Installation Guide for Cisco Network Registrar

Software Release 7.2
August 2011

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-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-20608-01

Cisco Network Registrar Installation Guide

CONTENTS

Preface v

Cisco Network Registrar Documentation v

Obtaining Documentation, Obtaining Support, and Security Guidelines vi

CHAPTER 1 **Overview** 1-1

About Cisco Network Registrar 1-1

System Requirements 1-2

Installation Modes 1-4

License Files 1-4

Backup Software and Virus Scanning Guidelines 1-4

Modifying ACLs in Windows Installations 1-5

Server Event Logging 1-5

Running Performance Monitoring Software on Windows 1-6

Running Other Protocol Servers 1-6

CHAPTER 2 **Installing and Upgrading Cisco Network Registrar** 2-1

Checklist 2-1

Before You Begin 2-2

Obtaining Cisco Network Registrar License Files 2-2

Installation and Upgrade Procedure 2-3

Upgrade Considerations 2-3

Upgrading on Windows 2-4

Upgrading on Solaris/Linux 2-5

Installing Cisco Network Registrar 7.2 2-5

Reverting to Earlier Product Version 2-11

Starting Cisco Network Registrar 2-12

Starting and Stopping Servers 2-13

Starting and Stopping Servers on Windows 2-13

Starting and Stopping Servers on Solaris or Linux 2-14

Moving an Installation to a New Machine 2-14

Troubleshooting the Installation 2-15

Uninstalling Cisco Network Registrar 2-16

Uninstalling on Windows 2-16

Uninstalling on Solaris 2-16
Uninstalling on Linux 2-17

CHAPTER 3 **Installing and Upgrading Cisco Network Registrar Virtual Appliance** 3-1

System Requirements 3-1
Installing and Configuring Cisco Network Registrar Virtual Appliance 3-2
Preparing to Deploy Cisco Network Registrar Virtual Appliance 3-2
Deploying Cisco Network Registrar Virtual Appliance 3-3
Booting and Configuring Cisco Network Registrar Virtual Appliance 3-5
Configuring Cisco Network Registrar 3-7
Configuring Cisco Network Registrar with CLI on Virtual Appliance 3-8
Configuring Virtual Appliance to Automatically Power Up 3-8
Upgrading Cisco Network Registrar Virtual Appliance 3-9
Upgrading Cisco Network Registrar Installation to run on Cisco Network Registrar Virtual Appliance 3-9
Upgrading Cisco Network Registrar Virtual Appliance Operating System 3-10
Managing Cisco Network Registrar Virtual Appliance 3-12

APPENDIX A **Performing a Silent Installation** A-1

APPENDIX B **Lab Evaluation Installations** B-1

Installing Cisco Network Registrar in a Lab B-1
Testing the Lab Installation B-1
Uninstalling in a Lab Environment B-2

APPENDIX C **Enhancing Security for Web UI** C-1

INDEX

Preface

This guide describes how to install Cisco Network Registrar Release 7.2 on the supported operating systems: Windows, Solaris, and Linux. It is written for the system administrators who will be installing the software, and assumes that you understand your site configuration and the basic steps for installing the software. For information on configuring and managing Cisco Network Registrar, see the *User Guide for Cisco Network Registrar.*

The guide is organized into the following chapters and appendixes:

Chapter 1	Overview	Introduces Cisco Network Registrar and provides critical system information that must be read before installing the software.
Chapter 2	Installing and Upgrading Cisco Network Registrar	Describes how to install or upgrade Cisco Network Registrar; and how to uninstall it, stop and start servers, and troubleshoot the installation.
Chapter 3	Installing and Upgrading Cisco Network Registrar Virtual Appliance	Describes how to install or upgrade Cisco Network Registrar Virtual Appliance.
Appendix A	Performing a Silent Installation	Explains how to perform a silent installation, upgrade, or uninstallation of the Cisco Network Registrar product.
Appendix B	Lab Evaluation Installations	Explains how to install, upgrade, or uninstall Cisco Network Registrar if it is being used in a lab environment.
Appendix C	Enhancing Security for Web UI	Explains how to enhance the security level for Web UI.

Cisco Network Registrar Documentation

The Cisco Network Registrar 7.2 documentation set consists of:

- *Release Notes for Cisco Network Registrar Release 7.2*
- *User Guide for Cisco Network Registrar Release 7.2*
- *Quick Start Guide for Cisco Network Registrar Release 7.2*

- *Installation Guide for Cisco Network Registrar Release 7.2*
- *Command Reference Guide for Cisco Network Registrar Release 7.2*
- *Documentation Guide for Cisco Network Registrar Release 7.2*
- *Third Party and Open Source Licenses and Notices for Cisco Network Registrar Release 7.2*
- *Online help as part of the Cisco Network Registrar web UI application.*

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 1

Overview

This guide describes how to install Cisco Network Registrar Release 7.2 on Windows, Solaris, and Linux operating systems, and how to install the Cisco Network Registrar Virtual Appliance. You can also see the following documents for important information about configuring and managing Cisco Network Registrar:

- For configuration and management procedures for Cisco Network Registrar and Cisco Network Registrar Virtual Appliance, see the *User Guide for Cisco Network Registrar.*
- For details about commands available through the command line reference (CLI), see the *Command Reference Guide for Cisco Network Registrar*.

About Cisco Network Registrar

Cisco Network Registrar is a network server suite that automates managing enterprise IP addresses. It provides a stable infrastructure that increases address assignment reliability and efficiency. It includes the following servers (see Figure 1-1 on page 1-2):

- Dynamic Host Configuration Protocol (DHCP)
- Domain Name System (DNS)
- Router Interface Configuration (RIC)
- Simple Network Management Protocol (SNMP)
- Trivial File Transfer Protocol (TFTP)

You can control these servers by using the Cisco Network Registrar web-based user interface (web UI) or the command line interface (CLI). These user interfaces can also control server clusters that run on different platforms.

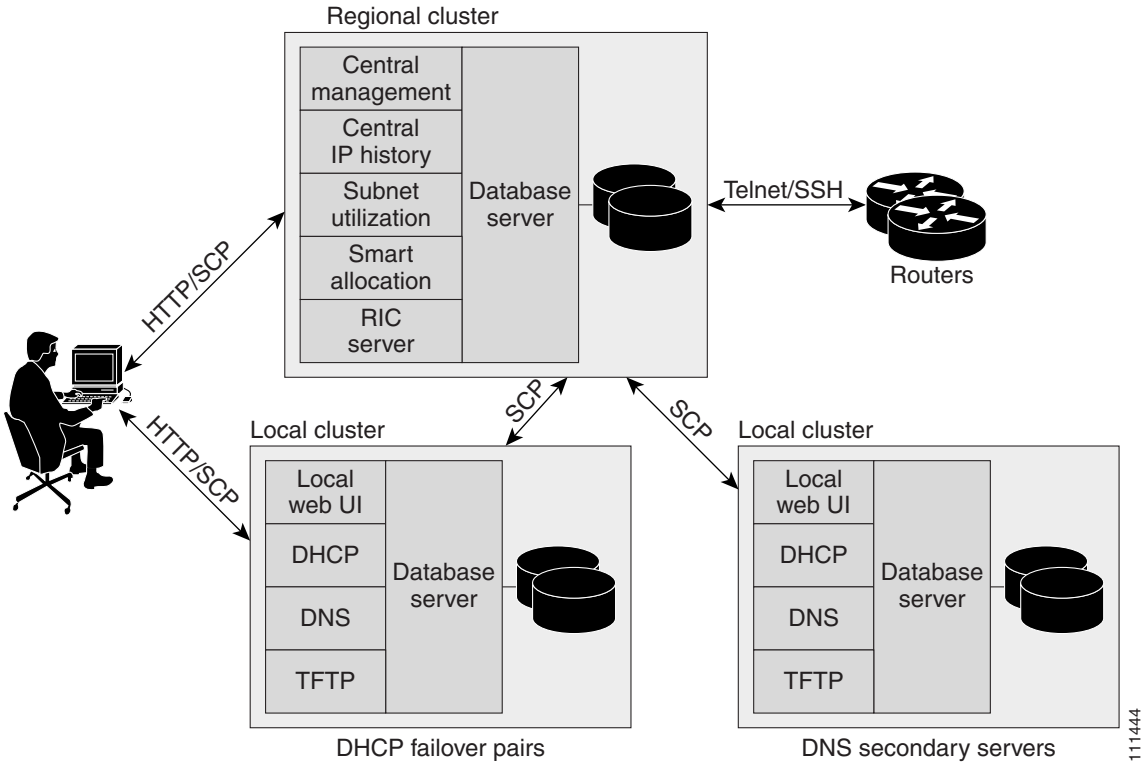
You can install Cisco Network Registrar in either local or regional mode:

- Local mode is used for managing local cluster protocol servers.
- Regional mode is used for managing multiple local clusters through a central management model.

A regional cluster centrally manages local cluster servers and their address spaces. The regional administrator can perform the following operations:

- Push and pull configuration data to and from the local DNS and DHCP servers.
- Obtain subnet utilization and IP lease history data from the local clusters.
- Manage the router interface configuration (RIC) server that integrates with cable modem termination systems (CMTSs) directly from the regional cluster.

Figure 1-1 Cisco Network Registrar User Interfaces and the Server Cluster



System Requirements

Review the system requirements before installing the Cisco Network Registrar 7.2 software:

- Java—You must have the Java Runtime Environment (JRE) 5.0 (1.5.0_06) or later, or the equivalent Java Development Kit (JDK) installed on your system. (The JRE is available from Oracle on its website.)
- Operating system—We recommend that your Cisco Network Registrar machine run on the Windows, Solaris, or Linux operating systems as described in Table 1-1 on page 1-3. Cisco Network Registrar must run on 32-bit or 64-bit operating systems.

Note Cisco Network Registrar applications are 32-bit applications and the system should support 32-bit applications (Java JRE/JDK, OpenLDAP library (for RH)).

- User Interface—Cisco Network Registrar currently includes two user interfaces: a web UI and a CLI:
  - The web UI runs on Microsoft Internet Explorer 7.1 and 8.0, Mozilla Firefox 3.0 and 3.5, and requires JRE 5.0 [1.5.0_06].
  - The CLI runs in a Windows, Solaris, or Linux command window.

Tip Include a network time service in your configuration to avoid time differences between the local and regional clusters. This method ensures that the aggregated data at the regional server appears consistently.

Table 1-1 Cisco Network Registrar Server Minimum Requirements

Component	Operating System		
	Solaris[1]	**Linux**	**Windows**
OS version[2]	Solaris 10[3]	• Red Hat Enterprise Linux ES 5.0[4]	Windows Server 2008 R2[4]
Disk space[5]	2 x 73/146 SAS[6] drives	With basic DHCP and optimal hardware configuration: • SATA[7] drives with 7500 RPM drive > 500 leases/second • SAS drives with 15K RPM drive > 1000 leases/second Recommended hard drive—146 GB	
Memory[8]	16 GB	Small networks—4 GB, Average networks—8 GB, or Large networks—16 GB	

1. Solaris support is restricted to Solaris Sparc.
2. Cisco Network Registrar must run on 32-bit or 64-bit operating systems.
3. Cisco Network Registrar 7.2 supports 128-KB block sizes in the Solaris 10 ZFS.
4. Cisco Network Registrar 7.2 supports running in a VMWARE (ESX Server 3.5) and LDOM environment for Red Hat Enterprise Linux ES 5.0, and Windows Server 2008 R2. Cisco Network Registrar 7.2 supports running in Cisco Unified Computing System (CUCS) and Sun Sparc Enterprise T5220.
5. Higher I/O bandwidth usually results in higher average leases per second.
6. Serial Attached SCSI.
7. Serial Advanced Technology Attachment (Serial ATA).
8. Faster CPU and more memory typically result in higher peak leases per second.

Note If you are upgrading from an earlier version of Cisco Network Registrar to Cisco Network Registrar 7.2, on the Solaris platform, make sure you upgrade the Solaris version as mentioned in "Installation and Upgrade Procedure" section on page 2-3.

Installation Modes

The modes of installation that exist for the local and regional clusters are new installations and upgrades from a previous version. These installations or upgrades are performed by using operating system-specific software installation mechanisms:

- Windows—InstallShield setup program
- Solaris—**pkgadd** command
- Linux—**install_cnr** script that uses RPM Package Manager (RPM)

License Files

Cisco Network Registrar uses the FLEXlm licensing tool. Your license file defines the features of Cisco Network Registrar to which you have access. When you install the software, you are prompted to provide the name of the license file and its location. You can give any name to the license file. You must specify this file name while you install Cisco Network Registrar.

A Cisco Network Registrar license file gives you the right to manage a specified number of IP addresses. A single license covers both IPv4 and IPv6 nodes. For example, to manage 24,000 IPv4 nodes and 10,000 IPv6 nodes in a local cluster, you must purchase an ip-node license that covers 34,000 total nodes.

This method also applies on a regional server. With a regional server, however, you must aggregate the licensed nodes from all managed local clusters. Consider the following scenario in which the regional server manages three local clusters:

- local cluster *A* has 24,000 IPv4 nodes and 10,000 IPv6 nodes
- local cluster *B* has 2,000 IPv4 nodes and 12,000 IPv6 nodes
- local cluster *C* has 48,000 IPv4 nodes and 1,000 IPv6 nodes

The regional cluster must have an license that covers 97,000 total nodes.

To learn about obtaining the license files for Cisco Network Registrar, see "Obtaining Cisco Network Registrar License Files" section on page 2-2.

Backup Software and Virus Scanning Guidelines

If you have automatic backup or virus scanning software enabled on your system, exclude the Cisco Network Registrar directories and their subdirectories from being scanned. If they are not excluded, file locking issues can corrupt the databases or make them unavailable to the Cisco Network Registrar processes. If you are installing on the default locations, exclude the following directories and their subdirectories:

Note In this documentation set, when *install-path* is used, it refers to all or part of the installation paths that were specified when installing Cisco Network Registrar.
As an example using the Solaris and Linux default local cluster paths of /opt/nwreg2/local and /var/nwreg2/local, the *install-path* may represent these paths or just the /opt/nwreg2 or /var/nwreg2 portion.

- Windows—

  install-path\data (for example, C:\NetworkRegistrar\Local\data and C:\Network Registrar\Regional\data)
  install-path\logs (for example, C:\NetworkRegistrar\Local\logs and C:\Network Registrar\Regional\logs)

- Solaris and Linux—

  install-path/data (for example, /var/nwreg2/local/data and /var/nwreg2/regional/data)
  install-path/logs (for example, /var/nwreg2/local/logs and /var/nwreg2/regional/logs)

Modifying ACLs in Windows Installations

The Cisco Network Registrar installation program for Windows does not try to modify ACLs to restrict access to installed files and directories. If you want to restrict access to these files and directories, use the native Microsoft utilities—**cacls** and **icacls**—to manually change file and directory permissions.

If you decide to manually change ACLs, we recommend that you control the settings so that the contents of the entire installation area are read-only to everyone except those in the Administrators system group.

The following files and sub directories contain data that you may want only the Administrators system group to access:

- *installdir***conf\cnr.conf**
- *installdir***tomcat\conf\server.xml**
- *installdir***conf\priv**
- *installdir***data**

Modifying the ACLs is strictly optional, and Cisco Network Registrar will function normally without making any changes to them. See documentation supplied by Microsoft for information about how to use the **cacls** and **icacls** utilities.

Server Event Logging

System activity begins logging when you start Cisco Network Registrar. The server maintains all the logs by default in the following directories:

- Windows—Local cluster: C:\NetworkRegistrar\Local\logs;
  Regional cluster: C:\NetworkRegistrar\Regional\logs
- Solaris and Linux—Local cluster: /var/nwreg2/local/logs;
  Regional cluster: /var/nwreg2/regional/logs

  To monitor the logs, use the **tail -f** command.

Caution In Windows, to avoid losing the most recent system Application Event Log entries if the Event Log fills up, use the Event Viewer system application and check the **Overwrite Events as Needed** check box in Event Log Settings for the Application Log. If the installation process detects that this option is not set properly, it displays a warning message advising corrective action.

Running Performance Monitoring Software on Windows

On Windows systems if you uninstall Cisco Network Registrar and try to remove the associated data directories while having software installed that integrates with the Windows Performance Monitor, the software might take possession of certain shared libraries. This action prevents you from removing these files from the Cisco Network Registrar folder and the directory itself. To keep this from happening:

1. Stop the service that is associated with the performance monitoring software.
2. Delete the Network Registrar folder.
3. Restart the service.

Running Other Protocol Servers

You cannot run the Cisco Network Registrar DNS, DHCP, or TFTP servers concurrently with any other DNS, DHCP, and TFTP servers. If the Cisco Network Registrar installation process detects that a conflict exists, it displays a warning message.

On Windows systems, use one of the following methods to change the configuration from the Service Control Manager:

- Change the Microsoft servers from a Startup Type of Automatic to Manual or Disabled.
- Stop the Cisco Network Registrar protocol server that conflicts with the Microsoft protocol server by using the Stop function in one of the user interfaces.

If you want to disable a protocol server and prevent the Cisco Network Registrar server from starting automatically after a system reboot, use the **server** {**dns** | **dhcp** | **tftp**} **disable start-on-reboot** command in the CLI.

CHAPTER 2

Installing and Upgrading Cisco Network Registrar

This chapter describes how to install Cisco Network Registrar 7.2 on Windows, Solaris, or Linux systems. It includes the following sections:

- Checklist
- Before You Begin
- Obtaining Cisco Network Registrar License Files
- Installation and Upgrade Procedure
- Starting Cisco Network Registrar
- Starting and Stopping Servers
- Moving an Installation to a New Machine
- Troubleshooting the Installation
- Uninstalling Cisco Network Registrar

Checklist

Before you perform the installation or upgrade, ensure that you are prepared by reviewing this checklist:

- Does my operating system meet the minimum requirements to support Cisco Network Registrar 7.2? (See the "System Requirements" section on page 1-2.)
- Does my hardware meet the minimum requirements? (See the "System Requirements" section on page 1-2.)
- If necessary, have I excluded Cisco Network Registrar directories and subdirectories from virus scanning? (See the "Backup Software and Virus Scanning Guidelines" section on page 1-4.)
- On Windows, are other applications closed, including any virus-scanning or automatic-backup software programs? Is the Debugger Users group included in the Local Users and Groups?
- Do I have the proper software license? (See the "License Files" section on page 1-4.)
- Am I authorized for the administrative privileges needed to install the software?
- Does the target installation server have enough disk space?
- Is this a new installation or an upgrade?
- Is the cluster mode of operation regional or local?

- Is this a full or client-only installation?
- Is the Java Runtime Environment (JRE) 5.0 (1.5.0_06) or later, or the equivalent Java Development Kit (JDK), installed on the system? If so, where?
- Should the web UI use an HTTP or HTTPS connection, or both?
- Am I upgrading from an earlier version of Cisco Network Registrar? If so:
  - Are there any active user interface sessions?
  - Is my database backed up?
  - Is my Cisco Network Registrar task list empty?
  - Am I upgrading from a supported version (Cisco Network Registrar 6.3 and later)?
  - Do I have the correct cnr_mcdexport tool?

Before You Begin

Verify that you are running a supported operating system and that your environment meets all other current system requirements (see the "System Requirements" section on page 1-2).

If you are running an unsupported operating system, back up your Cisco Network Registrar data and upgrade your operating system before installing this latest release.

To upgrade the operating system:

Step 1 Use the currently installed Cisco Network Registrar release to complete any configuration changes in progress, so that the existing database is consistent before you perform the upgrade.

Step 2 Ensure that no pending database tasks result from recent edits. You can confirm that the task lists are empty by viewing the CCM and MCD Tasks pages under the Administration menu in the web UI. Wait until both lists are empty before proceeding with the update.

Step 3 Back up your database. The installation program tries to detect configuration data from an earlier installation and will upgrade the data.

Step 4 Upgrade your operating system.

Obtaining Cisco Network Registrar License Files

When you purchase Cisco Network Registrar 7.2, you receive a FLEXlm license file in an e-mail attachment from Cisco, after you register the software.

You must copy the license file to a directory on the Cisco Network Registrar target machine before you attempt to install the software. Store the license file in any directory on the machine. The installation process asks you for the location of the license file.

To obtain a license file:

Step 1 Read the Software License Claim Certificate document packaged with the software.

Step 2 Note the Product Authorization Key (PAK) number printed on the certificate.

Step 3 Log in to one of the Web sites described on the certificate, and follow the registration instructions. The PAK number is required for the registration process.

You should receive the license file through e-mail within one hour of registration.

A typical license file might look like the following example:

```
FEATURE ip-node cisco 1.000 1-feb-2010 uncounted VENDOR_STRING=1000 \
    HOSTID=ANY SN=CNR12222006113344 NOTICE="<LicFileID>licenseFileName1 </LicFileID>
    SIGN=46764487EXMPL1
FEATURE ip-node cisco 1.000 3-mar-2037 uncounted VENDOR_STRING=50000 HOSTID=ANY \
    SN=CNR09082006112233 SIGN=776AB544EXMPL2
INCREMENT ipv6-node cisco 1.000 3-mar-2037 uncounted VENDOR_STRING=500000 HOSTID=ANY \
    SN=CNR09092006112233 SIGN=776AB544ZEXMPL3
```

Installation and Upgrade Procedure

The procedure is essentially the same for a new installation or upgrade; except that the upgrade requires a few additional steps, as explained in the following sections.

Upgrade Considerations

Cisco Network Registrar 7.2 supports direct upgrades from 6.3 (Linux, Solaris, and Windows), and later.

Cisco Network Registrar no longer supports the Red Hat 4.0, 3.0, and Solaris 8 and 9 operating systems. Backup your Cisco Network Registrar data and upgrade your operating system before installing this latest release. (See System Requirements, page 1-2 for currently supported operating systems.)

Note When upgrading from a pre-7.2 cluster to Cisco Network Registrar 7.2, a platform-specific tool cnr_mcdexport is required. This tool can be downloaded from CCO as an archive file. The archive contains an extensive README file with specific instructions on the process to be followed.

The MCD DB database technology has been in use in Cisco Network Registrar for several earlier versions. The cnr_mcdexport kit extracts the MCD DB data, which, during the upgrade procedure, is transferred to new locations.

When you install the software, the installation program automatically detects an existing version and upgrades the software to the latest release. The program first prompts you to archive existing Cisco Network Registrar data. If the program encounters errors during the upgrade, it restores the software to the earlier release.

During an upgrade, Cisco Network Registrar now displays any pre-existing HTTPS configuration defaults for the keystore filename and password to enable a secure connection for web UI logins. If you have enabled HTTPS, and are unaware of the keystore filename and password at the time of the upgrade, you can preserve HTTPS connectivity during the upgrade, and re-enter the defaults when prompted.

Note The default keystore filename and password appear only if you are upgrading from Cisco Network Registrar 6.3.1 or later versions, or reinstalling the Cisco Network Registrar 7.2.

Upgrading on Windows

To upgrade to Cisco Network Registrar 7.2:

Step 1 Ensure that your environment meets the current system requirements (see System Requirements, page 1-2).

Step 2 Use the currently installed release to complete any configuration changes in progress, so that the existing database is consistent before you perform the upgrade.

Step 3 Ensure that no pending database tasks result from recent edits. You can confirm that the task lists are empty by viewing the CCM and MCD Tasks pages under the Administration menu in the web UI. Wait until both lists are empty before proceeding with the update.

Step 4 Stop Cisco Network Registrar.

Step 5 Create the C:\NetworkRegistrar\{Local | Regional} directory.

Caution Do not create this directory under C:\Program Files (x86), C:\Program Files, or C:\ProgramData.

Step 6 Move the data, logs, and temp directories manually to the \NetworkRegistrar\{Local | Regional} folder.

Step 7 Modify C:\{Program Files | Program Files (x86)}\{Local | Regional}\conf\cnr.conf to point at the new locations for the data, logs and temp directories.

Step 8 Restart Cisco Network Registrar to ensure that all of the moves or edits were correct and that Cisco Network Registrar is functioning normally.

Step 9 Stop Cisco Network Registrar.

Step 10 Run cnr_mcdexport.exe to export the configuration objects to create an intermediate database. You can download the cnr_mcdexport_windows.tar tool from CCO as an archive file. The archive contains an extensive README file with specific instructions on the process to be followed.

Step 11 Backup your Cisco Network Registrar data on a different machine or a shared network device and upgrade your operating system to Windows Server 2008 R2. See documentation supplied by Microsoft for information about how to install / upgrade Windows servers.

Note If you install Windows Server 2008 R2 instead of upgrading and the disk is reformatted, you must restore the Cisco Network Registrar data to the C:\NetworkRegistrar\{Local | Regional}\data folder.

Step 12 Install Cisco Network Registrar 7.2 on the Windows Server 2008 R2 machine. For installation instructions, see "Installing Cisco Network Registrar 7.2" section on page 2-5. Ensure that you specify the C:\NetworkRegistrar\{Local | Regional} path for the location of the data, logs, and temp directories.

Note Ensure that you keep the old Cisco Network Registrar configuration and license information handy as you may need to re-enter this information during the Cisco Network Registrar installation.

We recommend upgrading the regional cluster before upgrading any local clusters, because an older version of a regional cluster cannot connect to newer local clusters.

Upgrading on Solaris/Linux

To upgrade to Cisco Network Registrar 7.2:

Step 1 Ensure that your environment meets the current system requirements (see System Requirements, page 1-2).

Step 2 Use the currently installed release to complete any configuration changes in progress, so that the existing database is consistent before you perform the upgrade.

Step 3 Ensure that no pending database tasks result from recent edits. You can confirm that the task lists are empty by viewing the CCM and MCD Tasks pages under the Administration menu in the web UI. Wait until both lists are empty before proceeding with the update.

Step 4 Stop the Cisco Network Registrar server agent and backup the current system (or at least the Cisco Network Registrar \Program Files\Network Registrar\ directories and contents). To stop the Cisco Network Registrar server agent, do the following:

- If local—**`/etc/init.d/nwreglocal stop`**
- If regional—**`/etc/init.d/nwregregion stop`**

Step 5 Run cnr_mcdexport to export the configuration objects to create an intermediate database. You can download the cnr_mcdexport_linux4.tar (or cnr_mcdexport_linux5.tar or cnr_mcdexport_solaris.tar) tool from CCO. The archive contains an extensive README file with specific instructions on the process to be followed.

Step 6 Install Cisco Network Registrar 7.2. For installation instructions, see "Installing Cisco Network Registrar 7.2" section on page 2-5.

Installing Cisco Network Registrar 7.2

To install Cisco Network Registrar 7.2:

Step 1 Log in to the target machine using an account that has administrative privileges:

- Windows—Account in the Administrators group
- Solaris and Linux—**su** (superuser) or root account

Windows—Close all open applications, including any antivirus software.

Step 2 Download and install the Java Runtime Environment (JRE) 5.0 (1.5.0_06) or later, or the equivalent Java Development Kit (JDK), if you have not already done so. These are available from the Oracle website.

Note On Windows, add the full path of the bin subdirectory of your Java installation folder to your PATH environment variable.

Step 3 If you are not configuring secure login to the web UI, skip to Step 4. If you are configuring secure login, you must create a keystore file by using the Java **keytool** utility, which is located in the bin subdirectory of the Java installation (see Step 2). Use the utility to define a self-signed certificate, or to request and later import a certificate from an external signing authority:

a. To create a keystore file containing a self-signed certificate, run this command and respond to the prompts:

```
> keytool -genkey -alias tomcat -keyalg RSA -keystore k-file
    Enter keystore password: password
    What is your first and last name? [Unknown]: name
    What is the name of your organizational unit? [Unknown]: org-unit
    What is the name of your organization? [Unknown]: org-name
    What is the name of your City or Locality? [Unknown]: local
    What is the name of your State or Province? [Unknown]: state
    What is the two-letter country code for this unit? [Unknown]: cc
    Is CN=name, OU=org-unit, O=org-name, L=local, ST=state, C=cc correct? [no]: yes
    Enter key password for <tomcat> (RETURN if same as keystore password):
```

The keystore filename (*k-file*) is its fully qualified path. You will be entering the keystore path and password in Step 13.

Note You must use 128-bit SSL to disable weak ciphers in the web UI. For more information, see Appendix C, "Enhancing Security for Web UI".

b. To create a Certificate Signing Request (CSR) that you will submit to the Certificate Authority (CA) when you request a certificate, create the keystore file as in the previous substep, then execute this command:

```
> keytool -certreq -keyalg RSA -alias tomcat -file certreq.cer -keystore k-file
    ...
```

Submit the resulting certreq.cer file to the CA. Once you receive the certificate from the CA, first download the Chain Certificate from the CA, then import the Chain Certificate and your new Certificate into the keystore file, as follows:

```
> keytool -import -alias root -keystore k-file -trustcacerts -file chain-cert-file
> keytool -import -alias tomcat -keystore k-file -trustcacerts -file new-cert-file
```

For details on the **keytool** utility, see the documentation at the Java website of Oracle. For details on the **keystore** file and Tomcat, see the documentation at the website of the Apache Software Foundation.

Caution The Cisco Network Registrar installation program for Windows does not try to modify ACLs to restrict access to installed files and directories. If you want to restrict access to these files and directories, use the native Microsoft utilities to manually change file and directory permissions. See Modifying ACLs in Windows Installations, page 1-5.

Step 4 Load the installation CD, or browse to the network resource where the Cisco Network Registrar software is located. If you download a distribution file from the Cisco website, run it from a different directory than where you will install Cisco Network Registrar.

- Windows—The cnr_7_2-windows.exe file is a self-extracting executable file that places the setup file and other files in the directory where you run it. (If you are not configured for Autostart, run the setup.exe file in that directory.) The Welcome to Cisco Network Registrar window appears.

  Click **Next**. The second welcome window introduces the setup program and reminds you to exit all current programs, including virus scanning software. If any programs are running, click **Cancel**, close these programs, and return to the start of Step 4. If you already exited all programs, click **Next**.

- Solaris and Linux—Be sure that the **gzip** and **gtar** utilities are available to uncompress and unpack the Cisco Network Registrar installation files. See the GNU organization website for information on these utilities. Do the following:

  1. Download the distribution file.
  2. Navigate to the directory in which you will uncompress and extract the installation files.

3. Uncompress and unpack the .gtar.gz file. Use **gtar** with the **–z** option:

   ```
   gtar -zxpf cnr_7_2-linux5.gtar.gz
   ```
   or
   ```
   gtar -zxpf cnr_7_2-solaris.gtar.gz
   ```

   To unpack the .gtar file that **gunzip** already uncompressed, omit the **–z** option:

   ```
   gtar -xpf cnr_7_2-linux5.gtar
   ```

4. Run the following command or program:

   Solaris—Run the **pkgadd** command with the **–d** option that specifies the directory from which you are installing, with the **–a** option in case you want to upgrade from a previous release. The name of the Cisco Network Registrar package is **nwreg2**:

   ```
   pkgadd -a pkgdir/solaris/nwreg2/install/cnradmin -d pkgdir/solaris nwreg2
   ```

   Linux—Run the install_cnr script from the directory containing the installation files:

   ```
   install-path # ./install_cnr
   ```

   The *install-path* is the CD-ROM directory that contains the installation files or the directory that contains the extracted Cisco Network Registrar installation files, if they were downloaded electronically.

Step 5 Specify whether you want to install Cisco Network Registrar in the local or regional cluster mode (see the "About Cisco Network Registrar" section on page 1-1):

- Windows—Keep the default Cisco Network Registrar Local or choose Cisco Network Registrar Regional. Click **Next**. The Select Program Folder appears, where you determine the program folder in which to store the program shortcuts in the Start menu. Accept the default, enter another name, or choose a name from the Existing Folders list. Click **Next**.
- Solaris and Linux—Enter **1** for a local, or **2** for regional. The default mode is 1.

Note If you are upgrading, the upgrade process autodetects the installation directory from the previous release.

Step 6 Enter the filename, as an absolute or relative path, for your base license (see the "License Files" section on page 1-4). On providing the license file, the installer prompts for the creation of superuser administrator. If there are no defined administrators, click **Yes** to create it by providing the username and password.

Entering the filename during installation is optional. However, if you do not enter the filename now, you must enter it when you first log in to the web UI or CLI.

Note If you install Cisco Network Registrar 7.0 or later using a Remote Desktop Connection to the Windows Server, you will not be able to enter the license information during the installation. Cisco Network Registrar will reject the licenses as invalid. You must therefore skip the license information step, and add the license after the installation completes, using either the web UI or CLI. See Starting Cisco Network Registrar, page 2-12 for details.

Step 7 Note these Cisco Network Registrar installation default directories and make any appropriate changes to meet your needs:

Windows default locations:

Caution Do not specify the \Program Files (x86) or \Program Files or \ProgramData for the location of the Cisco Network Registrar data, logs, and temporary files. If you do this, the behavior of Cisco Network Registrar may be unpredictable because of Windows security.

- Local cluster
  - Program files (32-bit OS)—C:\Program Files\Network Registrar\Local
  - Program files (64-bit OS)—C:\Program Files (x86)\Network Registrar\Local
  - Data files—C:\NetworkRegistrar\Local\data
  - Log files—C:\NetworkRegistrar\Local\logs
  - Temporary files—C:\NetworkRegistrar\Local\temp
- Regional cluster
  - Program files (32-bit OS)—C:\Program Files\Network Registrar\Regional
  - Program files (64-bit OS)—C:\Program Files (x86)\Network Registrar\Regional
  - Data files—C:\NetworkRegistrar\Regional\data
  - Log files—C:\NetworkRegistrar\Regional\logs
  - Temporary files—C:\NetworkRegistrar\Regional\temp

Solaris and Linux default locations:

- Local cluster:
  - Program files—/opt/nwreg2/local
  - Data files—/var/nwreg2/local/data
  - Log files—/var/nwreg2/local/logs
  - Temporary files—/var/nwreg2/local/temp
- Regional cluster:
  - Program files—/opt/nwreg2/regional
  - Data files—/var/nwreg2/regional/data
  - Log files—/var/nwreg2/regional/logs
  - Temporary files—/var/nwreg2/regional/temp

Step 8 Choose whether to archive the existing binaries and database in case this installation does not succeed. The default and recommended choice is **Yes** or **y**:

If you choose to archive the files, specify the archive directory. The default directories are:

- Windows—Local cluster (C:\NetworkRegistrar\Local.sav); Regional cluster (C:\NetworkRegistrar\Regional.sav). Click **Next**.
- Solaris and Linux—Local cluster (/opt/nwreg2/local.sav); Regional cluster (/opt/nwreg2/regional.sav)

Step 9 Choose the appropriate installation type: server and client (the default), or client-only:

- Windows—Choose **Both server and client (default)** or **Client only**. Click **Next.** The Select Port window appears.
- Solaris and Linux—Entering **1** installs the server and client (the default), or **2** installs the client only.

Note Choose **Client only** in a situation where you want the client software running on a different machine than the protocol servers. Be aware that you must then set up a connection to the protocol servers from the client.

Step 10 Choose the CCM management SCP port number. (You can change this port number on your target system.) These are the default port numbers:

- Local cluster—1234
- Regional cluster—1244

On Windows, click **Next**.

Step 11 Enter the location of the Java installation (JRE or JDK 1.5.0_06 selected in Step 2). (The installation or upgrade process tries to detect the location.):

- Windows—A dialog box reminds you of the Java requirements. Click **OK** and then choose the default Java directory or another one. Click **OK**. The Select Connection Type window appears.
- Solaris and Linux—Enter the Java installation location.

Note Do not include the bin subdirectory in the path. If you install a new Java version or change its location, rerun the Cisco Network Registrar installer, then specify the new location in this step.

Step 12 Choose whether to enable the web UI to use a nonsecure (HTTP) or secure (HTTPS) connection for web UI logins:

- Windows—Choose **Non-secure/HTTP (default)**, **Secure/HTTPS (requires JSSE)**, or **Both HTTP and HTTPS**.
- Solaris and Linux—Enter an HTTP port, a secure HTTPS port, or both HTTP and HTTPS ports.

Enabling the secure HTTPS port configures security for connecting to the Apache Tomcat web server (see Step 3 for configuration). (To change the connection type, rerun the installer, and then make a different choice at this step.)

- If you choose HTTPS, or HTTP and HTTPS, click **Next** and continue with Step 13.
- If you choose the default HTTP connection, click **Next**, and skip to Step 14.

Step 13 If you enabled HTTPS web UI connectivity, you are prompted for the location of the necessary keystore and keystore files:

- For the keystore location, specify the fully qualified path to the keystore file that contains the certificate(s) to be used for the secure connection to the Apache Tomcat web server. This is the keystore file that you created in Step 3.
- For the keystore password, specify the password given when creating the keystore file. On Windows, click **Next**.

Caution Do not include a dollar sign ($) in the keystore password as it will result in an invalid configuration on the Apache Tomcat web server.

Step 14 Enter a port number for the web UI connection. The defaults are:

- HTTP local cluster—8080
- HTTP regional cluster—8090
- HTTPS local cluster—8443
- HTTPS regional cluster—8453

On Windows, click **Next**.

The Cisco Network Registrar installation process begins. (Solaris prompts you to verify that you want to continue with the installation.) Status messages report that the installer is transferring files and running scripts. This process may take a few minutes:

- Windows—The Setup Complete window appears. Choose **Yes, I want to restart my computer now** or **No, I will restart my computer later,** and then click **Finish**.
- Solaris and Linux—Successful completion messages appear.

Note When you upgrade Cisco Network Registrar, the upgrade process takes place during the installation. Therefore, the installation and upgrade processes take a longer time depending on the number of scopes, prefixes, and reservations that you have configured.

Step 15 Verify the status of the Cisco Network Registrar servers:

- Windows—In the Services control panel, verify that the Cisco Network Registrar Local Server Agent or Cisco Network Registrar Regional Server Agent is running after rebooting the system when the installation has completed successfully.
- Solaris and Linux—Use the *install-path***/usrbin/cnr_status** command to verify status. See "Starting and Stopping Servers" section on page 2-13.

If the upgrade fails, you can revert to the earlier Cisco Network Registrar version. For details about reverting to the earlier version, see the "Reverting to Earlier Product Version" section on page 2-11.

Reverting to Earlier Product Version

The Cisco Network Registrar installation program provides the capability of reverting to an earlier version and archiving the existing product configuration and data when upgrading to a newer version of the product. If you chose this option, and the upgrade process fails, use the following procedure to revert to the earlier product version and configuration:

Caution To complete this process, you must have access to the product installer and license key or license file for the earlier Cisco Network Registrar version. Any attempt to proceed otherwise may destabilize the product.

If the installer had successfully performed the upgrade but you want to roll back to the earlier version at some later point, this procedure can result in network destabilization and data loss; for example, you will lose updates made to the Cisco Network Registrar database after the upgrade, including DHCP lease data and DNS dynamic updates.

Step 1 Verify that the archive directory that you specified during the upgrade process exists and is valid. These examples assume the default archive location provided during installation. Ensure that the path to the cnr_data_archive directory reflects the value of the archive directory that you specified during installation. If you are using:

- Windows—C:\NetworkRegistrar\{Local.sav | Regional.sav}
- Solaris and Linux—/opt/nwreg2/{local.sav | regional.sav}

Step 2 Uninstall Cisco Network Registrar using the procedure described in the Uninstalling Cisco Network Registrar, page 2-16.

Step 3 Other than the contents of the specified archive directory, delete any remaining files and directories in the Cisco Network Registrar installation paths.

Step 4 Reinstall the original version of Cisco Network Registrar. Ensure that you follow the reinstallation procedure described in *Cisco Network Registrar Installation Guide* that is specific to the original product version.

Step 5 After the installation ends successfully, stop the Cisco Network Registrar server agent:

- Windows—Local: **`net stop nwreglocal`**
  Regional: **`net stop nwregregion`**
- Solaris and Linux—Local: **`/etc/init.d/nwreglocal stop`**
  Regional: **`/etc/init.d/nwregregion stop`**

Step 6 Delete the contents of the Cisco Network Registrar *install-path*/data subdirectory.

Step 7 Extract the contents of the backup file to the reinstalled version of Cisco Network Registrar.

1. Change to the root directory of the filesystem. On Windows, this directory would be the base drive (such as C:\); on Solaris and Linux, it would be /.
2. Using the fully qualified path to the archive directory, extract the archive. These examples assume the default archive location provided during installation.

- Windows—Copy the C:\NetworkRegistrar\{Local.sav|Regional.sav}\cnr_data_archive\ contents to the target Cisco Network Registrar data directory. The following assume the default installation locations for a local cluster:

```
xcopy/s C:\NetworkRegistrar\Local.sav\cnr_data_archive
C:\NetworkRegistrar\Local\data\
```

Note There is also a cnr_file_archive directory which contains the installed files and generally this should not be recovered over a re-installation.

- Solaris and Linux—
  - Change to the root directory of the filesystem —cd /.
  - Using the fully qualified path to the archive directory containing the cnr_data_archive.tar file, extract the archive. These examples assume the default archive location provided during installation. Ensure that the paths to the tar executable and cnr_data_archive.tar file reflect the value of the archive directory that you specified during installation.

```
/opt/nwreg2/{local.sav | regional.sav}/tar -xf /opt/nwreg2/{local.sav |
regional.sav}/cnr_data_archive.tar
```

Note There is also a cnr_file_archive.tar which contains the installed files and generally this should not be recovered over a re-installation.

Step 8 Start the Cisco Network Registrar server agent:

- Windows—Local: **net start nwreglocal**
  Regional: **net start nwregregion**
- Solaris and Linux—Local: **/etc/init.d/nwreglocal start**
  Regional: **/etc/init.d/nwregregion start**

Step 9 Verify if the previous configuration, including scopes and zones, is intact.

Starting Cisco Network Registrar

To administer the local and regional clusters that you have installed, you must enter the contents of the appropriate license file (web UI) or the filename (CLI).

Follow this procedure to enter license information:

Step 1 Start the Cisco Network Registrar web UI or CLI:

- To access the web UI, open the Web browser and use the HTTP (nonsecure login) or HTTPS (secure login) website:

  http://*hostname*:*http-port*
  https://*hostname*:*https-port*

  where:
  - The *hostname* is the actual name of the target host.
  - The *http-port and the https-ports* are the default HTTP or HTTPS port that are specified during installation. (See the installation procedure, Step 14 on page 2-9).

  On Windows, you can access the web UI from the Start menu from the local host:

  - On a local cluster—Choose **Start > Programs > Network Registrar 7.2 > Network Registrar 7.2 local Web UI** (or **Network Registrar 7.2 local Web UI (secure)** if you enabled secure login).
  - On a regional cluster—Choose **Start > Programs > Network Registrar 7.2 > Network Registrar 7.2 regional Web UI** (or **Network Registrar 7.2 regional Web UI (secure)** if you enabled secure login).
- To start the CLI:
  - Windows—Navigate to the *install-path*\bin directory and enter this command:

    nrcmd -C *cluster-ipaddress* **-N** <username> **-P** <password>
  - Solaris and Linux—Navigate to the *install-path*\usrbin directory and enter this command:

    *install-path***/usrbin/nrcmd -C** *clustername* **-N** <username> **-P** <password>

Step 2 Enter the username and the password, that was created during the installation procedure.

Step 3 If you did not enter license information during the installation procedure, you must do so now:

- Web UI—Enter the name of the license file on the Add License page. Optionally, click **Browse** to navigate to the license file.
- CLI—Enter an absolute or relative path for the license filename, as follows:

  nrcmd> ***license create filename***

Starting and Stopping Servers

In Windows, you can stop and start the Cisco Network Registrar server agent from the Services feature of the Windows Control Panel. If the installation completed successfully and you enabled the servers, the Cisco Network Registrar DNS and DHCP servers start automatically each time you reboot the machine.

For the TFTP server, you must use this Cisco Network Registrar CLI command to enable it to restart on bootup:

nrcmd> **tftp enable start-on-reboot**

All servers in the cluster are controlled by the Cisco Network Registrar regional or local server agent. You can stop or start the servers by stopping or starting the server agent.

For details on stopping and starting servers, see the *User Guide for Cisco Network Registrar*.

Starting and Stopping Servers on Windows

Follow this procedure to start and stop servers on Windows:

Step 1 Choose **Start > Settings > Control Panel > Administrative Tools > Services**.

Step 2 From the Service list, choose **Network Registrar Local Server Agent** or **Network Registrar Regional Server Agent**.

Step 3 Click **Restart** or **Stop**, as required, and then click **Close**.

Starting and Stopping Servers on Solaris or Linux

In Solaris or Linux, the Cisco Network Registrar servers automatically start up after a successful installation or upgrade. You do not need to reboot the system. Follow this procedure to start and stop servers on Solaris or Linux:

Step 1 Log in as superuser.

Step 2 Start the server agent by running the nwreglocal or nwregregion script with the *start* argument:

```
# /etc/init.d/nwreglocal start ;for the local cluster
# /etc/init.d/nwregregion start ;for the regional cluster
```

Step 3 Enter the **cnr_status** command to check that the servers are running:

```
# install-path/usrbin/cnr_status
```

Step 4 Stop the server agent by running the nwreglocal or nwregregion script with the *stop* argument:

```
# /etc/init.d/nwreglocal stop ;for the local cluster
# /etc/init.d/nwregregion stop ;for the regional cluster
```

Moving an Installation to a New Machine

Before you begin, ensure that the new machine meets the current system requirements (see System Requirements, page 1-2). To move an existing Cisco Network Registrar installation to a new machine:

Step 1 Stop the server agent on the old machine.

- Windows—Local: **net stop nwreglocal**;
  Regional: **net stop nwregregion**
- Solaris and Linux—Local: **/etc/init.d/nwreglocal stop**;
  Regional: **/etc/init.d/nwregregion stop**

Step 2 Zip up the data directory on the old machine.

Step 3 Copy the zip file over to the same location on the new machine.

Step 4 Install Cisco Network Registrar on the new machine (on Solaris and Linux, use the –a option). The installation will detect an upgrade and will do so based on the copied data.

This procedure preserves your original data on the old machine.

Troubleshooting the Installation

The Cisco Network Registrar installation process creates a log file, install_cnr_log, in the Cisco Network Registrar log file directory. For upgrades, one additional log file is created: lease_upgrade_log. The log directory is set to these locations by default:

- Windows:
  - Local cluster: C:\NetworkRegistrar\Local\logs
  - Regional cluster: C:\NetworkRegistrar\Regional\logs
- Solaris and Linux:
  - Local cluster: /var/nwreg2/local/logs
  - Regional cluster: /var/nwreg2/regional/logs

If the installation or upgrade does not complete successfully, first check the contents of these log files to help determine what might have failed. Some examples of possible causes of failure are:

- An incorrect version of Java is installed.
- Insufficient disk space is available.
- Inconsistent data exists for an upgrade.

If the log messages do not clearly indicate the failure, you can gather additional debug information by using the debug_install utility script. This script appears only if the installation failed and is located by default in the Cisco Network Registrar program files directory:

- Windows:
  - Local cluster: C:\Program Files(x86)\Network Registrar\Local\debug_install.cmd
  - Regional cluster: C:\Program Files\Network Registrar\Regional\debug_install.cmd
- Solaris and Linux:
  - Local cluster: /opt/nwreg2/local/debug_install.sh
  - Regional cluster: /opt/nwreg2/regional/debug_install.sh

If the `## Executing checkinstall script` part of the Solaris **pkgadd** fails, ensure that the /tmp directory has sufficient permissions to allow a nonprivileged installation user ID to write to it.

If you still need help determining the cause or resolution of the failure, forward the output of this script to Cisco Systems for further analysis. To contact Cisco for assistance, see the following Cisco website:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Uninstalling Cisco Network Registrar

The uninstallation procedure differs based on the operating system you are using. You must have administrator or superuser privileges to uninstall Cisco Network Registrar, just as you must to install it.

To back up your database before uninstalling Cisco Network Registrar, see the *User Guide for Cisco Network Registrar* for the procedure.

Note Uninstallation stops the Cisco Network Registrar server agents first. If you find that the server processes are not shutting down, see the "Starting and Stopping Servers" section on page 2-13.

Uninstalling on Windows

To uninstall Cisco Network Registrar on Windows:

Step 1 Choose the Add/Remove Program function from the Windows control panel.

Or,

Choose **Uninstall Network Registrar 7.2** from the Windows Start menu. The uninstallation program removes the server and user interface components but does not delete user data files. Optionally, delete all Cisco Network Registrar data by deleting the Cisco Network Registrar folder.

Note Temporarily stop any service that is related to software that integrates with Performance Monitoring that might interfere with removing shared libraries in the Cisco Network Registrar folder.

Step 2 Reboot after the uninstallation completes.

Uninstalling on Solaris

To uninstall Cisco Network Registrar on Solaris:

Step 1 From the root account, use the **pkgrm** program to remove the **nwreg2** package:

```
pkgrm nwreg2
```

The uninstallation procedure removes the server and user interface components; but does not delete user data, such as the log and data files. Optionally, delete the database and log files that are associated with Cisco Network Registrar, as mentioned in the instructions at the end of the **pkgrm** process.

Uninstalling on Linux

To uninstall Cisco Network Registrar on Linux:

Step 1 Run the **uninstall_cnr** program from the *install-path*/usrbin directory:

```
./uninstall_cnr
Stopping Server Agent...
Deleting startup files...
Removing Network Registrar...
cannot remove /opt/nwreg2/usrbin - directory not empty
cannot remove /opt/nwreg2/conf - directory not empty
package optnwreg2 not found in file index
Note that any files that have been changed (including your database) have _not_ been
uninstalled. You should delete these files by hand when you are done with them, before you
reinstall the package.
```

The `cannot remove` warnings mean that, although the uninstall program removes the server and user interface components, it cannot delete directories that are not empty. Certain configuration and data files that are created during installation remain deliberately after uninstallation. Optionally, delete the database and log files that are associated with Cisco Network Registrar, as mentioned in the instructions at the end of the **uninstall_cnr** script execution.

CHAPTER 3

Installing and Upgrading Cisco Network Registrar Virtual Appliance

The Cisco Network Registrar virtual appliance includes all the functionality available in a version of Cisco Network Registrar 7.2 installed on any Linux operating system.

This chapter describes how to install Cisco Network Registrar virtual appliance and includes the following sections:

- System Requirements
- Installing and Configuring Cisco Network Registrar Virtual Appliance, page 3-2
- Configuring Virtual Appliance to Automatically Power Up, page 3-8
- Upgrading Cisco Network Registrar Virtual Appliance, page 3-9
- Managing Cisco Network Registrar Virtual Appliance, page 3-12

System Requirements

The memory and storage parameters are specified in the OVF file. However, you should ensure that sufficient resources are available on the host that you are targeting for the deployment to meet these requirements.

The OVF deployment allocates 2 GB of RAM to the virtual appliance. In addition, you may find that you also will need disk space beyond the 14 GB minimum allocation provided when the virtual appliance is installed. It is possible to expand the disk usage after the virtual appliance is installed.

Note It is worth some effort to determine the likely amount of disk storage that you need at the time you first install the virtual appliance. If you increase the size of the disk space after you have configured and used the product, you must back up all the work that you have done prior to increasing the disk storage. However, if you increase the disk storage when you first install the product, no backup is necessary, since in the unlikely event something goes wrong while expanding the disk storage, nothing valuable would be lost. At worst, you would simply have to reinstall the virtual appliance.

The Cisco Network Registrar virtual appliance is supported only on VMware ESXi 4.1 and later systems that are themselves supported ESXi 4.1 systems. You can run ESXi 4.1 on hardware systems that do not meet the minimum support requirements for ESXi 4.1. In this case it will run, but some features or capabilities will not be available. VMware provides a bootable program which helps you identify whether the hardware on which it is run supports ESXi 4.1.

Installing and Configuring Cisco Network Registrar Virtual Appliance

Cisco Network Registrar virtual appliance is supported for production use on VMware ESXi 4.x and can be accessed or managed using vSphere client of VMware. The Cisco Network Registrar virtual appliance is installed using the Open Virtualization Format (OVF) package.

The VMware vSphere client can be connected directly to your ESXi installation, or it can be connected to a vCenter server which in turn is connected to your vSphere installation. Connecting through vCenter provides a number of capabilities that connecting directly to ESXi does not. If a vCenter server is available and associated with the ESXi installation, it should be used.

See Also

Preparing to Deploy Cisco Network Registrar Virtual Appliance, page 3-2

Deploying Cisco Network Registrar Virtual Appliance, page 3-3

Booting and Configuring Cisco Network Registrar Virtual Appliance, page 3-5

Preparing to Deploy Cisco Network Registrar Virtual Appliance

In order to deploy the Cisco Network Registrar virtual appliance and configure its network connection, you have to answer several questions. Some of these questions concern the networking environment in which the virtual appliance is being deployed, and some of them concern values which are unique to the particular virtual appliance being deployed.

The questions that are unique to the installation of this particular virtual appliance are listed below. You must decide on answers to these questions before you deploy the virtual appliance.

- A virtual machine name for the deployed virtual appliance.
- A root password for the underlying Linux CentOS operating system.
- An IPv4 address for the virtual appliance.
- A DNS name associated with the IPv4 address of the virtual appliance.
- A username and password for the initial administrator account for the Cisco Network Registrar application.

The questions concerning the networking environment are as follows. The answers to these questions are not unique to the virtual appliance, but are instead values that are determined by the environment in which you will deploy the virtual appliance:

- The IP address or DNS name of the ESXi installation on which you intend to deploy the virtual appliance.
- The IP address or DNS name of any vCenter server associated with the ESXi installation, above.
- The network mask associated with the IP address of the virtual appliance itself.
- The default gateway address for the virtual appliance.
- The IP address of at least one DNS server that can be accessed by the virtual appliance, although it is best if you have the IP address of two DNS servers to provide additional availability.
- Any proxy values necessary for the virtual appliance to access the Internet (if you want the virtual appliance to have access to the Internet).

Deploying Cisco Network Registrar Virtual Appliance

Note Before deploying the virtual appliance, verify that your VMware server is running on VMware supported hardware. If you are not sure whether your environment can support a 64-bit client, you can verify by downloading and running the VMware "CPU Identification Utility" which indicates 64-bit VMware support. This utility can be found on the VMware site at: http://www.vmware.com/download/shared_utilities.html

To install the Cisco Network Registrar virtual appliance, you must first download the correct installation file. There are two files available, a regional virtual appliance and a local cluster virtual appliance. Each of these virtual appliances are provided as a zip file.

The names are:

- cnr_7_2_local_ovf.zip for the local virtual appliance
- cnr_7_2_regional.ovf.zip for the regional virtual appliance

Download the virtual appliance of your choice, and unzip the contents of the .zip file into an empty directory of your choice.

Note You should unzip each virtual appliance into separate directories if you are using both regional and local. Do not attempt to have them share the same directory.

Using vSphere, connect directly to the ESXi installation or the vCenter server, and select the ESXi installation where the OVF is to be deployed.

If you have a vCenter server available, you can connect the ESXi hypervisor to your existing vCenter server and manage it through that vCenter server. Managing all your VMware hypervisors through a common vCenter server provides many benefits.

The screens that you see while managing the ESXi hypervisor with a vSphere client through a vCenter server are different from the screens that you see while connecting the vSphere client directly to the ESXi hypervisor. You can see additional screens if connected through vCenter server. These screens do not actually provide any benefit for the operations in which you will engage to deploy the Cisco Network Registrar virtual appliance. The benefits to using the vCenter server approach come after the initial deployment of the virtual appliance.

Step 1 From vSphere menu, choose **File > Deploy OVF Template**.

The Deploy OVF Template Source window appears.

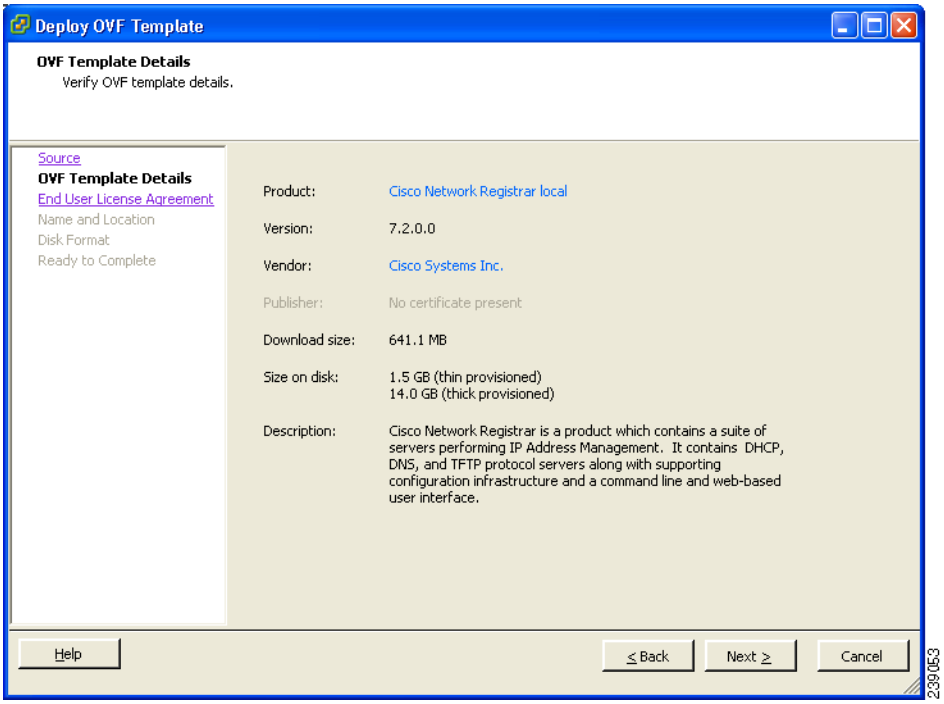
Step 2 To import the OVF file from hard disk, click **Browse** and choose the OVF file (.ovf) available in the local machine where the vSphere is running, usually **CNR_local_OVF10.ovf (or CNR_regional_OVF10.ovf)** in the directory in which you unzipped the file earlier. You can also enter a URL to download and install the OVF package from the internet.

Note You cannot deploy a zipped file. You cannot browse for URLs and you must enter the full path to the .ovf file.

Step 3 Click **Next**.

The OVF Template Details window appears. It displays the product name, the size of the OVF file, and the amount of disk space that needs to be available for the virtual appliance.

Figure 3-1 OVF Template Details



Step 4 Verify the OVF template details and click **Next**.

The End User License Agreement window appears.

Step 5 If you accept the license terms, check the Accept check box and click **Next**.

The Name and Location window appears.

Step 6 Enter the name of the new virtual appliance. If you are using the vCenter to manage the virtual machine, then you have the option of selecting the location of the inventory too. Click **Next** to continue.

The default name is generic. You may want to change it to something more specific, such as Cisco Network Registrar 7.2 Local or Cisco Network Registrar 7.2 Regional.

Note You can change the name of the virtual machine running the virtual appliance after the virtual appliance is deployed. However, while the name of the virtual machine will change, the original name (entered in Step 6) continues to be used as the location of the disk files that describe the virtual machine. Thus, confusion may arise in the future as whatever name you enter on this page remains for the life of the virtual machine and the virtual machine name and the disk file names will differ.

If you are using the vCenter to manage the virtual machine, then the Host/Cluster window appears. Go to Step 7.

If you are managing the ESXi host directly, then the Disk Format window appears. Go to Step 8.

Step 7 Choose the destination host on which you want to deploy the virtual machine and click **Next**.

The Disk Format window appears.

Step 8 The Thick provisioned format is selected by default. Click **Next** to continue.

Note Choosing thin provisioning may have performance implications.

If you are using the vCenter to manage the virtual machine, then the Network Mapping window appears. Go to Step 9.

If you are managing the ESXi host directly, then the Ready to Complete window appears. Go to Step 13.

Step 9 To map the networks used in this OVF template to the networks in your inventory, select the current destination network and choose the destination network from the Destination Networks drop-down list. Click **Next**.

The IP Address Allocation window appears.

Step 10 The **Fixed** check box is checked by default. Click **Next** to continue.

The Properties window appears.

Step 11 Enter the IP address in the **Network 1 IP Address** field provided.

Note You should not enter the root password in this window.

Step 12 Click **Next.**

The Ready to Complete window appears.

Step 13 Review the setting details of your deployment and click **Finish** to complete the deployment.

Booting and Configuring Cisco Network Registrar Virtual Appliance

To boot and then configure the Cisco Network Registrar virtual appliance:

Step 1 After deploying the Virtual Appliance OVF, select the virtual machine name in vSphere, right-click on it and select **Open Console**.

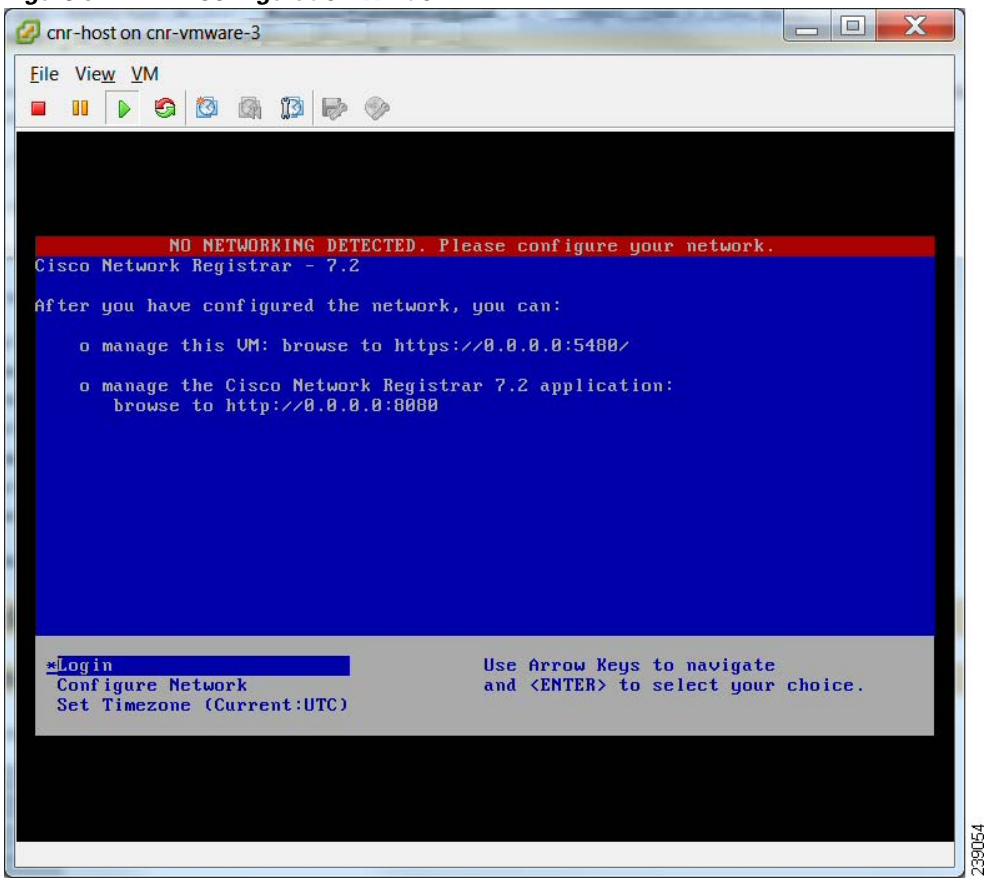
Step 2 Click the **Power on** button ( ) on the console and click in the window after clicking the Power on button.

During the initial boot of the newly deployed machine, you will be prompted to enter a root (system) password, which is not the Cisco Network Registrar password.

Note This is the root password for the underlying Linux operating system on which the Cisco Network Registrar 7.2 application is installed. You will be asked to enter this password twice. You will need root access to the underlying Linux operating system at various times in the future, so make sure that you remember this password.

The boot process can take a while, both before you are asked for a root password, as well as after you enter the root password. Eventually the console will display the configuration window, as shown in Figure 3-2.

Figure 3-2 Configuration Window



Step 3 Use the Arrow Keys to highlight **Configure Network** option, and press Enter. You must configure the virtual appliance to use a static address, so answer n (No) and configure the following:

- IP Address of the virtual appliance
- Netmask of the virtual appliance
- Gateway of the network in which you are creating virtual appliance
- DNS Server 1
- DNS Server 2
- Hostname of the virtual appliance
- Whether or not you need a proxy set

Step 4 To save the settings, select y (Yes) when prompted, after reviewing the settings. Select n (No) if you do not want to save the settings.

Step 5 Using the arrow keys, highlight **Set Timezone** and press Enter. Follow the instructions to set the timezone.

See Also

Configuring Cisco Network Registrar, page 3-7

Configuring Cisco Network Registrar with CLI on Virtual Appliance, page 3-8

Configuring Cisco Network Registrar

The URLs for managing the virtual appliance and Cisco Network Registrar application will be displayed in the console window after network configuration.

Note If the console window does not get displayed or is corrupted, press CTRL+C or Enter a few times.

To recover your mouse cursor after interacting with the console window on vSphere, press CTRL and ALT simultaneously.

The URLs to manage Cisco Network Registrar are the URLs displayed on the Console screen under **manage the Cisco Network Registrar 7.2 application**.

Both the insecure as well as the secure access links are provided on the Configuration Window after successfully entering the network configuration.

Note The local server and regional server use different ports for both standard and secure access.

To manage the Cisco Network Registrar 7.2 application, do the following:

Step 1 Browse to any URL displayed under **manage the Cisco Network Registrar 7.2 application** (either secure or standard access).

Note If you are using secure access for login, choose **I understand the risks** when you get the warning 'This Connection is Untrusted' and click **Add Exception** and **Confirm Security Exception** for this page.

The Cisco Network Registrar New Product Installation page is displayed.

Step 2 Use the browser to locate the Cisco Network Registrar FLEXlm license file for Cisco Network Registrar 7.2, and enter it on this page.

For more details regarding the FLEXlm licenses, see "Obtaining Cisco Network Registrar License Files" section on page 2-2".

Step 3 Enter the Name and Password for the superuser administrator in the New Product Installation > Add Superuser Administrator page.

Note This account is different from the root password which you entered earlier. This is an account in the Cisco Network Registrar product for the most privileged Cisco Network Registrar administrator, who will have permission to create additional administrator accounts in the Cisco Network Registrar product.

Step 4 Create other administrators now if you wish. To create and manage administrators in the future you can login with the account that you just created.

To manage the virtual appliance, do the following:

Step 1 Browse to the initial URL displayed in the console window under **manage this VM** to manage the virtual appliance. This URL displays the Virtual Appliance Management Infrastructure (VAMI) which provides a Web console to configure network settings, review basic system information for the virtual appliance, and stop or restart the virtual appliance.

Step 2 Choose **I understand the risks** when you get the warning 'This Connection is Untrusted'.

Step 3 Click **Add Exception** and **Confirm Security Exception** for this page.

The virtual appliance login page is displayed.

Configuring Cisco Network Registrar with CLI on Virtual Appliance

The Cisco Network Registrar command line interpreter (CLI) can be used to configure the virtual appliance in two ways:

- You can use the nrcmd CLI on the virtual appliance directly by using SSH to connect into the underlying Linux operating system on the virtual appliance. You can use any username and password which you have created on the virtual appliance for the SSH login, and you must use an administrator username and password for the Cisco Network Registrar to use the nrcmd CLI to configure Cisco Network Registrar.

Note As distributed, there is only one valid user for the Linux operating system—root. While you can login as root to use the Cisco Network Registrar CLI, you might want to add additional users to the system. Use the useradd program to add additional users. You can type **man useradd** for more information on how to add additional users.

- Alternatively, you can use the nrcmd CLI on some other system in the network to configure and manage Cisco Network Registrar on the virtual appliance the same way that you would use it to manage any remote installation of Cisco Network Registrar. This requires installing Cisco Network Registrar (either the entire product or client-only installation) on this other system.

Configuring Virtual Appliance to Automatically Power Up

You can configure the ESXi hypervisor to automatically power up the Cisco Network Registrar virtual appliance when power is restored to the ESXi hypervisor layer. Do the following for configuring automatic power up:

Step 1 In the vSphere client, select the ESXi machine to which you are connected. It is not a specific virtual machine that you have to select but the ESXi hypervisor on which they reside.

Step 2 Select the **Configuration** tab.

Step 3 Click the **Virtual Machine Startup/Shutdown** link under the **Software** area. You should see the virtual machine in the list shown in window.

Step 4 Click the **Properties...** link present at the top right corner of the page. If you do not see that, resize the window until you do.

The Virtual Machine Startup and Shutdown page is displayed.

Step 5 Check the **Allow virtual machines to start and stop automatically with the system** check box.

Step 6 Select the virtual machine running the Cisco Network Registrar virtual appliance and use the **Move Up** button on the right to move it up into the group labelled **Automatic Startup**.

Click **OK**.

This ensures that whenever power is restored to the ESXi hypervisor the Cisco Network Registrar appliance powers up automatically.

Upgrading Cisco Network Registrar Virtual Appliance

This section describes the procedure for upgrading Cisco Network Registrar to Cisco Network Registrar virtual appliance and upgrading the operating system for Cisco Network Registrar virtual appliance.

See Also

Upgrading Cisco Network Registrar Installation to run on Cisco Network Registrar Virtual Appliance, page 3-9

Upgrading Cisco Network Registrar Virtual Appliance Operating System, page 3-10

Upgrading Cisco Network Registrar Installation to run on Cisco Network Registrar Virtual Appliance

This section describes how to upgrade an existing installation of Cisco Network Registrar to become a Cisco Network Registrar virtual appliance.

Note This procedure upgrades a current version of Cisco Network Registrar running on a Linux operating system to a current version of the Cisco Network Registrar virtual appliance. If you need to move from a different platform, you have to first convert to the Linux platform prior to upgrading to a virtual appliance. If you need to move from a different version of Cisco Network Registrar to the current version of the virtual appliance, you have to first upgrade to the current version of Cisco Network Registrar on an external Linux system before upgrading to the virtual appliance. See "Installation and Upgrade Procedure" section on page 2-3.

Step 1 Install the Cisco Network Registrar virtual appliance.

Step 2 Shut down the Cisco Network Registrar system being upgraded using the following command: `/etc/init.d/nwreglocal stop`

Step 3 Copy the file **cnr_prepareforupgrade** from `/opt/nwreg2/{local | regional}/usrbin` from the virtual appliance system to the Cisco Network Registrar installation being upgraded.

Note You have to choose either local or regional from `{local | regional}` based on the upgrade that you are doing, that is, local upgrade or regional upgrade.

You can do it using sftp, for example:

```
[root@cnr-machine-being-upgraded usrbin]# sftp 10.10.10.12
Connecting to 10.10.10.12...
Warning: Permanently added '10.10.10.12' (RSA) to the list of known hosts.
root@10.10.10.12's password:
sftp> cd /opt/nwreg2/local/usrbin
sftp> get cnr_prepareforupgrade
Fetching /opt/nwreg2/local/usrbin/cnr_prepareforupgrade to cnr_prepareforupgrade
/opt/nwreg2/local/usrbin/cnr_prepareforupgrad 100% 3265     3.2KB/s   00:00
```

Step 4 Execute **cnr_prepareforupgrade** on the system being upgraded.

Step 5 If the version of Cisco Network Registrar which you are moving to the virtual appliance is a version earlier than Cisco Network Registrar 7.2, then perform the following steps:

a. Download the upgrade preparation kit, cnr_mcdexport_linux5.tar, from Cisco.com.

b. Untar the downloaded archive and run the script cnr_mcdexport.

Step 6 Tar the existing ***install-path*/local/data** directory using the command:

```
tar cvf tarfile.tar data
```

Step 7 Copy the tar file created to the new virtual appliance.

Step 8 Shut down Cisco Network Registrar on the new virtual appliance using the command:

```
/etc/init.d/nwreglocal stop
```

Step 9 Rename the existing database to **.orig** using the command:

```
mv /var/nwreg2/local/data /var/nwreg2/local/data.orig
```

Step 10 Untar the latest database, transferred in Step 4, using **tar xvf tarfile.tar**

Step 11 Reboot the Cisco Network Registrar virtual appliance using VMware vSphere**.**

If an upgrade is not required, then the Cisco Network Registrar will start up normally and will display a message to the console that no upgrade is required. But, if an upgrade is required, Cisco Network Registrar will not start and will instead display a message on the console that an upgrade is required before startup.

Step 12 Run the following if you get a message that an upgrade is required:

```
/opt/nwreg2/{local | regional}/usrbin/cnr_upgradedata
```

This upgrades the database to the latest version.

Upgrading Cisco Network Registrar Virtual Appliance Operating System

To upgrade the operating system for an existing Cisco Network Registrar virtual appliance, install a new virtual appliance which has the new operating system version on it, and then move the data and configuration from the existing virtual appliance to the new virtual appliance. To do this:

Step 1 Deploy the latest Cisco Network Registrar virtual appliance (with the new OS version) on the ESXi machine where an existing Cisco Network Registrar virtual appliance resides.

Step 2 Shut down Cisco Network Registrar on the existing virtual appliance.

Step 3 Run **cnr_prepareforupgrade** on the existing appliance.

Step 4 Shut down the virtual machine of the existing appliance.

Step 5 Copy the data disk from the existing virtual appliance to the new virtual appliance. Use vSphere to make this copy. Ensure that you have shut down the virtual appliances before copying.

Step 6 Select the ESXi platform in vSphere. It is not a particular virtual machine that you have to select, but rather the container in which these virtual machines appear.

Step 7 Select the **Configuration** tab and click the **Storage** link under Hardware area. You can now see the datastores in the right hand window. Determine the datastore in which the files for your virtual machines reside.

Note You should have selected the datastore when you deployed the virtual machines, if you have more than one datastore. If you have only one, no selection was required at the time of deployment.

Step 8 Right-click the datastore that contains the existing virtual machine. Select **Browse Datastore...**. A Datastore Browser is displayed which shows you the file structure of your ESXi datastore.

Note The directories which you see in the Datastore Browser use the names given to the virtual appliances when they were first deployed, which may or may not be the current names of the virtual appliances. If you changed the name of a virtual appliance after it was deployed, that name change will not be reflected in the file structure in the datastore.

Step 9 Select the folder for the existing virtual appliance from the tree structure displayed at the left pane of the Database Browser window. You can see the files which are associated with the existing virtual appliance in the right pane of the Database Browser window. Find the existing data disk from the list of files displayed in the right pane. The name of the file ends with **_1.vmdk** and is the largest file in the virtual machine.

Step 10 Right-click the file you found in Step 9 and select **Copy**.

Step 11 Select the folder of the new virtual appliance in the left pane of the Datastore Browser window. You can see the files currently associated with the new virtual appliance in the right pane of the window. Right-click in the right pane, and not on a particular file, and select **Paste**. Since the file you are copying may be rather large, you can see a progress popup which shows the copy progress. Close the Datastore Browser window when the copy is complete.

Step 12 Select the new virtual appliance in the left pane of the vSphere client window and select **Edit virtual machine settings**. The Virtual Machine Properties window is displayed. The Hardware tab is selected by default. If it is not, then select it.

Step 13 Select Hard disk 2 and click **Remove**. Accept the default **Removal Option** of **Remove from virtual machine** which does not delete the virtual disk file itself, but rather just removes it from the virtual machine.

Step 14 Select the new virtual appliance in the left pane of the vSphere client window and select **Edit virtual machine settings** again. Click **Add** in the Virtual Machine Properties window to add the hard disk you copied from the existing virtual machine.

The **Add Hardware** window is displayed.

Step 15 Choose **Hard Disk** from the list of device types and click **Next**.

Step 16 Check the **Use an existing virtual disk** check box to reuse the previously configured virtual disk and click **Next.**

Step 17 Click **Browse** to locate the disk file path. Select the datastore where you placed the copy of the virtual disk in the Browse Datastore window. Click **Open** and you can see the list of virtual machines on this datastore. Select the directory of the new virtual appliance from the list and click **Open**. You can see the

list of virtual disks in the directory for that virtual machine. Probably two of them will be named the same as the new virtual machine, and one of them will be named based on the existing virtual machine. Select the one named for the existing virtual machine and click **OK**. Click **Next**.

Step 18 Click **Next** again to accept the **Advanced Options** unchanged.

Step 19 Click **Finish** to complete the operation.

This takes you back to the Virtual Machine Properties window, and the list of hardware in the virtual machine now has the **New Hard Disk (adding)** in the list. Click **OK** to finish.

You can now start the new virtual machine.

Managing Cisco Network Registrar Virtual Appliance

You can manage the underlying Linux operating system, which is based on CentOS 5.4, by logging in as the root user. You may use SSH to login to the virtual appliance with the username root and the root password you specified when you first booted the virtual appliance.

You will probably want to create additional users on the Linux system so that people can access the Linux system with a username other than root.

The Linux system which is included on the virtual appliance is stripped down to a considerable degree and thus does not include things that are not required to run or manage the Cisco Network Registrar application, such as a window system manager and its associated GUI user interface. However, all the tools necessary to support and manage the Cisco Network Registrar application are included on the Linux operating system used inside of the virtual appliance.

You may also want to take additional steps to secure the SSH connection. For instance, configuring it to prevent logging on as root, and requiring a user to **su** to gain root privileges after logging on as another user.

You may wish to perform other configuration changes on the underlying Linux operating system in order to lock it down in ways appropriate to your environment.

Note The 'vsftpd' FTP server is available on the operating system, but it is not started by default. You can issue the command `/etc/init.d/vsftpd start` to start the vsftpd server. Even if you start it, you cannot log into it as root, but only as some other user.

APPENDIX A

Performing a Silent Installation

This appendix describes how to perform a silent installation, upgrade, or uninstallation of the Cisco Network Registrar (Cisco Network Registrar) product. A silent installation or upgrade allows for unattended product installations based on the configuration values that are provided at the time that a silent installation response file was created.

Caution Unpredictable results can occur if you try to use a silent-response file that does not contain the correct settings for the system undergoing the silent installation.

To generate or create a silent-response file:

Step 1 For each silent installation or upgrade, use these commands to create a separate response file:

- Windows:

  ```
  setup.exe -r
  ```

  Complete the installation or upgrade steps as you normally would. This command installs or upgrades Cisco Network Registrar according to the parameters that you specified. It also generates the setup.iss silent-response file based on these parameters. Look for this file in the Windows installation directory, such as C:\WINDOWS. Each time you use the command, the file is overwritten.

  We recommend that you rename or relocate this file before running the silent process in Step 2. Rename the file to something distinguishable, such as local-nr-https-install, and relocate it to a temporary folder.

- Solaris:

  ```
  pkgask -d install-path -r response-file nwreg2
  ```

  Complete the installation or upgrade steps as you normally would. This action does not actually install or upgrade Cisco Network Registrar, but simply generates a silent-response file by the specified name that includes the installation or upgrade parameters that you want to replicate for additional installations or upgrades. We recommend that you name the file something distinguishable, such as local-nr-upgrade or regional-nr-https-install.

- Linux:

  Create a text silent-response file that includes the entries in Table A-1 on page A-2.

Table A-1 Silent-Response File Entries for Linux

Silent-Response File Entry	Description
BACKUPDIR=	Path where to store the current Cisco Network Registrar installation files, but only if PERFORM_BACKUP=y.
CCM_PORT=	Central Configuration Management (CCM) port; default value is: • **1234** if CNR_CCM_MODE=local • **1244** if CNR_CCM_MODE=regional
CNR_CCM_MODE=	CCM mode; set to **local** or **regional**.
CNR_CCM_TYPE=	Reserved for GSS installation. Introduced in Cisco Network Registrar 7.0; always set to **cnr**.
CNR_EXISTS=	If set to **y** (recommended), tries to kill any open CLI connections when installing or upgrading; otherwise, basically deprecated.
CNR_LICENSE_FILE=	For Cisco Network Registrar 7.*x* and later only, the fully qualified path to the license file.
DATADIR=	Fully qualified path to the data directory
JAVADIR=	Fully qualified path to the Java installation (JRE 1.5.0_6 or later).
KEYSTORE_FILE=	If USE_HTTPS=y, the fully qualified path to the keystore file.
KEYSTORE_PASSWORD=	If USE_HTTPS=y, the password used when generating the keystore file.
LOGDIR=	Fully qualified path to the log file directory.
PERFORM_BACKUP=	Specifies whether or not to back up the current installation files, if present. Can be set to **y** even on a clean installation (see also BACKUPDIR).
ROOTDIR=	Fully qualified installation path for the product files; contains bin, classes, cnrwebui, conf, docs, examples, extensions, lib, misc, schema, tomcat, and usrbin subdirectories.
START_SERVERS=	Sets whether or not to start the Cisco Network Registrar servers automatically at the end of the product installation. Should be set to **y** unless you explicitly want to manually start the servers.
TEMPDIR=	Fully qualified path to the temp directory.
USE_HTTP=	Sets whether or not the web UI server listens for HTTP connections; one or both of USE_HTTP or USE_HTTPS must be set to **y**.
USE_HTTPS=	Sets whether or not the web UI server listens for HTTPS connections; one or both of USE_HTTP or USE_HTTPS must be set to **y** (see also KEYSTORE_FILE and KEYSTORE_PASSWORD).
WEBUI_PORT=	Port number that the web UI uses for HTTP traffic; default value is: • **8080** if CNR_CCM_MODE=local • **8090** if CNR_CCM_MODE=regional
WEBUI_SEC_PORT=	Port number that the web UI uses for HTTPS traffic; default value is: • **8443** if CNR_CCM_MODE=local • **8453** if CNR_CCM_MODE=regional

Step 2 Use these commands to invoke the silent installation or upgrade for each instance:

- Windows:

  setup.exe -s -f1*path+response-file*

Note The silent installation fails if you do not specify the **–f1** argument with a fully qualified path to the response file, unless the response file is located in the i386 directory and setup.exe is run from that directory.

- Solaris:

  pkgadd -a *pkgdir***/nwreg2/install/cnradmin -d** *pkgdir* **-r** *response-file* **nwreg2**

- Linux:

  install_cnr -r *response-file*

Step 3 If you want to uninstall the product, invoke the silent uninstallation:

- Windows:

  uninst.exe -y -f"*install-dir***\DeIsL1.isu" -c"***install-dir***\unregistrar.dll"**

- Solaris:

  pkgrm -a *pkgdir***/nwreg2/install/cnradmin -n nwreg2**

- Linux (this command is noninteractive except during an error):

  uninstall_cnr

APPENDIX B

Lab Evaluation Installations

This appendix describes how to install, upgrade, and uninstall Cisco Network Registrar regional and local clusters on a single machine to support smaller test configurations for evaluation purposes.

Caution Installing the regional and local clusters on a single machine is intended only for lab evaluations, and should not be chosen for production environments. The aggregated regional cluster databases are expected to be too large to be reasonably located with a local server that is also running DNS or DHCP services. Running out of free disk space causes these servers to fail.

Installing Cisco Network Registrar in a Lab

To install Cisco Network Registrar on a single machine for evaluation purposes:

Step 1 Check whether the machine has enough disk space to accommodate two separate installations of Cisco Network Registrar.

Step 2 Install or upgrade the local cluster on the machine, according to the procedures in Chapter 2, "Installing and Upgrading Cisco Network Registrar." Specify the Local cluster installation. In Windows, do not reboot.

Step 3 Install or upgrade the regional cluster on the same machine, according to the same procedures. Specify the Regional cluster installation. In Windows, this time reboot.

Testing the Lab Installation

To test the installation:

Step 1 Start and log in to the web UI for the local cluster, using the URL appropriate to the port number. By default, the local port numbers are **8080** for HTTP connections and **8443** for HTTPS (secure) connections. In Windows, from the Start menu, choose **Network Registrar 7.2 local Web UI**.

Step 2 Add DNS zones and DHCP scopes, templates, client-classes, or virtual private networks (VPNs) as a test to pull data to the regional cluster.

Step 3 Start and log in to the web UI for the regional cluster, using the URL appropriate to the port number. By default, the regional port numbers are **8090** for HTTP connections and **8453** for HTTPS (secure) connections. In Windows, from the Start menu, choose **Network Registrar 7.2 regional Web UI**.

Step 4 Test the regional cluster for single sign-on connectivity to the local cluster. Try to pull DNS zone distributions, DHCP scopes, templates, client-classes, or VPNs from the local cluster to the regional replica database.

Uninstalling in a Lab Environment

If you need to uninstall Cisco Network Registrar, follow the procedure in the "Starting and Stopping Servers" section on page 2-13.

No option exists to uninstall only the regional or local cluster in a dual-mode installation environment.

APPENDIX C

Enhancing Security for Web UI

When connected through the Secured Socket Layer (SSL) protocol using HTTPS, the web UI uses the default ciphers for the Java Virtual Machine (JVM). These ciphers usually include weak cipher session keys and can affect system security. Therefore, you may want to adjust the ciphers to disable the use of weak ciphers in the web UI.

To adjust the ciphers:

Step 1 Open the **server.xml** file in the *install-path*/tomcat/conf folder in your Cisco Network Registrar installation folder.

Step 2 Add a *ciphers* statement to the HTTPS connector statement and list down the allowed ciphers as described in the following example:

Note The values for **port**, **keystoreFile**, and **keystorePass** must match the values that you have configured in your system.

```
<Connector port="8443"
           maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
           maxHttpHeaderSize="8192"
           enableLookups="false"
           disableUploadTimeout="true"
           acceptCount="100" scheme="https" secure="true"
           clientAuth="false"
           ciphers="SSL_RSA_WITH_RC4_128_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA"
           keystoreFile="conf/.keystore"
           keystorePass="changeit"
           sslProtocol="TLS" />
```

The *ciphers* attribute can carry a comma-separated list of encryption ciphers that this socket is allowed to use. By default, the web UI uses the default ciphers for the Java Virtual Machine (JVM). These contain the weak export-grade ciphers in the list of available ciphers. This results in the web UI supporting weak cipher session keys.

Note The ciphers are specified using the Java Secure Socket Extension (JSSE) cipher naming convention.

Step 3 Restart Cisco Network Registrar for the changes to take effect.

INDEX

A

Add License page, web UI 2-13
archive directories 2-8
archiving 2-8

C

CCM port 2-9
certificate file, importing 2-6
checklist, installation 2-1
ciphers
    adjusting C-1
CLI 1-1
    license set key command 2-13
    requirements 1-3
    starting 2-12
client-only installation 2-9
clusters
    local 2-7
    modes 2-7
    regional 2-7
cnr_status utility 2-10, 2-14
command line interface 1-1
connection type 2-9

D

database status 2-8
debug_install script 2-15
DHCP servers 1-1
disk space requirements 1-3
DNS servers 1-1

E

error logging 1-5, 1-6
excluding directories for virus scanning 1-4

G

gtar utility 2-6, 2-7
gzip utility 2-6

H

HTTP connection 2-9
HTTPS connection 2-9

I

install_cnr_log file 2-15
install_cnr utility 2-7, A-3
installation 2-1
    CCM port 2-9
    CD 2-6
    checklist 2-1
    cluster mode 2-7
    connection type 2-9
    directory 2-7
    JAVA_HOME setting 2-5
    Java directory 2-9
    JRE/JDK requirements 2-5
    lab evaluation B-1
    license keys 2-1
    log files
        install_cnr_log 2-15

lease_upgrade_log 2-15
modes
new 1-4
upgrade with data migration 1-4
upgrade without data migration 1-4
network distribution 2-6
noninteractive A-1
overview 1-1
process 2-3
processing messages 2-10
secure login 2-5
silent A-1
system privileges 2-5
troubleshooting 2-15
types 2-9
Web UI port 2-10

J

Java
directory 2-9
requirements 1-2
JAVA_HOME setting 2-5
Java Development Kit (JDK) 2-5
Java Runtime Environment (JRE) 2-5

K

keystore file 2-5
keytool utility 2-5, 2-6

L

lab evaluation installations B-1
lease_upgrade_log file 2-15
license keys 1-4, 2-1, 2-12
license set key command (CLI) 2-13
Linux
cnr_status 2-10, 2-14
gtar 2-6, 2-7
gzip 2-6
install_cnr 2-7, A-3
requirements 1-3
superuser/root accounts 2-5
uninstall_cnr 2-17
uninstallation 2-17
variable declaration file A-1
Local.sav directory 2-8
Local directory 2-7
local mode 2-7
log files 2-15
logging
server events 1-5, 1-6
startups 1-5, 1-6
Windows 1-5

N

Network Registrar, about 1-1
noninteractive installations A-1
nwreg2 package 2-7
nwreglocal utility 2-14
nwregregion utility 2-14

O

operating system
requirements 1-2
versions 1-3
overview 1-1
OVF 3-1

P

pkgadd utility 2-7, A-3
pkgask utility A-1

pkgrm utility 2-16, A-3
processing messages 2-10

R

RAM requirements 1-3
Regional.sav directory 2-8
Regional directory 2-7
regional mode 2-7
RIC servers 1-1
root accounts 2-5
router interface configuration servers 1-1

S

secure login 2-5
self-extracting executable 2-6
self-signed certificates 2-5
server agents, checking status 2-10
server-client installation 2-9
servers
  DHCP 1-1
  DNS 1-1
  logging events 1-5, 1-6
  RIC 1-1
  running with other 1-6
  starting/stopping 2-13
setup.exe file 2-6
silent installations A-1
Solaris
  cnr_status 2-10, 2-14
  gtar 2-6, 2-7
  gzip 2-6
  nwreg2 2-7
  nwreglocal and nwregregion 2-14
  pkgadd 2-7, A-1, A-3
  pkgrm 2-16, A-3
  requirements 1-3
  superuser/root accounts 2-5
  uninstallation 2-16
starting
  CLI 2-12
  logging when 1-5, 1-6
  servers 2-13
  Web UI 2-12
Start menu
  access 2-12
  setup 2-7
status of server agents 2-10
stopping servers 2-13
superuser accounts 2-5
system privileges 2-5

T

tail command 1-5
troubleshooting 2-15

U

uncompressing the media 2-6
uninst.exe utility A-3
uninstall_cnr utility 2-17
uninstallation 2-16
  lab evaluation B-2
  Linux 2-17
  Solaris 2-16
  Windows 2-16
unpacking the media 2-6, 2-7
upgrade 2-1
  archive directories 2-8
  archiving 2-8
  CCM port 2-9
  CD 2-6
  checklist 2-1
  cluster mode 2-7

cnr_mcdexport 2-3, 2-4, 2-5
connection type 2-9
database status 2-8
JAVA_HOME setting 2-5
Java directory 2-9
JRE/JDK requirements 2-5
lab evaluation B-1
license keys 2-1
network distribution 2-6
noninteractive A-1
overview 1-1
process 2-3
processing messages 2-10
secure login 2-5
silent A-1
system privileges 2-5
types 2-9
Web UI port 2-10
ciphers C-1
ports 2-10
requirements 1-3
starting 2-12
Windows
logging 1-5
program run location 2-7
requirements 1-3
self-extracting executable 2-6
setup.exe file 2-6
Start menu 2-7, 2-12
uninst.exe A-3
uninstallation programs 2-16

V

viewing server logs 1-5, 1-6
virtual appliance
automatic power up 3-8
booting and configuring 3-5
deploying 3-3
installing and configuring 3-2
managing 3-9
upgrading 3-9
virus scanning, excluding directories 1-4
VMWare vCenter 3-3
VMWare vSphere 3-3

W

web-based user interface 1-1
Web UI 1-1
Add License page 2-13