No need: CM, CMW, PS, SDNS, MC, MCC, SASL, SVM, SMM, SVCVIEWER, HTTPGW, R2R
offline	The offline message toggle. JSM can send offline messages according to the value	A valid hostname. Must be one of the following values: 1 – 0 2 – 1	Must have: None Optional: JSM No need: CM, CMW, PS, SDNS, MC, MCC, SASL, SVM, SMM, SVCVIEWER, HTTPGW, R2R
svmid	The SVM with which the SMM/SVCVIEWER works	A valid hostname. The value is the hostname of the SVM component.	Must have: SMM, SVCVIEWER Optional: None No need: CM, CMW, JSM, PS, SDNS, MC, MCC, SASL, SMM, HTTPGW, R2R
algo	The algorithm that the JSM subtype SDNS component uses	A valid name. The value is hard-coded to "db" in the Videoscape Control Suite for the SDNS database mapping algorithm.	Must have: None Optional: SDNS(JSM) No need: CM, CMW, JSM, PS, SDNS(PS, SVM, SASL, CD, OTHERS), MC, MCC, SASL, SVM, SMM, SVCVIEWER, HTTPGW, R2R
secret	The password of a peer router with an R2R connection	A value of the PASSWORD type	Must have: R2R Optional: None No need: CM, CMW, PS, JSM, SDNS, MC, MCC, SASL, SVM, SMM, SVCVIEWER, HTTPGW

Appendix A

The cluster.xml Files

Attribute	Description	Value	Optional?
isforsvc	Service related JSM flag	A valid value. Must be the one of the following: <ul style="list-style-type: none">■ 0■ 1 The default value is 0.	Must have: None Optional: JSM, SDNS No need: CM, CMW, PS, MC, MCC, SASL, SVM, SMM, SVCVIEWER, HTTPGW, R2R
eb	The component ID to which event brokers are redirected	A valid name	Must have: None Optional: JSM No need: CM, CMW, PS, SDNS, MC, MCC, SASL, SVM, SMM, SVCVIEWER, HTTPGW, R2R
msg	The toggle for enabling or disabling the mod_msg, which broadcasts messages to the same bare JID	A valid value. Must be the one of the following: <ul style="list-style-type: none">■ 0■ 1 The default value is 0.	Must have: None Optional: JSM No need: CM, CMW, PS, SDNS, MC, MCC, SASL, SVM, SMM, SVCVIEWER, HTTPGW, R2R
rosternotifyurl	The URL to which roster provisions send notifications	A valid URL	Must have: None Optional: JSM No need: CM, CMW, PS, SDNS, MC, MCC, SASL, SVM, SMM, SVCVIEWER, HTTPGW, R2R
svcip6	The IPv6 address to which the service listens. If specified, a virtual IP is configured.	A valid IPv6 address. A new eth1 is created with this attribute value.	Must have: None Optional: CM, CMW No need: JSM, PS, SDNS, MC, MCC, SASL, SVM, SMM, SVCVIEWER, HTTPGW, R2R

Attribute	Description	Value	Optional?
svcip6prefixlen	The IP prefix length for the service IPv6 address	A valid IP prefix length	Must have: None Optional: CM, CMW No need: JSM, PS, SDNS, MC, MCC, SASL, SVM, SMM, SVCVIEWER, HTTPGW, R2R
port6	The port to which the CM with an IPv6 address listens	A valid port. If not specified, the default value is 5222 (CM) or 5280 (CMW/BOSH).	Must have: None Optional: CM, CMW No need: JSM, PS, SDNS, MC, MCC, SASL, SVM, SMM, SVCVIEWER, HTTPGW, R2R
compport6	The port to which the compatible service on CM, with an IPv6 address listens. If specified, an old CM SSL service will be created and will listen to this port.	A valid port. If not specified, the default value is 5223 (CM).	Must have: None Optional: CM No need: JSM, PS, SDNS, MC, MCC, SASL, SVM, SMM, SVCVIEWER, HTTPGW, R2R
jsmdomain	The domain name that the HTTPGW component needs to create a jid	A valid hostname	Must have: HTTPGW Optional: None No need: CM, CMW, JSM, PS, SDNS, MC, MCC, SASL, SVM, SMM, SVCVIEWER, R2R
jsmid	The JSM component id to which HTTPGW should be bound	A valid name. All characters must be lower-case	Must have: HTTPGW Optional: None No need: CM, CMW, JSM, PS, SDNS, MC, MCC, SASL, SVM, SMM, SVCVIEWER, R2R

Appendix A

The cluster.xml Files

Attribute	Description	Value	Optional?
ungnotify	The UNG notification toggle. JSM sends an offline pubsub message to the UNG service instance.	Must be one of the following valid values: 1. 0 2. 1 Default value is 0.	Must have: none Optional: JSM No need: CM, CMW, PS, SDNS, MC, MCC, SASL, SVM, SMM, SVCVIEWER, HTTPGW, R2R
s2s	The S2S configuration toggle for the CM component	Must be one of the following valid values: 1. 0 2. 1 Default value is 0.	Must have: none Optional: CM No need: CMW, JSM, PS, SDNS, MC, MCC, SASL, SVM, SMM, SVCVIEWER, HTTPGW, R2R

The service type of the component is described in the following table:

Service type	Service Description
CM	The plain XMPP connection manager
CMW	The BOSH connection manager
JSM	Jabber Session Manager
PS	Pubsub service Note: This service is reserved by the internal trap notification service.
SASL	SASL service
SDNS	Single Domain Name Service for JSM, PS, SASL, SVM, CD and OTHERS subtype
MC	Management Core service. This service type is the only service type allowed on a bootstrap router on the management node.
MCC	Management Console Component. This service type is the only service type allowed on a bootstrap router on the management node.
SMM	Service Mapping Manager
SVM	Service Virtualization Manager
SVCVIEWER	Service Viewer
HTTPGW	HTTP Gateway
R2R	Router-to-Router Connection

CM Component

A fully-formatted CM component configuration looks similar to this:

```
<component type="CM" name="cm-1" isforsvc="0" s2s="0" svcip="172.17.3.105"
svcipmask="255.255.0.0" port="5222" compport="5223"
svcip6="2001:da8:208::9500" svcip6prefixlen="64" port6="5222"
compport6="5223"/>
```

The CM component sets up listening sockets on ("svcip":"port"), ("svcip":"compport"), ("svcip6":"port6"), and ("svcip6":"compport6").

- If the "svcip" attribute is not explicitly specified, the "svcip" value is automatically bound to the local router IP address.
- If the "svcip" attribute is explicitly specified and the value is not equal to either the local router admin IP address or the local router IP address, a new eth1 interface is created per the "svcip" and "svcipmask" values.
- If the "svcip6" attribute is explicitly specified, a new eth1 interface is created per the "svcip6" and "svcip6prefixlen" values.
- Users can choose to bind the CM component only to the IPv4 address or IPv6 addresses.

```
<component type="CM" name="cm-1" svcip="172.17.3.105"
svcipmask="255.255.0.0" port="5222" compport="5223" />
<component type="CM" name="cm-1" svcip6="2001:da8:208::9500"
svcip6prefixlen="64" port6="5222" compport6="5223"/>
```

- Users can configure the CM component with minimum attributes, which automatically bind to (local router ip:5222).

```
<component type="CM" name="cm-1" />
```

Per CM component usage, the CM component can be divided into two logical types:

- **Client CM**
- **Service CM**

The *Client CM* deals with the client-facing session. The typical IPv4 Client CM component configuration looks like this:

```
<component type="CM" name="cm-1" isforsvc="0" svcip="172.17.3.105"
svcipmask="255.255.0.0" port="5222" />
```

- The "isforsvc" attribute is set to "0" by default. The Client CM component can be configured implicitly.

The Service CM deals with the service instance session. The typical IPv4 Service CM component configuration looks like this:

```
<component type="CM" name="cm-1" isforsvc="1" svcip="172.17.3.105"
svcipmask="255.255.0.0" port="5222" />
```

Appendix A

The cluster.xml Files

- The “isforsvc” attribute is set to “0” by default. The Service CM component should be configured explicitly with value “1”.

The CM component can be configured with “s2s” to enable the S2S feature. The “svcip” and “port” are configured with the local router IPv4 address (5269 by default).

```
<component type="CM" name="cm-1" s2s="1" />
```

CMW Component

A fully-formatted CMW component configuration looks similar to this:

```
<component type="CMW" name="cmw-1" svcip="172.17.3.105"
  svcipmask="255.255.0.0" port="5280" svcip6="2001:da8:208::9500"
  svcip6prefixlen="64" port6="5280" />
```

The CMW component would set up listening sockets on (“svcip”：“port”) and (“svcip6”：“port6”).

- If the “svcip” attribute is not explicitly specified, the “svcip” value is automatically bound to the local router IP address.
- If the “svcip” attribute is explicitly specified and the value is not equal to the local router admin IP or the local router IP, a new eth1 interface is created per “svcip” and “svcipmask” values.
- If the “svcip6” attribute is explicitly specified, a new eth1 interface is created per “svcip6” and “svcip6prefixlen” values.
- Users could choose to bind the CMW component only to the IPv4 address or the IPv6 address

```
<component type="CMW" name="cmw-1" svcip="172.17.3.105"
  svcipmask="255.255.0.0" port="5280" />
<component type="CMW" name="cmw-1" svcip6="2001:da8:208::9500"
  svcip6prefixlen="64" port6="5280" />
```

- Users could configure the CMW component with minimal attributes, which are automatically bound to (local router ip:5280).

```
<component type="CMW" name="cmw-1" />
```

The CMW component can be divided into two logical types:

- Client CMW
- Service CMW

The Client CMW deals with the client-facing session. The typical IPv4 Client CMW component configuration should look like this:

```
<component type="CMW" name="cmw-1" isforsvc="0" svcip="172.17.3.105"
svcipmask="255.255.0.0" port="5280" />
```

- The “isforsvc” attribute is set to “0” by default. The Client CMW component can be configured implicitly.

The Service CMW deals with the service instance session. The typical IPv4 Service CMW component configuration should look like this:

```
<component type="CMW" name="cmw-1" isforsvc="1" svcip="172.17.3.105"
svcipmask="255.255.0.0" port="5280" />
```

- The “isforsvc” attribute is set to “0” by default. The Service CMW component should be configured explicitly with value “1”.

JSM Component

A fully-formatted JSM component configuration looks similar to this:

```
<component type="JSM" name="jsm-1" hostname="cisco.conductor.com"
isforsvc="1" msg="1" offline="0" bcc="svm.svc.conductor.com" eb="sdns-cd-
1.router-vm-debug-2" rosternotifyurl="http://www.cisco.com/notify" />
```

Per JSM component usage, the JSM component could be divided into three logical types,

- Client JSM
- Service JSM
- Management JSM

The Client JSM deals with the plain client session. The typical Client JSM component configuration should look like this:

```
<component type="JSM" name="jsm-1" hostname="cisco.conductor.com" msg="1"
eb="sdns-cd-1.router-vm-debug-2"
rosternotifyurl="http://www.cisco.com/notify" />
```

- The “isforsvc” attribute is set to “0” by default; the Client JSM component can be configured implicitly.
- The “msg” attribute is set to “0” by default; the Client JSM should be configured explicitly with value “1” to be enabled.
- The “offline” attribute is set to “1” by default; the Client JSM could be configured implicitly.
- The “eb”, “rosternotifyurl” attribute for the Client JSM should be explicitly configured to implement Roster Provision.

Appendix A

The cluster.xml Files

The Service JSM deals with the service instance session. The typical Service JSM component configuration should look like this:

```
<component type="JSM" name="jsm-1" hostname="cisco.conductor.com"  
isforsvc="1" offline="0" bcc="svm.svc.conductor.com" />
```

- The “isforsvc” attribute is set to “0” by default; the Service JSM component should be configured explicitly with the value “1”.
- The “msg” attribute is set to “0” by default; the Service JSM could be configured implicitly to be disabled.
- The “offline” attribute is set to “1” by default; the Service JSM should be configured explicitly with the value “0” to disable offline messages.
- The “bcc” attribute for Service JSM should be explicitly configured to implement the Service Directory.

The Management JSM deals with the management client session. The typical Management JSM component configuration should look like this:

```
<component type="JSM" name="jsm-1" hostname="mgmt.cisco.conductor.com" />
```

- All optional attributes could be configured implicitly to be set to their default values.

PS Component

A fully-formatted PS component configuration should look like this. The PS component in the management node should be configured with a fixed hostname “pubsub.service” for internal platform usage, and the PS components on non-management nodes must not be configured with a hostname of “pubsub.service”.

```
<component hostname="ps.conductor" name="pubsub-1" type="PS"/>
```

SASL Component

A fully-formatted SASL component configuration should look like this:

```
<component name="sasl-1" type="SASL"/>
```

SDNS Component

A SDNS service is defined as a proxy of other components with “subtype”. It has one or more sub-components, which are defined by “compid”. If the SDNS service is defined, all sub-components should ignore the “hostname” attribute configuration. The SDNS only owns the following listed subtypes:

- JSM
- PS
- SASL
- SVM

- CD
- OTHERS

The SDNS with the Service JSM-subtype should also be configured explicitly with a value of "1". Others could be configured implicitly.

```
<component type='SDNS' subtype='JSM' name='sdns-jsm-1' isforsvc='1'
hostname='conductor.cisco.com' >
    <compid>jsm-1.jsmzone001</compid>
    <compid>jsm-1.jsmzone002</compid>
</component>
```

A CD-subtype/SASL-subtype SDNS component could be configured even without the "hostname" attribute.

```
<component name="sdns-cd-1" subtype="CD" type="SDNS">
    <compid>cd-1.router-vm-debug-2</compid>
</component>
```

A Service JSM-subtype SDNS component should be configured with the "algo" attribute set to "db" to enable the db-mapping algorithm for Service Directory. The <compid> must only contain the one and only child <compid> tag.

```
<component type='SDNS' subtype='JSM' algo='db' name='sdns-jsm-1'
hostname='conductor.cisco.com' >
    <compid>jsm-1.jsmzone001</compid>
</component>
```

MC Component

A fully-formatted MC component configuration should look like this:

```
<component type='MC' name='mc-1' hostname='mc.cisco.conductor.com' />
```

The MC component should only be deployed on management type nodes, and, at most, on a single instance.

MCC Component

A fully-formatted MCC component configuration should look like this:

```
<component type='MCC' name='mcc-1' hostname='mcc.cisco.conductor.com' />
```

The MCC component should only be deployed on management type nodes, and, at most, on a single instance.

SMM Component

A fully-formatted SMM component configuration should look like this. It should be deployed along with the Client/Serivice JSM.

```
<component type="SMM" name="smm-1" svmid="svm.svc.conductor.com"  
hostname="smm.svc.conductor.com" />
```

SVM Component

A fully-formatted SVM component configuration should look like this:

```
<component type="SVM" name="svm-1" hostname="svm.svc.conductor.com" />
```

SVCVIEWER Component

A fully-formatted SVCVIEWER component configuration should look like this:

```
<component type="SVCVIEWER" name="svm-1"  
hostname="svcviewer.svc.conductor.com" svmid="svm.svc.conductor.com" />
```

HTTPGW Component

A fully-formatted HTTPGW component configuration should look like this:

```
<component type="HTTPGW" name="httpgw-1" cmip="192.168.2.18" cmpport="5222"  
jsmdomain="svc.conductor.com" jsmid="jsm-1.rtr-svc" />
```

A HTTPGW component behaves as a plain client to connect to the Conductor Msginfra and to provide information to whomever uses the HTTP interface.

- The “cmip” attribute should be configured with the Service CM IPaddress.
- The “cmpport” attribute should be configured with the Service CM port.
- The “jsmdomain” attribute should be configured with the Service JSM hostname or Service JSM-subtype SDNS hostname.
- The “jsmid” attribute should be configured with the Service JSM component ID.

R2R Component

A fully-formatted R2R component configuration should look like this:

```
<component type="R2R" name="jabberd-port-1" ip="192.168.1.1" port="7400"  
secret="cisco123"/>
```

A R2R component could set up a direct connection with a peer router.

- The “ip” attribute should be configured with the peer router IP address.
- The “port” attribute should be configured with the peer router master accept port.
- The “secret” attribute should be configured with the peer router password for connection setup.

Cluster File Examples

Sample cluster.R2-5.xml File (Explained)

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <clusters>
        <!-- admin user/secret is used for web controller -->
        <!-- clusterid should be unique in subnet -->
        <!-- clustersecret is used for routers to connect with each other in same cluster -->
        <cluster admin="admin" adminsecret="cisco123" clusterid="conductor"
            clustersecret="cisco123" type="MSGINFRA">
            <zones>
                <!-- datasource should be pointed to a name under datasource defination, all
                    components under single zone are based on same datasource -->
                <zone datasource="data1" name="infrazone">
                    <adminjid>
                        <!-- adminjid user should be defined as
                            "5555@MGMT_DOMAIN_JSM_HOSTNAME" which is defined in management
                            node -->
                        <jid>admin@management.cisco.conductor.com</jid>
                        <secret>cisco123</secret>
                    </adminjid>
                    <nodes>
                        <!-- the name should match the "hostname" configuration in
                            platformConfig.xml -->
                        <!-- "INFRA" type node should be configured with msginfra function
                            component -->
                        <node name="vm-svc-1" type="INFRA">
                            <realms>
                                <!-- a "BOOTSTRAP" router is a MUST on each node for internal control
                                    plane usage -->
                                <!-- mdns should be "on" for routers to discovery each other automatically -
                                    ->
                                <realm adminip="10.0.0.1" adminport="7300" ip="10.0.0.1"
                                    ipmask="255.255.0.0" mdns="on" port="7400" realmid="boot-vm-svc-1"
                                    type="BOOTSTRAP"/>
                                <!-- adminport/port should be different with each router -->
                            </realms>
                        </node>
                    </nodes>
                </zone>
            </zones>
        </cluster>
    </clusters>
</configuration>
```

Cluster File Examples

```
<realm adminip="10.0.0.1" adminport="7301" ip="10.0.0.1"
ipmask="255.255.0.0" mdns="on" port="7401" realmid="router-vm-svc-1"
type="HADISABLED">

    <!-- CMW component is used for BOSH client, listening port on 5280 -->
    <component name="cmw-1" port="5280" svcip="10.0.0.1"
svcipmask="255.255.0.0" type="CMW"/>

    <!-- CM component is used for general client, listening port on 5222 -->
    <component name="cm-1" port="5222" svcip="10.0.0.1"
svcipmask="255.255.0.0" type="CM"/>

    <!-- SASL component is used for user authentication -->
    <component name="sasl-1" type="SASL"/>

    <!-- JSM component is used for user session operation -->
    <!-- the JSM component here is for client side usage, the hostname is
defined as CLIENT_DOMAIN_JSM_HOSTNAME -->

    <!-- user should register jid by
"5555@CLIENT_DOMAIN_JSM_HOSTNAME" -->
    <component hostname="cisco.conductor.com" name="jsm-1" msg="1"
type="JSM"/>

    <!-- SMM component is used for service redirection and load balancer -->
    <!-- SMM component hostname is used for client/service sdk to discovery
-->

    <!-- SMM component svmid should be configured explicitly to SVM
component hostname -->
    <component hostname="smm.svc.conductor.com"
svmid="svm.svc.conductor.com" name="smm-1" type="SMM"/>

    <!-- PS component is used to implement publish/subscribe function -->
    <!-- PS component hostname is used for user to discovery -->
    <component hostname="ps.conductor" name="pubsub-1" type="PS"/>

        <component algo="db" isforsvc="1"
hostname="svc.conductor.com" name="sdns-1" subtype="JSM" type="SDNS">
            <compid>jsm-1.router-vm-svc-2</compid>
        </component>
    </realm>

    <realm adminip="10.0.0.1" adminport="7302" ip="10.0.0.1"
ipmask="255.255.0.0" mdns="on" port="7402" realmid="router-vm-svc-2"
type="HADISABLED">

        <!-- CM component here is used for service instance, listening port on 5223
-->
        <component name="cm-1" port="5223" svcip="10.0.0.1"
svcipmask="255.255.0.0" type="CM"/>

        <component name="sasl-1" type="SASL"/>
```

Appendix A

The cluster.xml Files

```
<!-- the JSM component here is for service instance side usage, it should be
configured explicitly with "isforsvc" flag to "1"-->
<!-- the service side JSM hostname is defined as
SERVICE_DOMAIN_JSM_HOSTNAME -->
<component offline="0" bcc="svm.svc.conductor.com" isforsvc="1"
name="jsm-1" type="JSM"/>
<!-- SMM component hostname should be equal to each other in same
cluster -->
<component hostname="smm.svc.conductor.com"
svmid="svm.svc.conductor.com" name="smm-1" type="SMM"/>
<!-- SVCVIEWER component is used to display service side information
on web gui -->
<!-- SVCVIEWER component svmid should be configured explicitly to
SVM component hostname -->
<component name="svcviewer-1" svmid="svm.svc.conductor.com"
type="SVCVIEWER"/>
<!-- SVM component is used for service virtualization -->
<!-- SVM component hostname is used for SMM/SVCVIEWER to
discovery -->
<component hostname="svm.svc.conductor.com" name="svm-1"
type="SVM"/>
<!-- HTTPGW component is used for service side HTTP service gateway -->
<!-- HTTPGW component jsmdomain should be pointed to the service side
JSM/SDNS hostname -->
<!-- HTTPGW component jsmid should be configured with the component
id of service side JSM component -->
<component name="httpgw-1" cmip="10.0.0.1" cmport="5223"
jsmdomain="svc.conductor.com" jsmid="jsm-1.router-vm-svc-2" type="HTTPGW"/>
<!-- PS component here is dedicated for service directory usage, must be
named as pubsub.virtual -->
<component hostname="pubsub.virtual" name="pubsub-1" type="PS"/>
<!-- SDNS component is used for msginfra internal load balance for other
components -->
<!-- A JSM-subtype SDNS component for service side should be
configured explicitly with "isforsvc" flag to "1" -->
<!-- A JSM-subtype SDNS component for service side should be
configured explicitly with "db" algorithm -->
<!-- A JSM-subtype SDNS component for service side with "db" algorithm
should contain the one and only <compid> sub-element -->
```

Cluster File Examples

```
<component algo="db" isforsvc="1" hostname="svc.conductor.com"
name="sdns-1" subtype="JSM" type="SDNS">
    <compid>jsm-1.router-vm-svc-2</compid>
    </component>
</realm>
</realms>
</node>
</nodes>
</zone>
<zone datasource="data1" name="svczone">
    <adminjid>
        <jid>admin@management.cisco.conductor.com</jid>
        <secret>cisco123</secret>
    </adminjid>
    <nodes>
        <node name="vm-svc-2" type="SERVICE">
            <realms>
<!-- a "SERVICE" type node should only be deployed with single bootstrap
router --&gt;
                &lt;realm adminip="10.0.0.3" adminport="7300" ip="10.0.0.3"
ipmask="255.255.0.0" mdns="on" port="7400" realmid="boot-vm-svc-2"
type="BOOTSTRAP"/&gt;
            &lt;/realms&gt;
        &lt;/node&gt;
    &lt;/nodes&gt;
&lt;/zone&gt;
&lt;zone datasource="data1" name="mgmtzone"&gt;
    &lt;adminjid&gt;
        &lt;jid&gt;admin@management.cisco.conductor.com&lt;/jid&gt;
        &lt;secret&gt;cisco123&lt;/secret&gt;
    &lt;/adminjid&gt;
    &lt;nodes&gt;
<!-- management node should be configured to "MGMT" --&gt;
        &lt;node name="vm-mgmt-1" type="MGMT"&gt;
            &lt;realms&gt;
                &lt;realm adminip="10.0.0.2" adminport="7300" ip="10.0.0.2"
ipmask="255.255.0.0" mdns="on" port="7400" realmid="boot-vm-mgmt-1"
type="BOOTSTRAP"&gt;
                    &lt;!-- only MC/MCC component should be deployed on BOOTSTRAP
router in management node --&gt;
            &lt;/realms&gt;
        &lt;/node&gt;
    &lt;/nodes&gt;
&lt;/zone&gt;</pre>
```

Appendix A

The cluster.xml Files

```
<!-- MC component is used for management core function -->
<component hostname="mc.cisco.conductor.com" name="mc-1"
type="MC"/>

<!-- MCC component is used to implement management core console -->
<component hostname="mcc.cisco.conductor.com" name="mcc-1"
snmpport="11162" type="MCC"/>
</realm>
<realm adminip="10.0.0.2" adminport="7301" ip="10.0.0.2"
ipmask="255.255.0.0" mdns="on" port="7401" realmid="router-vm-mgmt-1"
type="HADISABLED">

<!-- the JSM component here is for management side usage, the hostname
is defined as MGMT_DOMAIN_JSM_HOSTNAME -->
<component hostname="management.cisco.conductor.com" name="jsm-1"
type="JSM"/>

<!-- CM component here is used for management side usage, listening port
on 5222 -->
<component name="cm-1" port="5222" svcip="10.0.0.2"
svcipmask="255.255.0.0" type="CM"/>
<component name="sasl-1" type="SASL"/>

<!-- PS component hostname here MUST be "pubsub.service" for internal
usage, so other PS components should not be named as "pubsub.service" -->
<component hostname="pubsub.service" name="pubsub-1" type="PS"/>
</realm>
</realms>
</node>
</nodes>
</zone>
</zones>
</cluster>
</clusters>
<datasource>

<!-- only one data source could be deployed in single cluster -->
<!-- the name defined here should be referred in each zone -->
<!-- ip could be IP address or RAC domain name -->
<!-- msginfrauser/platformuser is used for creating two database user in oracle
database server, they must be upper case -->
<!-- msginfrausersecret/platformusersecret is used as database administrator
users-->
<!-- dbsvrsuperps should be defined with the ssh password of database node -->
```

Cluster File Examples

```
<data dbtype="oracle-oci" service="wcs" msginfrauser="MSGINFRA"  
msginfrausersecret="MSGINFRA" platformuser="PLATFORM"  
platformusersecret="PLATFORM" ip="10.0.0.1" name="data1" port="1521"/>  
</datasource>  
</configuration>
```

Sample cluster.simple.R2-5 File

A sample cluster.simple.R2-5.xml file follows.

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration version="@VERSION@">
    <clusters>
        <cluster admin="@ADMINID@" adminsecret="@ADMINPASSWD@"
            clusterid="@CLUSTERID@" clustersecret="@CLUSTERPASSWD@" type="MSGINFRA">
                <zones>
                    <zone datasource="data1" name="@SVCTYPE@zone">
                        <adminjid>
                            <jid>admin@@MGMTJSM@</jid>
                            <secret>@ADMINJIDPASSWD@</secret>
                        </adminjid>
                        <nodes>
                            <node name="@SVCVM@-1" type="INFRA">
                                <realms>
                                    <realm adminip="@ADMINIP1@" adminport="7300" ip="@SVCIP1@"
                                        ipmask="@SVCNETMASK@" mdns="on" port="7400" realmid="boot-@SVCVM@-1"
                                        type="BOOTSTRAP"/>
                                    <realm adminip="@ADMINIP1@" adminport="7301" ip="@SVCIP1@"
                                        ipmask="@SVCNETMASK@" mdns="on" port="7401" realmid="router-@SVCVM@-1"
                                        type="HADISABLED">
                                        <component name="cmw-1" port="5280" svcip="@CMIP1@"
                                            svcipmask="@CMNETMASK@" type="CMW"/>
                                        <component compport="5223" name="cm-1" port="5222"
                                            svcip="@CMIP1@" svcipmask="@CMNETMASK@" type="CM"/>
                                        <component name="sasl-1" type="SASL"/>
                                        <component hostname="@CLIENTJSM@" name="jsm-1" msg="1"
                                            type="JSM"/>
                                        <component hostname="@SVCSMM@" svmid="@SVCSV@" name="smm-1"
                                            type="SMM"/>
                                        <component hostname="@SVCPS@" name="pubsub-1" type="PS"/>
                                        <component algo="db" isforsvc="1" hostname="@SVCJSM@"
                                            name="sdns-1" subtype="JSM" type="SDNS">
                                            <compid>jsm-1.router-@SVCVM@-2</compid>
                                        </component>
                                    </realm>
                                    <realm adminip="@ADMINIP1@" adminport="7302" ip="@SVCIP1@"
                                        ipmask="@SVCNETMASK@" mdns="on" port="7402" realmid="router-@SVCVM@-2"
                                        type="HADISABLED">
                                        <component compport="5225" name="cm-1" port="5224"
                                            svcip="@CMIP1@" svcipmask="@CMNETMASK@" isforsvc="1" type="CM"/>
                                    </realm>
                                </nodes>
                            </node>
                        </nodes>
                    </zone>
                </zones>
            </cluster>
        </clusters>
    </configuration>
```

```

<component name="sasl-1" type="SASL"/>
<component offline="0" bcc="@SVCSVMM@" isforsvc="1"
name="jsm-1" type="JSM"/>
<component hostname="@SVCSMM@" svmid="@SVCSVMM@" name="smm-
1" type="SMM"/>
<component name="svcviewer-1" svmid="@SVCSVMM@" type="SVCVIEWER"/>
<component hostname="@SVCSVMM@" name="svm-1" type="SVM"/>
<component name="httpgw-1" cmip="@CMIP1@" cmport="5224"
jsmdomain="@SVCJSM@" jsmid="jsm-1.router-@SVCVM@-2" type="HTTPGW"/>
<component hostname="pubsub.virtual" name="pubsub-1"
type="PS"/>
<component algo="db" isforsvc="1" hostname="@SVCJSM@"
name="sdns-1" subtype="JSM" type="SDNS">
<compid>jsm-1.router-@SVCVM@-2</compid>
</component>
</realm>
</realms>
</node>
</nodes>
</zone>
<zone datasource="data1" name="@MGMNTTYPE@zone">
<adminjid>
<jid>admin@@MGMNTJSM@</jid>
<secret>@ADMINJIDPASSWD@</secret>
</adminjid>
<nodes>
<node hahlthchkcnt="3" hahlthchkigncnt="3" hahlthchkintrvl="30"
harestartcnt="5" harestartperiod="1200" name="@MGMNTVMM@-1" type="MGMNT">
<realms>
<realm adminip="@ADMINIP2@" adminport="7300" ip="@SVCIP2@"
ipmask="@SVCNETMASK@" mdns="on" port="7400" realmid="boot-@MGMNTVMM@-1"
type="BOOTSTRAP">
<component hostname="@MGMNTMC@" name="mc-1" type="MC"/>
<component hostname="@MGMNTMCC@" cmip="@CMIP2@"
cmport="5222" name="mcc-1" snmpport="11162" type="MCC">
<managedomain>@MGMNTJSM@</managedomain>
</component>
</realm>
<realm adminip="@ADMINIP2@" adminport="7301" ip="@SVCIP2@"
ipmask="@SVCNETMASK@" mdns="on" port="7401" realmid="router-@MGMNTVMM@-1"
type="HADISABLED">
<component hostname="@MGMNTJSM@" name="jsm-1" type="JSM"/>

```

Appendix A

The cluster.xml Files

```
        <component compport="5223" name="cm-1" port="5222"
svcip="@CMIP2@" svcipmask="@CMNETMASK@" type="CM"/>
        <component name="sasl-1" type="SASL"/>
        <component hostname="pubsub.service" name="pubsub-1"
type="PS"/>
    </realm>
</realms>
</node>
</nodes>
</zone>
</zones>
</cluster>
</clusters>
<datasource>
    <data conductordb="@CDBNAME@" dbsecret="@DBPASSWD@" dbsvrsuperps="cisco"
dbuser="@DBADMIN@" ip="@SVCIP1@" msginfradb="@MDBNAME@" name="data1"
port="5432"/>
</datasource>
</configuration>
<!--Configuration Parameters
Deployment Mode:          @DEPLOYMODE@
Traffic Model:
Quantity of Users:
Quantity of UCS hosts:
VM Template Version:      4.0/5.0
Service Node Template:     @SVCTEMPLATE@
Database Node Template:   @SVCTEMPLATE@
Management Node Template: @MGMTTEMPLATE@
Cluster Name:             @CLUSTERID@
Cluster Password:         @CLUSTERPASSWD@
Router Admin Username:    @ADMINID@
Router Admin Password:    @ADMINPASSWD@
JSM Domain Name:          @CLIENTJSMD@*
Pubsub Domain Name:        @SVCPSD@*
Service Virtualization Domain Name:  @SVCJSMD@*
Router IP address:         @SVCIP1@*
Router IP netmask:         @SVCNETMASK@*
```

Cluster File Examples

Router Admin IP address: @ADMINIP1@
Router IP netmask: @ADMINNETMASK@
CM IP address: @CMIP1@
CM IP netmask: @CMNETMASK@
Database Admin Username: @DBADMIN@
Database Admin Password: @DBPASSWD@
Conductor Database Name: @CDBNAME@
Msginfra Database Name: @MDBNAME@
Admin Jid Password: @ADMINJIDPASSWD@
-->

Sample cluster.single.R2-5 File

A sample cluster.single.R2-5.xml file follows.

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration version="@VERSION@">
  <clusters>
    <cluster admin="@ADMINID@" adminsecret="@ADMINPASSWD@"
      clusterid="@CLUSTERID@" clustersecret="@CLUSTERPASSWD@" type="MSGINFRA">
        <zones>
          <zone datasource="data1" name="singlezone">
            <adminjid>
              <jid>admin@@MGMTJSM</jid>
              <secret>@ADMINJIDPASSWD@</secret>
            </adminjid>
            <nodes>
              <node name="@MGMTVVM@-1" type="MGMT">
                <realms>
                  <realm adminip="@ADMINIP@" adminport="7300" ip="@SVCIP@"
                    ipmask="@SVCNETMASK@" mdns="on" port="7400" realmid="boot-@MGMTVVM@-1"
                    type="BOOTSTRAP">
                    <component hostname="@MGMTMC@" name="mc-1" type="MC"/>
                    <component hostname="@MGMTMCC@" cmip="@CMIP@"
                      compport="5222" name="mcc-1" snmpport="11162" type="MCC">
                      <manageddomain>@MGMTJSM</manageddomain>
                    </component>
                  </realm>
                  <realm adminip="@ADMINIP@" adminport="7301" ip="@SVCIP@"
                    ipmask="@SVCNETMASK@" mdns="on" port="7401" realmid="router-@MGMTVVM@-1"
                    type="HADISABLED">
                    <component compport="5223" name="cm-1" port="5222"
                      svcip="@CMIP@" svcipmask="@CMNETMASK@" type="CM"/>
                    <component name="sasl-1" type="SASL"/>
                    <component hostname="@MGMTJSM@" name="jsm-1" type="JSM"/>
                    <component hostname="pubsub.service" name="pubsub-1"
                      type="PS"/>
                  </realm>
                  <realm adminip="@ADMINIP@" adminport="7302" ip="@SVCIP@"
                    ipmask="@SVCNETMASK@" mdns="on" port="7402" realmid="router-@MGMTVVM@-2"
                    type="HADISABLED">
                    <component compport="5225" name="cm-1" port="5224"
                      svcip="@CMIP@" svcipmask="@CMNETMASK@" type="CM"/>
                  </realm>
                </realms>
              </node>
            </nodes>
          </zone>
        </zones>
      </cluster>
    </clusters>
  </configuration>
```

```

<component name="cmw-1" port="5280" svcip="@CMIP@"
svcipmask="@CMNETMASK@" type="CMW"/>
<component name="sasl-1" type="SASL"/>
<component hostname="@CLIENTJSM@" name="jsm-1" msg="1"
type="JSM"/>
<component hostname="@SVCSMM@" svmid="@SVCSVM@" name="smm-
1" type="SMM"/>
<component hostname="@SVCPS@" name="pubsub-1" type="PS"/>
<component algo="db" isforsvc="1" hostname="@SVCJSM@"
name="sdns-1" subtype="JSM" type="SDNS">
<compid>jsm-1.router-@MGMTVM@-3</compid>
</component>
</realm>
<realm adminip="@ADMINIP@" adminport="7303" ip="@SVCIP@"
ipmask="@SVCNETMASK@" mdns="on" port="7403" realmid="router-@MGMTVM@-3"
type="HADISABLED">
<component compport="5227" name="cm-1" port="5226"
svcip="@CMIP@" svcipmask="@CMNETMASK@" isforsvc="1" type="CM"/>
<component name="sasl-1" type="SASL"/>
<component offline="0" bcc="@SVCSVM@" isforsvc="1"
name="jsm-1" type="JSM"/>
<component hostname="@SVCSMM@" svmid="@SVCSVM@" name="smm-
1" type="SMM"/>
<component name="svcviewer-1" svmid="@SVCSVM@"
type="SVCVIEWER"/>
<component hostname="@SVCSVM@" name="svm-1" type="SVM"/>
<component name="httpgw-1" cmip="@CMIP@" cmport="5226"
jsmdomain="@SVCJSM@" jsmid="jsm-1.router-@MGMTVM@-3" type="HTTPGW"/>
<component hostname="pubsub.virtual" name="pubsub-1"
type="PS"/>
<component algo="db" isforsvc="1" hostname="@SVCJSM@"
name="sdns-1" subtype="JSM" type="SDNS">
<compid>jsm-1.router-@MGMTVM@-3</compid>
</component>
</realm>
</realms>
</node>
</nodes>
</zone>
</zones>
</cluster>
</clusters>
<datasource>

```

Appendix A

The cluster.xml Files

```
<data conductordb="@CDBNAME@" dbsecret="@DBPASSWD@" dbsvrsuperps="cisco"
dbuser="@DBADMIN@" ip="@SVCIP@" msginfradb="@MDBNAME@" name="data1"
port="5432"/>
</datasource>
</configuration>
<!--Configuration Parameters
Deployment Mode: @DEPLOYMODE@
Traffic Model:
Quantity of Users:
Quantity of UCS hosts:
VM Template Version: 4.0/5.0
Service Node Template: @MGMTTEMPLATE@
Database Node Template: @MGMTTEMPLATE@
Management Node Template: @MGMTTEMPLATE@
Cluster Name: @CLUSTERID@
Cluster Password: @CLUSTERPASSWD@
Router Admin Username: @ADMINID@
Router Admin Password: @ADMINPASSWD@
JSM Domain Name: @CLIENTJSM@
Pubsub Domain Name: @SVCPS@
Service Virtualization Domain Name: @SVCJSM@
Router IP address: @SVCIP@
Router IP netmask: @SVCNETMASK@
Router Admin IP address: @ADMINIP@
Router IP netmask: @ADMINNETMASK@
CM IP address: @CMIP@
CM IP netmask: @CMNETMASK@
Database Admin Username: @DBADMIN@
Database Admin Password: @DBPASSWD@
Conductor Database Name: @CDBNAME@
Msginfra Database Name: @MDBNAME@
Admin Jid Password: @ADMINJIDPASSWD@
-->
```

Sample cluster.all-in-one.oracle.R2-5.xml File

A sample cluster.all-in-one.oracle.R2-5.xml file follows.

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <clusters>
    <cluster admin="admin" adminsecret="cisco123" clusterid="conductor25"
    clustersecret="cisco123" type="MSGINFRA">
      <zones>
        <zone datasource="data1" name="singlezone">
          <adminjid>
            <jid>admin@management.cisco.conductor.com</jid>
            <secret>cisco123</secret>
          </adminjid>
          <nodes>
            <node name="single-mgmt" type="MGMT">
              <realms>
                <realm adminip="90.0.60.201" ipmask="255.255.0.0"
                  adminport="7300" ip="90.0.60.201" mdns="on" port="7400" realmid="boot-
                  single-mgmt-1" type="BOOTSTRAP">
                  <component hostname="mc.cisco.conductor.com" name="mc-1"
                  type="MC"/>
                  <component hostname="mcc.cisco.conductor.com"
                  cmip="90.0.60.201" cmport="5222" name="mcc-1" snmpport="11162" type="MCC">
                </realm>
                <realm adminip="90.0.60.201" ipmask="255.255.0.0"
                  adminport="7301" ip="90.0.60.201" mdns="on" port="7401" realmid="router-
                  single-mgmt-1" type="HADISABLED">
                  <component compport="5223" name="cm-1" port="5222"
                  svcip="90.0.60.201" svcipmask="255.255.0.0" type="CM"/>
                  <component name="sasl-1" type="SASL"/>
                  <component hostname="management.cisco.conductor.com"
                  name="jsm-1" type="JSM"/>
                  <component hostname="pubsub.service" name="pubsub-1"
                  type="PS"/>
                </realm>
                <realm adminip="90.0.60.201" ipmask="255.255.0.0"
                  adminport="7302" ip="90.0.60.201" mdns="on" port="7402" realmid="router-
                  single-mgmt-2" type="HADISABLED">
              </components>
            </node>
          </nodes>
        </zone>
      </zones>
    </cluster>
  </clusters>
</configuration>
```

Appendix A

The cluster.xml Files

```
<component compport="5225" name="cm-1" port="5224"
svcip="90.0.60.201" svcipmask="255.255.0.0" svcip6="2001:da8:207::9500"
svcip6prefixlen="64" compport6="5225" port6="5224" type="CM"/>

<component name="cmw-1" port="5280" svcip="90.0.60.201"
svcipmask="255.255.0.0" svcip6="2001:da8:207::9500" svcip6prefixlen="64"
port6="5280" type="CMW"/>

<component name="sasl-1" type="SASL"/>

<component hostname="cisco.conductor.com" name="jsm-1"
eb="sdns-cd-1.router-single-mgmt-2"
rosternotifyurl="http://www.cisco.com/notify" msg="1" type="JSM"/>

<component name="sdns-cd-1" subtype="CD" type="SDNS">
    <compid>cd-1.router-single-mgmt-2</compid>
</component>

<component hostname="smm.svc.conductor.com"
svmid="svm.svc.conductor.com" name="smm-1" type="SMM"/>

<component hostname="ps.conductor" name="pubsub-1"
type="PS"/>

<component algo="db" hostname="svc.conductor.com"
name="sdns-jsm-1" isforsvc="1" subtype="JSM" type="SDNS">
    <compid>jsm-1.router-single-mgmt-3</compid>
</component>

</realm>

<realm adminip="90.0.60.201" ipmask="255.255.0.0"
adminport="7303" ip="90.0.60.201" mdns="on" port="7403" realmid="router-
single-mgmt-3" type="HADISABLED">

    <component compport="5227" name="cm-1" port="5226"
svcip="90.0.60.201" svcipmask="255.255.0.0" isforsvc="1" type="CM"/>

        <component name="sasl-1" type="SASL"/>

        <component offline="0" bcc="svm.svc.conductor.com"
name="jsm-1" isforsvc="1" type="JSM"/>

            <component algo="db" hostname="svc.conductor.com"
name="sdns-jsm-1" isforsvc="1" subtype="JSM" type="SDNS">
                <compid>jsm-1.router-single-mgmt-3</compid>
            </component>

            <component hostname="smm.svc.conductor.com"
svmid="svm.svc.conductor.com" name="smm-1" type="SMM"/>

            <component name="svcreader-1"
svmid="svm.svc.conductor.com" type="SVCREADER"/>

            <component hostname="svm.svc.conductor.com" name="svm-1"
type="SVM"/>

            <component name="httpgw-1" cmip="90.0.60.201"
cmport="5222" jsmdomain="svc.conductor.com" jsmid="jsm-1.router-single-mgmt-
3" type="HTTPGW"/>

            <component hostname="pubsub.virtual" name="pubsub-1"
type="PS"/>

        </realm>
</realms>
```

Cluster File Examples

```
</node>
</nodes>
</zone>
</zones>
</cluster>
</clusters>
<datasource>
  <data dbtype="oracle-oci" service="wcs" msginfrauser="MSGINFRA"
msginfrausersecret="MSGINFRA" platformuser="PLATFORM"
platformusersecret="PLATFORM" ip="90.0.60.200" name="data1" port="1521"/>
</datasource>
</configuration>
```

Sample cluster.all-in-one.postgres.R2-5.xml File

A sample cluster.all-in-one.postgres.R2-5.xml file follows.

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <clusters>
        <cluster admin="admin" adminsecret="cisco123" clusterid="conductor25"
            clustersecret="cisco123" type="MSGINFRA">
            <zones>
                <zone datasource="data1" name="singlezone">
                    <adminjid>
                        <jid>admin@management.cisco.conductor.com</jid>
                        <secret>cisco123</secret>
                    </adminjid>
                    <nodes>
                        <node name="single-mgmt" type="MGMT">
                            <realms>
                                <realm adminip="90.0.60.201" ipmask="255.255.0.0"
                                    adminport="7300" ip="90.0.60.201" mdns="on" port="7400" realmid="boot-
                                    single-mgmt-1" type="BOOTSTRAP">
                                    <component hostname="mc.cisco.conductor.com" name="mc-1"
                                        type="MC"/>
                                    <component hostname="mcc.cisco.conductor.com"
                                        cmip="90.0.60.201" cmport="5222" name="mcc-1" snmpport="11162" type="MCC">
                                </realm>
                                <realm adminip="90.0.60.201" ipmask="255.255.0.0"
                                    adminport="7301" ip="90.0.60.201" mdns="on" port="7401" realmid="router-
                                    single-mgmt-1" type="HADISABLED">
                                    <component compport="5223" name="cm-1" port="5222"
                                        svcip="90.0.60.201" svcipmask="255.255.0.0" type="CM"/>
                                    <component name="sasl-1" type="SASL"/>
                                    <component hostname="management.cisco.conductor.com"
                                        name="jsm-1" type="JSM"/>
                                    <component hostname="pubsub.service" name="pubsub-1"
                                        type="PS"/>
                                </realm>
                                <realm adminip="90.0.60.201" ipmask="255.255.0.0"
                                    adminport="7302" ip="90.0.60.201" mdns="on" port="7402" realmid="router-
                                    single-mgmt-2" type="HADISABLED">
                            </realms>
                        </node>
                    </nodes>
                </zone>
            </zones>
        </cluster>
    </clusters>
</configuration>
```

```

        <component compport="5225" name="cm-1" port="5224"
svcip="90.0.60.201" svcipmask="255.255.0.0" svcip6="2001:da8:208::9500"
svcip6prefixlen="64" compport6="5225" port6="5224" type="CM"/>

        <component name="cmw-1" port="5280" svcip="90.0.60.201"
svcipmask="255.255.0.0" svcip6="2001:da8:208::9500" svcip6prefixlen="64"
port6="5280" type="CMW"/>

        <component name="sasl-1" type="SASL"/>

        <component hostname="cisco.conductor.com" name="jsm-1"
eb="sdns-cd-1.router-single-mgmt-2"
rosternotifyurl="http://www.cisco.com/notify" msg="1" type="JSM"/>

        <component name="sdns-cd-1" subtype="CD" type="SDNS">
            <compid>cd-1.router-single-mgmt-2</compid>
        </component>

        <component hostname="smm.svc.conductor.com"
svmid="svm.svc.conductor.com" name="smm-1" type="SMM"/>

        <component hostname="ps.conductor" name="pubsub-1"
type="PS"/>

            <component algo="db" hostname="svc.conductor.com"
name="sdns-jsm-1" isforsvc="1" subtype="JSM" type="SDNS">
                <compid>jsm-1.router-single-mgmt-3</compid>
            </component>
        </realm>

        <realm adminip="90.0.60.201" ipmask="255.255.0.0"
adminport="7303" ip="90.0.60.201" mdns="on" port="7403" realmid="router-
single-mgmt-3" type="HADISABLED">

            <component compport="5227" name="cm-1" port="5226"
svcip="90.0.60.201" svcipmask="255.255.0.0" isforsvc="1" type="CM"/>

            <component name="sasl-1" type="SASL"/>

            <component offline="0" bcc="svm.svc.conductor.com"
name="jsm-1" isforsvc="1" type="JSM"/>

            <component algo="db" hostname="svc.conductor.com"
name="sdns-jsm-1" isforsvc="1" subtype="JSM" type="SDNS">
                <compid>jsm-1.router-single-mgmt-3</compid>
            </component>

            <component hostname="smm.svc.conductor.com"
svmid="svm.svc.conductor.com" name="smm-1" type="SMM"/>

            <component name="svcreader-1"
svmid="svm.svc.conductor.com" type="SVCREADER"/>

            <component hostname="svm.svc.conductor.com" name="svm-1"
type="SVM"/>

            <component name="httpgw-1" cmip="90.0.60.201"
cmport="5222" jsmdomain="svc.conductor.com" jsmid="jsm-1.router-single-mgmt-
3" type="HTTPGW"/>

            <component hostname="pubsub.virtual" name="pubsub-1"
type="PS"/>

        </realm>
    </realms>

```

Appendix A

The cluster.xml Files

```
</node>
</nodes>
</zone>
</zones>
</cluster>
</clusters>
<datasource>
    <data conductordb="platform" dbsecret="cisco123" dbsvrsuperps="cisco"
dbuser="conductor" ip="90.0.60.201" msginfradb="msginfra" name="data1"
port="5432"/>
</datasource>
</configuration>
```

Sample cluster.ha.oracle.R2-5 xml File

A sample cluster.ha.oracle.R2-5 xml file follows.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<configuration>
  <clusters>
    <cluster admin="admin" adminsecret="cisco123" clusterid="conductor25"
    clustersecret="cisco123" type="MSGINFRA">
      <zones>
        <zone datasource="data1" name="clientzone">
          <adminjid>
            <jid>admin@management.cisco.conductor.com</jid>
            <secret>cisco123</secret>
          </adminjid>
          <nodes>
            <node name="r25-client-1" type="INFRA">
              <realms>
                <realm adminip="90.0.60.202" ipmask="255.255.0.0"
                  adminport="7300" ip="90.0.60.202" mdns="on" port="7400" realmid="bootstrap-
                  r25-client-1" type="BOOTSTRAP"/>
                <realm adminip="90.0.60.202" ipmask="255.255.0.0"
                  adminport="7301" ip="90.0.60.202" mdns="on" port="7401" realmid="cm-r25-
                  client-1" type="HADISABLED">
                  <component name="cmw-1" port="5280" svcip="90.0.60.202"
                    svcipmask="255.255.0.0" port6="5280" svcip6="2001:da8:210::9000"
                    svcip6prefixlen="64" type="CMW"/>
                  <component compport="5223" name="cm-1" port="5222"
                    svcip="90.0.60.202" svcipmask="255.255.0.0" compport6="5223" port6="5222"
                    svcip6="2001:da8:210::9000" svcip6prefixlen="64" type="CM"/>
                  <component name="sasl-1" type="SASL"/>
                </realm>
                <realm adminip="90.0.60.202" ipmask="255.255.0.0"
                  adminport="7302" ip="90.0.60.202" mdns="on" port="7402" realmid="jsm-ha-r25-
                  client" type="HAENABLED">
                  <component hostname="cisco.conductor.com" name="jsm-1"
                    eb="sdns-cd-1.jsm-ha-r25-client"
                    rosternotifyurl="http://www.cisco.com/notify" msg="1" type="JSM"/>
                  <component hostname="smm.svc.conductor.com" name="smm-1"
                    svmid="svm.svc.conductor.com" threadingpolicy="source" type="SMM"/>
                  <component name="sdns-cd-1" subtype="CD" type="SDNS">
                    <compid>cd-1.jsm-ha-r25-client</compid>
                  </component>
                  <component algo="db" hostname="svc.conductor.com"
                    name="sdns-svcjsm-1" subtype="JSM" isforsvc="1" type="SDNS"/>
                </realm>
              </nodes>
            </cluster>
          </configuration>
```

Appendix A

The cluster.xml Files

```
<compid>jsm-1.cm-jsm-nonha-r25-service</compid>
</component>
</realm>
</realms>
</node>

<node name="r25-client-2" type="INFRA">
<realms>

<realm adminip="90.0.60.203" ipmask="255.255.0.0"
adminport="7300" ip="90.0.60.203" mdns="on" port="7400" realmid="bootstrap-
r25-client-2" type="BOOTSTRAP"/>
<realm adminip="90.0.60.203" ipmask="255.255.0.0"
adminport="7301" ip="90.0.60.203" mdns="on" port="7401" realmid="ps-r25-
client-2" type="HADISABLED">
<component hostname="ps.conductor" name="pubsub-1"
type="PS"/>
</realm>
<realm adminip="90.0.60.203" ipmask="255.255.0.0"
adminport="7302" ip="90.0.60.203" mdns="on" port="7402" realmid="jsm-ha-r25-
client" type="HAENABLED">
<component hostname="cisco.conductor.com" name="jsm-1"
eb="sdns-cd-1.jsm-ha-r25-client"
rosternotifyurl="http://www.cisco.com/notify" msg="1" type="JSM"/>
<component hostname="smm.svc.conductor.com" name="smm-1"
svmid="svm.svc.conductor.com" threadingpolicy="source" type="SMM"/>
<component name="sdns-cd-1" subtype="CD" type="SDNS">
<compid>cd-1.jsm-ha-r25-client</compid>
</component>
<component algo="db" hostname="svc.conductor.com"
name="sdns-svcjsm-1" subtype="JSM" isforsvc="1" type="SDNS">
<compid>jsm-1.cm-jsm-nonha-r25-service</compid>
</component>
</realm>
</realms>
</node>
</nodes>
</zone>
<zone datasource="data1" name="svzone">
<adminjid>
<jid>admin@management.cisco.conductor.com</jid>
<secret>cisco123</secret>
</adminjid>
<nodes>
<node name="r25-service" type="INFRA">
```

```

<realms>
    <realm adminip="90.0.60.204" ipmask="255.255.0.0"
adminport="7300" ip="90.0.60.204" mdns="on" port="7400" realmid="bootstrap-
r25-service" type="BOOTSTRAP"/>
    <realm adminip="90.0.60.204" ipmask="255.255.0.0"
adminport="7301" ip="90.0.60.204" mdns="on" port="7401" realmid="cm-jsm-
nonha-r25-service" type="HADISABLED">
        <component name="cmw-1" port="5280" svcip="90.0.60.204"
svcipmask="255.255.0.0" isforsvc="1" type="CMW"/>
        <component compport="5223" name="cm-1" port="5222"
svcip="90.0.60.204" svcipmask="255.255.0.0" isforsvc="1" type="CM"/>
        <component name="sasl-1" type="SASL"/>
        <component offline="0" bcc="svm.svc.conductor.com"
name="jsm-1" isforsvc="1" type="JSM"/>
        <component hostname="smm.svc.conductor.com" name="smm-1"
svmid="svm.svc.conductor.com" threadingpolicy="id" type="SMM"/>
        <component name="svcviewer-1"
svmid="svm.svc.conductor.com" type="SVCVIEWER"/>
        <component name="httpgw-1" cmip="90.0.60.204"
cmport="5222" jsmdomain="svc.conductor.com" jsmid="jsm-1.cm-jsm-nonha-r25-
service" type="HTTPGW"/>
        <component hostname="svm.svc.conductor.com" name="svm-1"
type="SVM"/>
        <component hostname="pubsub.virtual" name="pubsub-1"
type="PS"/>
        <component algo="db" hostname="svc.conductor.com"
name="sdns-svcjsm-1" subtype="JSM" isforsvc="1" type="SDNS">
            <compid>jsm-1.cm-jsm-nonha-r25-service</compid>
        </component>
    </realm>
</realms>
</node>
</nodes>
</zone>
<zone datasource="data1" name="mgmtzone">
    <adminjid>
        <jid>admin@management.cisco.conductor.com</jid>
        <secret>cisco123</secret>
    </adminjid>
    <nodes>
        <node name="r25-mgmt-1" type="MGMNT">
            <realms>
                <realm adminip="90.0.60.205" ipmask="255.255.0.0"
adminport="7300" ip="90.0.60.205" mdns="on" port="7400" realmid="bootstrap-
r25-mgmt-1" type="BOOTSTRAP">

```

Appendix A

The cluster.xml Files

```
<component hostname="mc1.cisco.conductor.com" name="mc-1"
type="MC"/>

<component hostname="mcc1.cisco.conductor.com"
cmip="90.0.60.205" cmport="5222" cmipbak="90.0.60.206" cmportbak="5222"
name="mcc-1" snmpport="11162" type="MCC">

<managedomain>management.cisco.conductor.com</managedomain>
</component>

<component algo="db" hostname="svc.conductor.com"
name="sdns-svcjsm-1" subtype="JSM" isforsvc="1" type="SDNS">
<compid>jsm-1.cm-jsm-nonha-r25-service</compid>
</component>
</realm>

<realm adminip="90.0.60.205" ipmask="255.255.0.0"
adminport="7301" ip="90.0.60.205" mdns="on" port="7401" realmid="jsm-ha-r25-
mgmt" type="HAENABLED">
<component hostname="management.cisco.conductor.com"
name="jsm-1" type="JSM"/>
<component compport="5223" name="cm-1" port="5222"
svcip="90.0.60.205" svcipmask="255.255.0.0" type="CM"/>
<component name="sasl-1" type="SASL"/>
<component hostname="pubsub.service" name="pubsub-1"
type="PS"/>
<component algo="db" hostname="svc.conductor.com"
name="sdns-svcjsm-1" subtype="JSM" isforsvc="1" type="SDNS">
<compid>jsm-1.cm-jsm-nonha-r25-service</compid>
</component>
</realm>
</realms>
</node>

<node name="r25-mgmt-2" pref="SECONDARY" type="MGMT">
<realms>
<realm adminip="90.0.60.206" ipmask="255.255.0.0"
adminport="7300" ip="90.0.60.206" mdns="on" port="7400" realmid="bootstrap-
r25-mgmt-2" type="BOOTSTRAP">
<component hostname="mc2.cisco.conductor.com" name="mc-1"
type="MC"/>
<component hostname="mcc2.cisco.conductor.com"
cmip="90.0.60.206" cmport="5222" cmipbak="90.0.60.205" cmportbak="5222"
name="mcc-1" snmpport="11162" type="MCC">

<managedomain>management.cisco.conductor.com</managedomain>
</component>
<component algo="db" hostname="svc.conductor.com"
name="sdns-svcjsm-1" subtype="JSM" isforsvc="1" type="SDNS">
<compid>jsm-1.cm-jsm-nonha-r25-service</compid>
```

```
</component>
</realm>
<realm adminip="90.0.60.206" ipmask="255.255.0.0"
adminport="7301" ip="90.0.60.206" mdns="on" port="7401" realmid="jsm-ha-r25-
mgmt" type="HAENABLED">
    <component hostname="management.cisco.conductor.com"
name="jsm-1" type="JSM"/>
        <component compport="5223" name="cm-1" port="5222"
svcip="90.0.60.206" svcipmask="255.255.0.0" type="CM"/>
            <component name="sasl-1" type="SASL"/>
            <component hostname="pubsub.service" name="pubsub-1"
type="PS"/>
                <component algo="db" hostname="svc.conductor.com"
name="sdns-svcjsm-1" subtype="JSM" isforsvc="1" type="SDNS">
                    <compid>jsm-1.cm-jsm-nonha-r25-service</compid>
                </component>
            </realm>
        </realms>
    </node>
</nodes>
</zone>
</zones>
</cluster>
</clusters>
<datasource>
    <data dbtype="oracle-oci" service="wcs" platformuser="PLATFORM"
platformusersecret="PLATFORM" msginfrauser="MSGINFRA"
msginfrausersecret="MSGINFRA" ip="90.0.60.201" name="data1" port="1521"/>
</datasource>
</configuration>
```

Sample cluster.ha.postgres.R2-5.xml File

A sample cluster.ha.postgres.R2-5.xml file follows.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<configuration>
    <clusters>
        <cluster admin="admin" adminsecret="cisco123" clusterid="conductor25"
            clustersecret="cisco123" type="MSGINFRa">
            <zones>
                <zone datasource="data1" name="dbzone">
                    <adminjid>
                        <jid>admin@management.cisco.conductor.com</jid>
                        <secret>cisco123</secret>
                    </adminjid>
                    <nodes>
                        <node name="r25-db" type="INFRA">
                            <realms>
                                <realm adminip="90.0.60.201" ipmask="255.255.0.0"
                                    adminport="7300" ip="90.0.60.201" mdns="on" port="7400" realmid="bootstrap-
                                    r25-db" type="BOOTSTRAP"/>
                            </realms>
                        </node>
                    </nodes>
                </zone>
                <zone datasource="data1" name="clientzone">
                    <adminjid>
                        <jid>admin@management.cisco.conductor.com</jid>
                        <secret>cisco123</secret>
                    </adminjid>
                    <nodes>
                        <node name="r25-client-1" type="INFRA">
                            <realms>
                                <realm adminip="90.0.60.202" ipmask="255.255.0.0"
                                    adminport="7300" ip="90.0.60.202" mdns="on" port="7400" realmid="bootstrap-
                                    r25-client-1" type="BOOTSTRAP"/>
                                <realm adminip="90.0.60.202" ipmask="255.255.0.0"
                                    adminport="7301" ip="90.0.60.202" mdns="on" port="7401" realmid="cm-r25-
                                    client-1" type="HADISABLED">
                                    <component name="cmw-1" port="5280" svcip="90.0.60.202"
                                        svcipmask="255.255.0.0" port6="5280" svcip6="2001:da8:210::9000"
                                        svcip6prefixlen="64" type="CMW"/>
                            </realms>
                        </node>
                    </nodes>
                </zone>
            </zones>
        </cluster>
    </clusters>
</configuration>
```

Cluster File Examples

```

<component compport="5223" name="cm-1" port="5222"
svcip="90.0.60.202" svcipmask="255.255.0.0" compport6="5223" port6="5222"
svcip6="2001:da8:210::9000" svcip6prefixlen="64" type="CM"/>
    <component name="sasl-1" type="SASL"/>
</realm>
    <realm adminip="90.0.60.202" ipmask="255.255.0.0"
adminport="7302" ip="90.0.60.202" mdns="on" port="7402" realmid="jsm-ha-r25-
client" type="HAENABLED">
        <component hostname="cisco.conductor.com" name="jsm-1"
eb="sdns-cd-1.jsm-ha-r25-client"
rosternotifyurl="http://www.cisco.com/notify" msg="1" type="JSM"/>
        <component hostname="smm.svc.conductor.com" name="smm-1"
svmid="svm.svc.conductor.com" threadingpolicy="source" type="SMM"/>
        <component name="sdns-cd-1" subtype="CD" type="SDNS">
            <compid>cd-1.jsm-ha-r25-client</compid>
        </component>
        <component algo="db" hostname="svc.conductor.com"
name="sdns-svcjsm-1" subtype="JSM" isforsvc="1" type="SDNS">
            <compid>jsm-1.cm-jsm-nonha-r25-service</compid>
        </component>
    </realm>
</realms>
</node>
<node name="r25-client-2" type="INFRA">
    <realms>
        <realm adminip="90.0.60.203" ipmask="255.255.0.0"
adminport="7300" ip="90.0.60.203" mdns="on" port="7400" realmid="bootstrap-
r25-client-2" type="BOOTSTRAP"/>
        <realm adminip="90.0.60.203" ipmask="255.255.0.0"
adminport="7301" ip="90.0.60.203" mdns="on" port="7401" realmid="ps-r25-
client-2" type="HADISABLED">
            <component hostname="ps.conductor" name="pubsub-1"
type="PS"/>
        </realm>
        <realm adminip="90.0.60.203" ipmask="255.255.0.0"
adminport="7302" ip="90.0.60.203" mdns="on" port="7402" realmid="jsm-ha-r25-
client" type="HAENABLED">
            <component hostname="cisco.conductor.com" name="jsm-1"
eb="sdns-cd-1.jsm-ha-r25-client"
rosternotifyurl="http://www.cisco.com/notify" msg="1" type="JSM"/>
            <component hostname="smm.svc.conductor.com" name="smm-1"
svmid="svm.svc.conductor.com" threadingpolicy="source" type="SMM"/>
            <component name="sdns-cd-1" subtype="CD" type="SDNS">
                <compid>cd-1.jsm-ha-r25-client</compid>
            </component>
    </realms>
</node>

```

Appendix A

The cluster.xml Files

```
<component algo="db" hostname="svc.conductor.com"
name="sdns-svcjsm-1" subtype="JSM" isforsvc="1" type="SDNS">
    <compid>jsm-1.cm-jsm-nonha-r25-service</compid>
</component>
</realm>
</realms>
</node>
</nodes>
</zone>
<zone datasource="data1" name="svzone">
    <adminjid>
        <jid>admin@management.cisco.conductor.com</jid>
        <secret>cisco123</secret>
    </adminjid>
    <nodes>
        <node name="r25-service" type="INFRA">
            <realms>
                <realm adminip="90.0.60.204" ipmask="255.255.0.0"
adminport="7300" ip="90.0.60.204" mdns="on" port="7400" realmid="bootstrap-
r25-service" type="BOOTSTRAP"/>
                <realm adminip="90.0.60.204" ipmask="255.255.0.0"
adminport="7301" ip="90.0.60.204" mdns="on" port="7401" realmid="cm-jsm-
nonha-r25-service" type="HADISABLED">
                    <component name="cmw-1" port="5280" svcip="90.0.60.204"
svcipmask="255.255.0.0" isforsvc="1" type="CMW"/>
                    <component compport="5223" name="cm-1" port="5222"
svcip="90.0.60.204" svcipmask="255.255.0.0" isforsvc="1" type="CM"/>
                    <component name="sasl-1" type="SASL"/>
                    <component offline="0" bcc="svm.svc.conductor.com"
name="jsm-1" isforsvc="1" type="JSM"/>
                    <component hostname="smm.svc.conductor.com" name="smm-1"
svmid="svm.svc.conductor.com" threadingpolicy="id" type="SMM"/>
                    <component name="svcreader-1"
svmid="svm.svc.conductor.com" type="SVCVIEWER"/>
                    <component name="httpgw-1" cmip="90.0.60.204"
cmport="5222" jsmdomain="svc.conductor.com" jsmid="jsm-1.cm-jsm-nonha-r25-
service" type="HTTPGW"/>
                    <component hostname="svm.svc.conductor.com" name="svm-1"
type="SVM"/>
                    <component hostname="pubsub.virtual" name="pubsub-1"
type="PS"/>
                    <component algo="db" hostname="svc.conductor.com"
name="sdns-svcjsm-1" subtype="JSM" isforsvc="1" type="SDNS">
                        <compid>jsm-1.cm-jsm-nonha-r25-service</compid>
</component>
```

```

        </realm>
    </realms>
</node>
</nodes>
</zone>
<zone datasource="data1" name="mgmtzone">
    <adminjid>
        <jid>admin@management.cisco.conductor.com</jid>
        <secret>cisco123</secret>
    </adminjid>
    <nodes>
        <node name="r25-mgmt-1" type="MGMNT">
            <realms>
                <realm adminip="90.0.60.205" ipmask="255.255.0.0"
                    adminport="7300" ip="90.0.60.205" mdns="on" port="7400" realmid="bootstrap-
                    r25-mgmt-1" type="BOOTSTRAP">
                    <component hostname="mc1.cisco.conductor.com" name="mc-1"
                        type="MC"/>
                    <component hostname="mcc1.cisco.conductor.com"
                        cmip="90.0.60.205" cmport="5222" cmipbak="90.0.60.206" cmportbak="5222"
                        name="mcc-1" snmpport="11162" type="MCC">
                </realm>
                <realm adminip="90.0.60.205" ipmask="255.255.0.0"
                    adminport="7301" ip="90.0.60.205" mdns="on" port="7401" realmid="jsm-ha-r25-
                    mgmt" type="HAENABLED">
                    <component hostname="management.cisco.conductor.com"
                        name="jsm-1" type="JSM"/>
                    <component compport="5223" name="cm-1" port="5222"
                        svcip="90.0.60.205" svcipmask="255.255.0.0" type="CM"/>
                    <component name="sasl-1" type="SASL"/>
                    <component hostname="pubsub.service" name="pubsub-1"
                        type="PS"/>
                    <component algo="db" hostname="svc.conductor.com"
                        name="sdns-svcjsm-1" subtype="JSM" isforsvc="1" type="SDNS">
                        <compid>jsm-1.cm-jsm-nonha-r25-service</compid>
                    </component>
                </realm>
            </realms>
        </node>
    </nodes>
</zone>

```

Appendix A

The cluster.xml Files

```
</realms>
</node>
<node name="r25-mgmt-2" pref="SECONDARY" type="MGMT">
    <realms>
        <realm adminip="90.0.60.206" ipmask="255.255.0.0"
            adminport="7300" ip="90.0.60.206" mdns="on" port="7400" realmid="bootstrap-
            r25-mgmt-2" type="BOOTSTRAP">
            <component hostname="mc2.cisco.conductor.com" name="mc-1"
                type="MC"/>
            <component hostname="mcc2.cisco.conductor.com"
                cmip="90.0.60.206" cmport="5222" cmipbak="90.0.60.205" cmportbak="5222"
                name="mcc-1" snmpport="11162" type="MCC">
            <managedomain>management.cisco.conductor.com</managedomain>
                </component>
                <component algo="db" hostname="svc.conductor.com"
                    name="sdns-svcjsm-1" subtype="JSM" isforsvc="1" type="SDNS">
                    <compid>jsm-1.cm-jsm-nonha-r25-service</compid>
                </component>
            </realm>
            <realm adminip="90.0.60.206" ipmask="255.255.0.0"
                adminport="7301" ip="90.0.60.206" mdns="on" port="7401" realmid="jsm-ha-r25-
                mgmt" type="HAENABLED">
                <component hostname="management.cisco.conductor.com"
                    name="jsm-1" type="JSM"/>
                <component compport="5223" name="cm-1" port="5222"
                    svcip="90.0.60.206" svcipmask="255.255.0.0" type="CM"/>
                <component name="sasl-1" type="SASL"/>
                <component hostname="pubsub.service" name="pubsub-1"
                    type="PS"/>
                <component algo="db" hostname="svc.conductor.com"
                    name="sdns-svcjsm-1" subtype="JSM" isforsvc="1" type="SDNS">
                    <compid>jsm-1.cm-jsm-nonha-r25-service</compid>
                </component>
            </realm>
        </realms>
    </node>
</nodes>
</zone>
</zones>
</cluster>
</clusters>
<datasource>
```

Cluster File Examples

```
<data conductordb="platform" dbsecret="cisco123" dbsvrsuperps="cisco"  
dbuser="conductor" ip="90.0.60.201" msginfradb="msginfra" name="data1"  
port="5432"/>  
</datasource>  
</configuration>
```


B

How to Write an IDC File

Introduction

The IDC configuration file (cluster.xml) is an XML file which contains the configuration of a deployment design for a cluster. Use this appendix for information on how to write a correct IDC file.

In This Appendix

- Prepare the Datasource and the Database Nodes 156
- Determine the Zone Configuration 158

Prepare the Datasource and the Database Nodes

A PostgreSQL server or an external Oracle server must be available before any nodes can be configured. There should only be one database server definition in single cluster. This database server can be a standalone server or virtual machine (VM), which is dedicated for database service. It can also be a Virtual Storage Operating System (VSOS) server, which is shared with other functionalities. To prepare a datasource, the user should follow these guidelines:

- Create one database server node for each data source definition (“data” tag within the “datasource” tag).
 - Choose “Conductor with PostgreSQL” when generating the platformConfig.xml file for the database servers.
 - The server could be a dedicated database server.
 - There is only one bootstrap realm defined in the node.
 - The server could be a shared resource server with other functionalities installed.
 - There may be multiple database servers, which provide a separate database service per “data” tag in the “datasource” tag.

Example: An example of a dedicated database server follows:

```
<zone name='dbzone' datasource='data1'>
  <nodes>
    <node name='database1' type='SERVICE'>
      <realms>
        <realm realmid='databaseboot001' type='BOOTSTRAP'
          ip='192.168.1.11' port='7400' adminip='192.168.2.11'
          adminipmask='255.255.255.0' adminport='7300' mdns='on'>
        </realm>
      </realms>
    </node>
  </nodes>
</zone>
```

- Write a datasource key in the IDC file (cluster.xml) according to this example:

PostgreSQL:

```
<configuration>
    <datasource>
        <data name='data1' msginfradb='msginfra' conductordb='platform'
dbsvrsuperps='cisco' dbuser='conductor' dbsecret='cisco123'
ip='192.168.1.11' port='5432' />
    </datasource>
</configuration>
```

External Oracle:

```
<configuration>
    <datasource>
        <data name='data1' dbtype='oracle-oci' service='svc'
msginfrauser='msginfra' msginfrausersecret='msginfra'
platformuser='platform' platformusersecret='platform' ip='192.168.1.11'
port='1521' />
    </datasource>
</configuration>
```

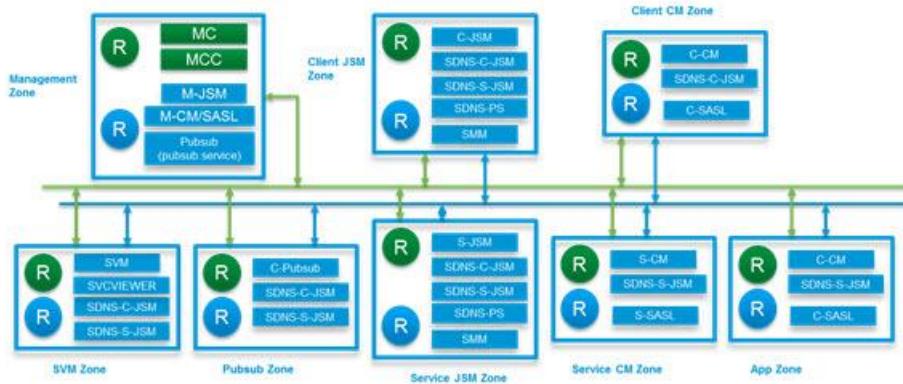
Notes:

- The details of the attributes of the “data” tag are found in *Data Source* (on page 103).
- Each “data” tag represents a database server.
- Be certain that the IP address represents the IP address of the database server.

Determine the Zone Configuration

Before you write the configuration for the nodes and realms, you first need to decide the zone configuration. A zone should be a node or server group in which all nodes or servers have the same functionalities.

The configuration of zones is very flexible according to the deployment topology of the cluster. There is no uniform configuration template for all deployments. The following sections provide some generic recommendations on all zones, as well as some specific design recommendations on the most-used types of zones.



Bootstrap Router

Each node/server has only one bootstrap router installed as the north-bound link for management traffic. The bootstrap router is started automatically when the server boots up. Most management commands, such as node/server configuration, JSM HA commands, running-state changes, and event reporting, pass through this dedicated link.

The bootstrap routers on the management node contain management-related components, such as MC and MCC.

```

<node name='database1' type='SERVICE'>
    <realms>
        <realm realmid='databaseboot001' type='BOOTSTRAP' ip='192.168.1.11' port='7400' adminip='192.168.2.11' adminipmask='255.255.255.0' adminport='7300' mdns='on'>
            </realm>
    </realms>
</node>

```

Administration JID

The administration JID tags define the administrators who can perform some privileged actions within the zone.

There must be at least one administrator JID named similarly to “555@\$management_domain” and a responding administrator JID password for all zones created by the MCC component. Here the “management_domain” is the value of the “managedomain” tag of the MCC component.

```
<adminjid>
    <jid>admin@conductor.cisco.com</jid>
    <secret>cisco123</secret>
</adminjid>
```

Database (DB) Zone

There must only be one PostgreSQL database server or external Oracle database server within the cluster. This server should be installed before the installation of any other servers.

The database server must have only one bootstrap router installed. Reference the example in the **Bootstrap Router** section, above.

```
<zone datasource="data1" name="genericdbzone">
    <adminjid>
        <jid>admin@management.conductor.cisco.com</jid>
    </adminjid>
    <nodes>
        <node name="vm-r2it-10" type="SERVICE">
            <realms>
                <realm adminip="90.0.60.209"
ipmask="255.255.0.0" adminport="7300" ip="90.0.60.209" mdns="on" port="7400"
realmid="bootstrap-vm-r2it-10" type="BOOTSTRAP"/>
            </realms>
        </node>
    </nodes>
</zone>
```

Client/Service Connection Manager (CM) Zone

The servers within the CM zone only contain the connection management service, which is the edge of the whole cluster. The connection management service supports both the native XMPP connection and the BOSH connection, which are provided by the CM and CMW components separately. A SDNS for JSM is used for balancing the load of JSM.

```
<node name='cmxzone1' type='SERVICE'>
    <realms>
        <realm realmid='cmxzoneboot001' type='BOOTSTRAP'
            ip='192.168.1.12' port='7400' adminip='192.168.2.12' ipmask='255.255.255.0'
            adminport='7300' mdns='on'>
            </realm>
        <realm realmid='cmxzone001'      type='HADISABLED'
            ip='192.168.1.12' port='7401' adminip='192.168.2.12' ipmask='255.255.255.0'
            adminport='7301' mdns='on'>
            <component type='SDNS' subtype='JSM' name='sdns-jsm-1'
                hostname='conductor.cisco.com' >
                <compid>jsm-1.jsmzone001</compid>
                <compid>jsm-1.jsmzone002</compid>
            </component>
            <component type='CM' name='cm-1'
                svcip='192.168.3.12' svcipmask='255.255.255.0' port='5222'
                compport='5223' />
                <component type='CM' name='cm-2'
                    svcip='192.168.3.12' svcipmask='255.255.255.0' port='5224'
                    compport='5225' />
                <component type='CMW' name='cmw-1'
                    svcip='192.168.3.12' svcipmask='255.255.255.0' port='5280' />
                <component type='SASL' name='sasl-1' />
            </realm>
        </realms>
    </node>
```

Client Jabber Session Manager (JSM) Zone

The servers within the JSM zone only contain the client session-management service, which is the home of the client session. The JSM zone also supports HA protection, which is enabled by the “type” attribute as set in HAENABLED. The following are examples for both Active and Standby servers/nodes configuration:

Active

```
<node name='jsmzone1' type='SERVICE' harestartperiod='1200' harestartcnt='5'
    hahlthchkintrvl='10' hahlthchkcnt='3'>
    <realms>
```

Determine the Zone Configuration

```
<realm realmid='jsmzoneboot001' type='BOOTSTRAP'
ip='192.168.1.14' port='7400' adminip='192.168.1.14' ipmask='255.255.255.0'
adminport='7300' mdns='on'>
</realm>

<realm realmid='jsmzone001'      type='HAENABLED'
ip='192.168.1.14' port='7401' adminip='192.168.2.14' ipmask='255.255.255.0'
adminport='7301' mdns='on'>
<component type='JSM' name='jsm-1' />
<component type='SMM' name='smm-1'
hostname='smm.conductor.cisco.com' svmid='svm.conductor.cisco.com' />
<component type='SDNS' subtype='JSM' name='sdns-jsm-1' hostname='conductor.cisco.com' >
<compid>jsm-1.jsmzone001</compid>
<compid>jsm-1.jsmzone002</compid>
</component>
</realm>
<realm realmid='jsmzone002'      type='HAENABLED'
ip='192.168.1.14' port='7402' adminip='192.168.2.14' ipmask='255.255.255.0'
adminport='7302' mdns='on'>
<component type='JSM' name='jsm-1' />
<component type='SMM' name='smm-1'
hostname='smm.conductor.cisco.com' svmid='svm.conductor.cisco.com' />
<component type='SDNS' subtype='JSM' name='sdns-jsm-1' hostname='conductor.cisco.com' >
<compid>jsm-1.jsmzone001</compid>
<compid>jsm-1.jsmzone002</compid>
</component>
</realm>
</realms>
</node>
<node name='jsmzone2' type='SERVICE' harestartperiod='1200' harestartcnt='5'
hahlthchkintrvl='10' hahlthchkcnt='3'>
<realms>
<realm realmid='jsmzoneboot005' type='BOOTSTRAP'
ip='192.168.1.15' port='7400' adminip='192.168.1.15' ipmask='255.255.255.0'
adminport='7300' mdns='on'>
</realm>
<realm realmid='jsmzone001'      type='HAENABLED'
ip='192.168.1.15' port='7401' adminip='192.168.2.15' ipmask='255.255.255.0'
adminport='7301' mdns='on'>
<component type='JSM' name='jsm-1' />
<component type='SMM' name='smm-1'
hostname='smm.conductor.cisco.com' svmid='svm.conductor.cisco.com' />
<component type='SDNS' subtype='JSM' name='sdns-jsm-1' hostname='conductor.cisco.com' >
```

Appendix B

How to Write an IDC File

```
<compid>jsm-1.jsmzone001</compid>
<compid>jsm-1.jsmzone002</compid>
</component>
</realm>
<realm realmid='jsmzone002'      type='HAENABLED'
ip='192.168.1.15' port='7402' adminip='192.168.2.15' ipmask='255.255.255.0'
adminport='7302' mdns='on'>
<component type='JSM' name='jsm-1' />
<component type='SMM' name='smm-1'
hostname='smm.conductor.cisco.com' svmid='svm.conductor.cisco.com' />
<component type='SDNS' subtype='JSM' name='sdns-jsm-1'
hostname='conductor.cisco.com' >
<compid>jsm-1.jsmzone001</compid>
<compid>jsm-1.jsmzone002</compid>
</component>
</realm>
</realms>
</node>
```

Standby

```
<node name='jsmzone2' type='SERVICE' reload='50' harestartperiod='1200'
harestartcnt='5' hahlthchkintrvl='10' hahlthchkcnt='3'>
<realms>
<realm realmid='jsmzoneboot005' type='BOOTSTRAP' ip='192.168.1.15'
port='7400' adminip='192.168.1.15' adminipmask='255.255.255.0'
adminport='7300' mdns='on'>
</realm>
<realm realmid='jsmzone001'      type='HAENABLED' ip='192.168.1.15'
port='7401' adminip='192.168.2.15' adminipmask='255.255.255.0'
adminport='7301' mdns='on'>
<component type='JSM' name='jsm-1' />
<component type='SDNS' subtype='JSM' name='sdns-jsm-1'
hostname='conductor.cisco.com' >
<compid>jsm-1.jsmzone001</compid>
<compid>jsm-1.jsmzone002</compid>
</component>
</realm>
<realm realmid='jsmzone002'      type='HAENABLED' ip='192.168.1.15'
port='7402' adminip='192.168.2.15' adminipmask='255.255.255.0'
adminport='7302' mdns='on'>
<component type='JSM' name='jsm-1' />
<component type='SDNS' subtype='JSM' name='sdns-jsm-1'
hostname='conductor.cisco.com' >
<compid>jsm-1.jsmzone001</compid>
```

```

        <compid>jsm-1.jsmzone002</compid>
    </component>
</realm>
</realms>
</node>

```

The JSM HA is in 1+1 active/standby mode. This means that there are two servers that have the identical Videoscape Control Suite configuration (realms/components, etc), except for the bootstrap router and platform level-configuration, such as IP address and port. Normally, the realms within the JSM zone should contain only one JSM component. There can be multiple realms within one server or node. A SDNS for JSM is used for balancing the load among multiple JSMs. If SDNS-JSM is configured with the XMPP domain name as the hostname attribute, the hostname of the JSM components should be deleted.

Service Jabber Session Manager (JSM) Zone

The Service JSM Zone is configured for service virtualization. The JSM subtype SDNS component in the Service JSM Zone should be configured for the db mapping algorithm.

```

<node name='jsmzone1' type='SERVICE' reload='50' harestartperiod='1200'
harestartcnt='5' hahlthchkintrvl='10' hahlthchkcnt='3'>

    <realms>

        <realm realmid='jsmzoneboot001' type='BOOTSTRAP'
ip='192.168.1.14' port='7400' adminip='192.168.1.14'
adminipmask='255.255.255.0' adminport='7300' mdns='on'>
            </realm>
            <realm realmid='jsmzone001'      type='HAENABLED'
ip='192.168.1.14' port='7401' adminip='192.168.2.14'
adminipmask='255.255.255.0' adminport='7301' mdns='on'>
                <component type='JSM' name='jsm-1' />
                <component type='SMM' name='smm-1'
hostname='smm.conductor.cisco.com' svmid='svm.conductor.cisco.com' />
                <component type='SDNS' subtype='JSM' name='sdns-jsm-1'
hostname='conductor.cisco.com' algo='db'>
                    <compid>jsm-1.jsmzone001</compid>
                </component>
            </realm>
            <realm realmid='jsmzone002'      type='HAENABLED'
ip='192.168.1.14' port='7402' adminip='192.168.2.14'
adminipmask='255.255.255.0' adminport='7302' mdns='on'>
                <component type='JSM' name='jsm-1' />
                <component type='SMM' name='smm-1'
hostname='smm.conductor.cisco.com' svmid='svm.conductor.cisco.com' />
                <component type='SDNS' subtype='JSM' name='sdns-jsm-1'
hostname='conductor.cisco.com' algo='db'>

```

Appendix B

How to Write an IDC File

```
<compid>jsm-1.jsmzone001</compid>
</component>
</realm>
</realms>
</node>

<node name='jsmzone2' type='SERVICE' reload='50' harestartperiod='1200'
harestartcnt='5' hahlthchkintrvl='10' hahlthchkcnt='3'>
<realms>
<realm realmid='jsmzoneboot005' type='BOOTSTRAP'
ip='192.168.1.15' port='7400' adminip='192.168.1.15'
adminipmask='255.255.255.0' adminport='7300' mdns='on'>
</realm>
<realm realmid='jsmzone001' type='HAENABLED'
ip='192.168.1.15' port='7401' adminip='192.168.2.15'
adminipmask='255.255.255.0' adminport='7301' mdns='on'>
<component type='JSM' name='jsm-1' />
<component type='SMM' name='smm-1'
hostname='smm.conductor.cisco.com' svmid='svm.conductor.cisco.com' />
<component type='SDNS' subtype='JSM' name='sdns-jsm-1'
hostname='conductor.cisco.com' algo='db'>
<compid>jsm-1.jsmzone001</compid>
</component>
</realm>
<realm realmid='jsmzone002' type='HAENABLED'
ip='192.168.1.15' port='7402' adminip='192.168.2.15'
adminipmask='255.255.255.0' adminport='7302' mdns='on'>
<component type='JSM' name='jsm-1' />
<component type='SMM' name='smm-1'
hostname='smm.conductor.cisco.com' svmid='svm.conductor.cisco.com' />
<component type='SDNS' subtype='JSM' name='sdns-jsm-1'
hostname='conductor.cisco.com' algo='db'>
<compid>jsm-1.jsmzone001</compid>
</component>
</realm>
</realms>
</node>
```

Service Virtualization Manager (SVM) Zone

The servers within the SVM zone contain the service virtualization manager and service viewer component. An SDNS for JSM is used for balancing the load of JSM.

```
<node name='svmzone1' type='SERVICE'>
<realms>
```

```

<realm realmid='svmzoneboot001' type='BOOTSTRAP'
ip='192.168.1.12' port='7400' adminip='192.168.2.12'
adminipmask='255.255.255.0' adminport='7300' mdns='on'>
</realm>

<realm realmid='svmzone001'      type='HADISABLED'
ip='192.168.1.12' port='7401' adminip='192.168.2.12'
adminipmask='255.255.255.0' adminport='7301' mdns='on'>
<component name="svcviewer-1" type="SVCVIEWER"/>
<component name="svm-1" type="SVM"/>
<component hostname="svc.conductor.com" name="sdns-svcjsm-1"
subtype="JSM" type="SDNS">
<compid>jsm-1.servicejsm-ha-router-1</compid>
<compid>jsm-1.servicejsm-ha-router-2</compid>
</component>
</realm>
</realms>
</node>

```

Management Zone

The management zone includes all management-related functions. It usually includes the following components:

- One MC component
- One MCC component
- One management JSM component, which is used by administrators and MCC
- One management CM component, which is used by administrators and MCC
- One pubsub component, which is used by SNMP trap reporting. The hostname of this pubsub component (or the corresponding SDNS) should be “pubusb.service.” The hostname should NEVER be used by any other components.

In the management HA environment, a “pref” attribute is configured to point to the node HA type.

```

<node hahlthchkcnt="3" hahlthchkigncnt="3" hahlthchkintrvl="10"
harestartcnt="5" harestartperiod="1200" name="vm-13" reload="50"
type="MGMT">
<realms>
<realm adminip="20.0.0.13" adminipmask="255.0.0.0"
adminport="7300" ip="20.0.0.13" mdns="on" port="7400" realmid="bootstrap-vm-
13" type="BOOTSTRAP">
<component hostname="mc1.cisco.conductor.com"
name="mc-1" type="MC"/>
<component cmip="20.0.0.13" cmippak="20.0.0.14"
cmport="5222" cmportbak="5222" name="mcc-1" snmpport="11162" type="MCC">

```

Appendix B

How to Write an IDC File

```
<manageddomain>management.cisco.conductor.com</manageddomain>
    </component>
    </realm>
        <realm adminip="20.0.0.13" adminipmask="255.0.0.0"
adminport="7301" ip="20.0.0.13" mdns="on" port="7401" realmid="mgmt-ha-
router-1" type="HAENABLED">
            <component hostname="management.cisco.conductor.com"
name="jsm-1" type="JSM"/>
                <component compport="5223" name="cm-1" port="5222"
svcip="20.0.0.13" svcipmask="255.0.0.0" type="CM"/>
                    <component name="sasl-1" type="SASL"/>
                    <component hostname="pubsub.service" name="pubsub-1"
type="PS"/>
            </realm>
        </realms>
    </node>
<node hahlthchkcnt="3" hahlthchkigncnt="3" hahlthchkintrvl="10"
harestartcnt="5" harestartperiod="1200" name="vm-14" pref="SECONDARY"
reload="50" type="MGMT">
    <realms>
        <realm adminip="20.0.0.14" adminipmask="255.0.0.0"
adminport="7300" ip="20.0.0.14" mdns="on" port="7400" realmid="bootstrap-vm-
14" type="BOOTSTRAP">
            <component hostname="mc2.cisco.conductor.com"
name="mc-1" type="MC"/>
            <component cmip="20.0.0.14" cmippak="20.0.0.13"
cmport="5222" cmportbak="5222" name="mcc-1" snmpport="11162" type="MCC"/>
    <manageddomain>management.cisco.conductor.com</manageddomain>
        </component>
        </realm>
    </realms>
    <realm adminip="20.0.0.14" adminipmask="255.0.0.0"
adminport="7301" ip="20.0.0.14" mdns="on" port="7401" realmid="mgmt-ha-
router-1" type="HAENABLED">
        <component hostname="management.cisco.conductor.com"
name="jsm-1" type="JSM"/>
            <component compport="5223" name="cm-1" port="5222"
svcip="20.0.0.14" svcipmask="255.0.0.0" type="CM"/>
            <component name="sasl-1" type="SASL"/>
            <component hostname="pubsub.service" name="pubsub-1"
type="PS"/>
        </realm>
    </realms>
</node>
```

App Zone

The app zone includes service-related nodes with a service cop file installation. The following components should be included:

- A XMPP Bootstrap router
- A XMPP Service router
 - CM service
 - SASL service
 - SDNS-Service-JSM service

The service located on a local node in the app zone connects to a local CM for access into the Conductor Msginfra.

The Default Configuration

If no cluster.xml file is provided and the platform type is chosen as “Videoscape Control Suite with PostgreSQL”, the installer should create a default installation based upon the current configuration of the host/node. The following is the information for a default installation.

The default installation will include:

- Database
- Router
- JSM
- CM (XMPP)
- CMW (BOSH)
- Pubsub
- SASL

The default installation has the following configuration:

- The JSM Domain is the fully qualified domain name (FQDN) of the server.
- The Admin JID is admin@\$FQDN.
- The hostname of pubsub is “pubsub.\$FQDN”.
- The web controller can be accessed via https://\$ip:7300.
- The database Ip/port is \$IP/5432.
- The Msginfra database (name/uid/pid) is msginfra/conductor/cisco123.
- The Videoscape Control Suite database (name/uid/pid) is conductor/conductor/cisco123.

**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

This document includes various trademarks of Cisco Systems, Inc. Please see the Notices section of this document for a list of the Cisco Systems, Inc., trademarks used in this document.

Product and service availability are subject to change without notice.

© 2013 Cisco and/or its affiliates. All rights reserved.

June 2013

Part Number OL-27702-03