Installation and Upgrade Guide for CiscoWorks Network Compliance Manager 1.8

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-27499-01

Installation and Upgrade Guide for CiscoWorks Network Compliance Manager 1.8

CONTENTS

Preface

Introduction

This guide describes how to install and upgrade to CiscoWorks Network Compliance Manager (NCM) 1.8.

CiscoWorks NCM tracks and regulates configuration and software changes in a multivendor network environment. It provides visibility into network changes and tracks compliance with a broad variety of regulatory, IT, corporate governance, and technology requirements. CiscoWorks NCM helps IT staff identify and correct trends that could lead to problems, such as network instability and service interruption.

CiscoWorks NCM is integrated with CiscoWorks and is initially launchable from the CiscoWorks home page. CiscoWorks NCM is interoperable with other CiscoWorks applications, such as the LAN Management Solution (LMS) bundle through the Common Services Device Credential Repository (DCR).

Conventions

This document uses the following conventions:

Table 1 Document Conventions

Convention	Indication
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Information you enter	**`boldface screen`** `font`
Variables you enter	*`italic screen`* font
Menu items and button names	**boldface** font
Selecting a menu item in paragraphs	**Option > Network Preferences**
Required alternative keywords are grouped in braces and separated by vertical bars	{x | y | z}

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Tip Means the following information will help you solve a problem.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Accessing the CiscoWorks NCM Documentation Set

All or any part of the CiscoWorks NCM documentation set, including this document, might be upgraded over time. Therefore, we recommend that you access the CiscoWorks NCM documentation set using the following URL:
http://www.cisco.com/en/US/products/ps6923/tsd_products_support_series_home.html

Tip To cut and paste a two-line URL into the address field of your browser, you must cut and paste each line separately to get the entire URL without a break.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

CHAPTER 1

CiscoWorks NCM 1.8 Support Matrix

This chapter provides information about the system requirements and supported platforms for CiscoWorks NCM 1.8. It contains the following sections:

Supported Platforms

Table 1-1 lists the supported operating systems for the NCM application and the NCM satellite.

Note The NCM 1.8 application runs on 64-bit architecture only. For information about upgrading from a 32-bit architecture, see Upgrading to NCM 1.8 from a Different System or Upgrading to CiscoWorks NCM 1.8.

Table 1-1 NCM-Supported Operating Systems

Operating System	NCM Application Supported Versions	NCM Satellite Supported Versions
Windows Server 2008:		

Table 1-1 NCM-Supported Operating Systems (continued)

Operating System	NCM Application Supported Versions	NCM Satellite Supported Versions
x64 Datacenter Edition, SP2	X	None
R2 x64 Datacenter Edition, SP1	X	
x64 Enterprise Edition, SP2	X	
R2 x64 Enterprise Edition, SP1	X	
x64 Standard Edition, SP2	X	
R2 x64 Standard Edition, SP1	X	
Note: RSA device authentication is not yet available on Windows Server 2008. If you run NCM on a Windows operating system require RSA device authentication, you cannot install or upgrade to NCM 1.8 at this time.		
Linux:		
Red Hat Enterprise Linux Server AS 4.0 or later minor version		X
Red Hat Enterprise Linux Server 5.4 or later minor version through 5.6	X	X
Red Hat Enterprise Linux Server 6.0 or later minor version	X	
SUSE Linux Enterprise Server 9		X
SUSE Linux Enterprise Server 11 SP1	X	
Tip: Red Hat does not support direct upgrades from Red Hat Enterprise Linux Server 5.x to 6.0.		
Solaris:		
Oracle Solaris 10 SPARC	X	X

Note:

- Before installing NCM on a Solaris platform, reconfigure the Syslog server to not listen for remote Syslog messages.
- NCM on a Solaris system requires a large amount of swap space because of the way the `fork()` system call works. For example, forking a 24 GB process allocates 24 GB in the swap file, which guarantees space to swap out the new process if necessary. If the 24 GB is not available in swap, the `fork()` system call fails.

64-bit Support

CiscoWorks NCM uses the 64-bit Java Virtual Machine (JVM) on a Solaris platform. To increase the number of task throughput (number of tasks per hour), you can allocate more memory for the CiscoWorks NCM Management Engine process (the jboss server).

Note During an 32-bit to 64-bit upgrade, the Jboss_conf file will be overwritten and replaced. All the user configuration that were set in this file will be lost.

The memory allocated to CiscoWorks NCM is configured in the $CWNCM/server/ext/wrapper/conf/jboss_wrapper.conf file. To increase the memory allocation, edit the following lines in this file:

```
wrapper.java.initmemory=512
wrapper.java.maxmemory=512
wrapper.java.additional.3=-Xmn170m
```

Note The numbers are specified in megabytes.

For optimal performance, set the initial memory and maximum memory to the same value

Note After modifying the jboss_wrapper.conf file, you must restart CiscoWorks NCM from the command line (or Services applet on a Windows platform). If you restart CiscoWorks NCM from the Web UI, the changes to the jboss_wrapper.conf file will be lost.

A large amount of swap space is required due to the fork() system call on Solaris. When you fork a 24 GB process, Solaris allocates 24 GB in the swap file. If 24 GB is not available in swap, the fork() system call fails.

Note For all operating system upgrades, please refer to the vendor documentation or consult your system support personnel. Cisco is not responsible for issues that might arise during third-party product upgrades.

Solaris CLI Installer

For CiscoWorks NCM 1.8, the Solaris CLI installer supports 64-bit. As a result:

- The Solaris CLI installer automatically installs 64-bit CiscoWorks NCM.
- The Solaris Service Provider Interface (SPI) will upgrade 32-bit CiscoWorks NCM to 64-bit CiscoWorks NCM.
- When upgrading to 64-bit CiscoWorks NCM, all wrapper configuration files (such as jboss_wrapper.conf and syslog_wrapper.conf) will be overwritten. Any user-specified settings will be reset. For example, if you had set the Jboss_wrapper.conf file to start CiscoWorks NCM with 8 GB Java Heap memory, the setting will be overwritten to the CiscoWorks NCM default.

Supported Databases

CiscoWorks NCM supports the following core databases:

- Databases for Standalone NCM Core, page 1-3
- Databases for Multimaster Distributed System, page 1-4
- Databases for Horizontal Scalability, page 1-5

Databases for Standalone NCM Core

The NCM database can be installed on any supported platform. Table 1-2 describes the supported databases for a standalone NCM Core environment.

Table 1-2 Standalone NCM Core - Supported Databases

Database Version	Supported NCM Versions	Notes
Oracle 10g R2 (10.2.0.2, 10.2.0.4, or 10.2.0.5) Standard or Enterprise Edition	1.8 with or without patches	64-bit Oracle is supported.
Oracle 11g R1 (11.1.0.7) Standard or Enterprise Edition	1.8 with or without patches	
Oracle 11g R2 (11.2.0.1 or 11.2.0.2) Standard or Enterprise Edition	1.8 with or without patches	
Oracle Real Application Clusters (RAC) on Oracle 11g R2 (11.2.0.1 or 11.2.0.2) Enterprise Edition	1.8 with or without patches	
Microsoft SQL Server 2005 Standard or Enterprise Edition (SP2 or higher)	1.8 with or without patches	64-bit Microsoft SQL Server is supported.
Microsoft SQL Server 2008 Standard or Enterprise Edition	1.8 with or without patches	NCM does not support the use of Microsoft SQL Server Named Instances.
MySQL 5.0.58	1.8 with or without patches	The supported version of MySQL ships with NCM and runs on all NCM-supported operating systems.

It is recommended to run the NCM application and the NCM database on separate physical machines. In addition, the database server should be dedicated to NCM, rather than serving multiple applications.

Databases for Multimaster Distributed System

Table 1-3 describes the supported databases for a Multimaster Distributed System environment.

Table 1-3 Multimaster Distributed System - Supported Databases

Database Version	Supported NCM Versions	Limitations
Oracle 10g R2 (10.2.0.2, 10.2.0.4, or 10.2.0.5) Enterprise Edition	1.8 with or without patches	No more than five NCM Cores can be configured together.
Oracle 11g R1 (11.1.0.7) Enterprise Edition	1.8 with or without patches	
Oracle 11g R2 (11.2.0.1 or 11.2.0.2) Enterprise Edition	1.8 with or without patches	

Table 1-3 Multimaster Distributed System - Supported Databases (continued)

Database Version	Supported NCM Versions	Limitations
Microsoft SQL Server Standard or Enterprise Edition 2005 (SP2 or higher)	1.8 with or without patches	No more than two NCM Cores can be configured together. The maximum number of managed devices should not exceed 6,500. NCM does not support the use of Microsoft SQL Server Named Instances.
Microsoft SQL Server Standard or Enterprise Edition 2008	1.8 with or without patches	
MySQL	None	MySQL is not supported for Multimaster Distributed System environments.

For information about configuring a Multimaster Distributed System environment, see the *Configuration Guide for High Availability Distributed System on Oracle* or the *Configuration Guide for High Availability Distributed System on Microsoft SQL Server.*

Databases for Horizontal Scalability

Table 1-4 describes the supported databases for a Horizontal Scalability environment

Table 1-4 Horizontal Scalability - Supported Databases

Database Version	Supported NCM Versions	Limitations
Oracle 10g R2 (10.2.0.2, 10.2.0.4, or 10.2.0.5) Standard or Enterprise Edition	1.8 with or without patches	No more than five CWNCM application servers can be configured together with a single database.
Oracle 11g R1 (11.1.0.7) Standard or Enterprise Edition	1.8 with or without patches	
Oracle 11g R2 (11.2.0.1 or 11.2.0.2) Standard or Enterprise Edition	1.8 with or without patches	
Oracle Real Application Clusters (RAC) on Oracle 11g R2 (11.2.0.1 or 11.2.0.2) Enterprise Edition	1.8 with or without patches	
Microsoft SQL Server Standard and Enterprise Edition 2005 (SP2 or higher)	1.8 with or without patches	No more than five CWNCM application servers can be configured together with a single database. NCM does not support the use of Microsoft SQL Server Named Instances.
Microsoft SQL Server Standard and Enterprise Edition 2008	1.8 with or without patches	
MySQL	None	MySQL is not supported for Horizontal Scalability environments.

For information about configuring a Horizontal Scalability environment, see the *Horizontal Scalability User Guide for CiscoWorks Network Compliance Manager.*

Additional Required Applications

You need to install the following applications:

- CiscoWorks NCM supports the following browsers:
  - Microsoft Internet Explorer (32-bit and 64-bit) version 8 (not running in Compatibility
  - Microsoft Internet Explorer (32-bit and 64-bit) version 9 (not running in Compatibility
  - Mozilla Firefox 10.x ESR

The Firefox ESR (Extended Support Release) browser is available from http://www.mozilla.org/firefox/organizations/all.html.

- Adobe® Flash Player 9.x and above for the browser.
- Microsoft Excel 2000 or higher, if you are viewing Summary Reports from the CiscoWorks NCM server.
- Adobe® Acrobat Reader™ version 4.0 or higher if you are viewing CiscoWorks NCM documentation from the CiscoWorks NCM server.
- ActivePerl 5.8.x for Windows.
- Perl 5.8.x for Solaris and Linux (CiscoWorks NCM Convert-to-Perl script feature uses Perl).
- Perl Net::SSH::Expect module (for using the Connect module with SSH)

Note Third-party products mentioned in this documentation are manufactured by vendors independent of Cisco. Cisco makes no warranty, implied or otherwise, regarding the performance or reliability of these products.

Authentication

For NCM user authentication into the NCM user interface, NCM has been validated with the following authentication components:

- Microsoft Active Directory on Windows Server 2008 with Domain and Forest function level: Windows 2000
- Cisco Secure Access Control System version 3.1 for TACACS and RADIUS
- Cisco Secure Access Control System version 5.1 for TACACS
- OpenLDAP version 2.4.23
- On the NCM application server, RSA Authentication Manager version 6.1 with SecurID Software Tokens version 3.x and SoftID version 3.0.7 or 4.1 (needed for the Windows operating system only)
- Single sign-on from HP Server Automation (HP SA) 9.00
- Single sign-on from HP Operations Orchestration (HP OO) 9.00

For NCM user authentication into the command-line interface (through telnet or SSH proxy), NCM has been validated with the following authentication components:

- Microsoft Active Directory on Windows Server 2008 with Domain and Forest function level: Windows 2000
- Cisco Secure Access Control System version 3.1 for TACACS and RADIUS

- Cisco Secure Access Control System version 5.1 for TACACS
- OpenLDAP version 2.4.23

For device authentication from NCM, NCM has been validated with the following authentication components:

- Cisco Secure Access Control System version 3.1 for TACACS and RADIUS
- Cisco Secure Access Control System version 5.1 for TACACS
- On the NCM application server, RSA Authentication Manager version 6.1 with SecurID Software Tokens version 3.x and SoftID version 3.0.7 or 4.1

Note RSA device authentication is available on Windows 2003, 32-bit only.

Additional CiscoWorks NCM Configurations

If you have configured a High Availability Distributed System, the database requirements for Oracle and Microsoft SQL Server include:

Database	Restrictions
Oracle 10g Standard or Enterprise Edition (10.2.0.2 and 10.2.0.4)	No more than five CiscoWorks NCM Cores can be configured together.
Oracle 11g Standard or Enterprise Edition (R1, 11.1.0.7.0 or R2, 11.2.0.1.0)	No more than five CiscoWorks NCM Cores can be configured together.
Microsoft SQL Server Standard and Enterprise Edition 2005 (SP2 or higher) and 2008	No more than two CiscoWorks NCM Cores can be configured together. The maximum number of devices should not exceed 6500.

If you have configured a Horizontal Scalability environment, the database requirements for Oracle and Microsoft SQL Server include:

Database	Restrictions
Oracle 10g Standard or Enterprise Edition (10.2.0.4)	No more than five CiscoWorks NCM application servers can be configured together with a single database.
Oracle 11g Standard or Enterprise Edition (R1, 11.1.0.7.0 or R2, 11.2.0.1.0)	No more than five CiscoWorks NCM Cores can be configured together with a single database.
Microsoft SQL Server Standard and Enterprise Edition 2005 (SP2 or higher) and 2008	No more than five CiscoWorks NCM application servers can be configured together with a single database.

See the *High Availability Distributed System Configuration Guide for CiscoWorks Network Compliance Manager* for information on configuring High Availability Distributed System environment.

See the *Horizontal Scalability User Guide for CiscoWorks Network Compliance Manager* for information on configuring Horizontal Scalability environment.

Note High Availability and Horizontal Scalability environments are not supported for MySQL.

Virtual Environments

Note the following points while running CiscoWorks NCM in a virtual environment:

- VMWare guests can be run on a VMWare ESX 3.5 or VMWare ESX 4.0 server (preferred). It is important that the Disk I/O be split. The ESX server must have two arrays, one for the ESX operating system and one for the virtual machines.
- Use of Vmotion is not recommended.
- If you plan to use virtual machines for both CiscoWorks NCM and your database, ensure that they are running on different VMWare Guests. You must set a limit on managed devices and keep it low. It is recommended that you have the database on a different ESX host so that there is no conflicting I/O on the array.
- If you plan to run VMWare in a Distributed System or Horizontal Scalability environment, the maximum number of CiscoWorks NCM Cores should not exceed two.
- Some VMWare Guests can incur significant time drift. Syncing to an external time source can solve this issue.

The CiscoWorks NCM VMWare Guest system requirements are double that of standalone server requirements.

CiscoWorks NCM can be network intensive, therefore, if you have many virtual machines sharing a virtual switch and network interface card, you could experience unexpected behavior, including time-outs and failed tasks. In addition, each virtual environment is different and could function differently under loads with shared VM Guests.

If you are running CiscoWorks NCM in a virtual environment and there are performance issues, do the following:

- Increase hardware resources
- Ensure that resources are dedicated through your ESX Administrator
- Decrease the number of VMWare Guests running simultaneously
- Add a dedicated network interface card to the ESX server for CiscoWorks NCM to use exclusively

Significant performance degradation has been seen on ESX servers running multiple virtual machines, where one or more virtual machine was under heavy load. It is critical that the ESX server running CiscoWorks NCM in a virtual environment be properly resourced to avoid performance degradation.

Note The number of managed devices does not have as significant of an impact on performance as the number of concurrent tasks. If performance issues are seen, reduce the number of concurrent tasks and ensure that CiscoWorks NCM is getting the appropriate resources.

CiscoWorks NCM Alert Center Service

CiscoWorks NCM Alert Center is a unique Security Alert service that provides network vulnerability alerts. Unlike traditional alerts that are typically delivered via email, the CiscoWorks NCM Alert Center delivers alerts as CiscoWorks NCM software compliance policies. Using these alerts, you can easily identify the vulnerable devices across your network and perform remediation before your environment security is compromised.

Note CiscoWorks NCM Alert Center can also be installed on CiscoWorks NCM server that is not directly connected to the Internet. This environment is referred to as air gapped or standalone environment. See Installing CiscoWorks NCM Alert Center in an Air Gapped Environment for details.

See the *Getting Started Guide for CiscoWorks Network Compliance Manager Alert Center* and the *Installation and Configuration Guide for CiscoWorks Network Compliance Manager Alert Center* for information on installing and using CiscoWorks NCM Alert Center.

Summary Reports

The Summary reports are generated in the Microsoft Excel (.xls) format. You can either run the Summary reports from a Windows client computer connected to your CiscoWorks NCM server or you can use another program to view the Summary reports if you are running CiscoWorks NCM on a Linux or Solaris platform.

Hardware Requirements

Before installing NCM, verify that your application server meets the following minimum requirements

Note The NCM application server must have a static IP address.

If you are using an external database, for the database server hardware and operating system requirements, see the database documentation.

Supported Hardware

Table 1-5 lists the physical hardware NCM supports

Table 1-5 NCM-Supported Hardware

Processor	Supported Operating System Types	Notes
Intel® 64-bit (x86-64) AMD 64-bit (AMD64)	Windows Linux	• Minimum of 2.5GHz • 1 physical CPU with 6 cores and 12 logical processors with hyper-threading • NCM does not support the Intel Itanium® processor family.
Oracle SPARC64 VI or later (M-Series) Oracle SPARC T4 or later (T-Series)	Oracle Solaris	• Minimum of 2.5GHz • 1 physical CPU with 6 cores and 12 virtual processors • For co-resident NCM and HP Network Node Manager i Software (NNMi), use an M-Series processor.

Supported Virtual Servers

Table 1-6 lists the virtual servers NCM supports.

Table 1-6 NCM-Supported Virtual Servers

Virtual Server	Supported Operating System Types	Notes
VMWare: • ESX Server 3.5 • ESX 4.0 or later minor version • ESXi 4.1 or later minor version • ESXi 5.0 or later minor version	• Host OS: — Windows — Linux • Guest OS: Any of the operating systems listed in Table 1-1	• The virtual environment must meet the x86-64 or AMD64 hardware requirements listed in Table 1-5.
Microsoft® Hyper-V R2	• Host OS: Windows Server 2008 R2 x64 • Guest OS: Any of the Windows operating systems listed in Table 1-1	
Oracle Solaris Zones	Oracle Solaris	

If you are running NCM in a virtual environment, review the follow guidelines:

- Because NCM can be network intensive, many virtual machines sharing a virtual switch and network interface card could result in unexpected behavior, including time-outs and failed tasks.
- Each virtual environment is different and could function differently under loads with shared VM guests.
- On a virtual server, it is recommended that the Disk I/O be split. The virtual server must have two arrays:
  - One array for the host operating system
  - One array for the virtual machines

- Live migration (for example, using Vmotion) of the NCM application server is not recommended.
- If you plan to use virtual machines for both the NCM application and the NCM database, ensure that they are running on different guests. It is recommended to host the database virtual machine on a different array to avoid conflicting I/O on the array. Verify that the database is supported in a virtual environment.
- When configuring NCM on virtual machines in a Multimaster Distributed System environment or a Horizontal Scalability environment, the maximum number of NCM application servers is two.
- Some virtual guests time drift, which can be an issue and should be corrected. Synchronizing the guests to an external time source can solve this issue.
- Each NCM guest system must be configured with a set reservation for CPU and memory. These reservations should be at least 125% of the standalone server requirements listed in System Configuration Requirements. Ensure that the resource pool containing the NCM guest system has adequate resources to consistently deliver the CPU and memory reservations to the NCM guest system.

Performance Issues

To counter performance issues while running NCM in a virtual environment, do the following:

- Increase hardware resources on the physical host.
- Ensure resources are dedicated to the NCM application server guest.
- Decrease the number of guests running simultaneously.
- Add a network interface card dedicated to NCM to the virtual server.

A large number of concurrent tasks increases NCM resource demand. If performance issues arise, reduce the number of concurrent tasks or provide more resources to the NCM virtual server. (This suggestion also applies to physical servers.)

Troubleshooting and Support

Cisco Support will endeavor to support NCM in a virtual environment, and Cisco does not require customers to recreate and troubleshoot every product issue in a non-virtual environment. However, Cisco reserves the right to request that customers diagnose certain issues in a native, certified operating system environment without the virtual image. Cisco will only make this request when there is strong indication to believe that the virtual environment is a contributing factor to the issue.

RAM, Swap/Disk Space, and Network Requirements

Table 1-7 lists the approximate minimum requirements and reflects levels tested by Cisco. If you have a particularly complex environment, you might want to provision more powerful hardware.

Table 1-7 System Configuration Requirements

Server	Memory	Swap Space	Disk
Separate Application Server	16 GB RAM	16 GB[1]	40 GB

Table 1-7 System Configuration Requirements (continued)

Server	Memory	Swap Space	Disk
Separate Database Server	16 GB RAM	16 GB	512 GB, Fast SCSI
Combined Application Server and Database Server	16 GB RAM	16 GB	512 GB, Fast SCSI

1.NCM on a Solaris system requires a large amount of swap space because of the way the `fork()` system call works. For example, forking a 24 GB process allocates 24 GB in the swap file, which guarantees space to swap out the new process if necessary. If the 24 GB is not available in swap, the `fork()` system call fails.

When the application and database servers are different systems, the connection between the servers should be at least 100 Mbps Fast Ethernet, full duplex.

Port Utilization

NCM communicates with devices using a combination of protocols and ports. If you use a given protocol, NCM requires access to the corresponding port. Specifically, if NCM communicates with devices protected by firewalls, these ports must be open, or you must use an alternative means of communication, such as an NCM Satellite server.

Operating Systems

International Language Support

CiscoWorks NCM 1.8 can be installed on an operating system running under the following non-English locales or character sets:

- UTF-8
- GB2312 for Simplified Chinese
- Shift-JIS for Japanese
- EUC-KR for Korean

Note To switch the locale of an English Win03 platform to Asian languages, double byte character set (DBCS) support must be enabled.

During CiscoWorks NCM installation, you are prompted to select a Collation Type while configuring a new Microsoft SQL Server database.

Microsoft SQL Server collation dictates the character set that is stored in the database. For example, if you select a Chinese collation, you can enter only Chinese characters. However, you can always enter Latin characters regardless of the collation type you select.

CiscoWorks NCM 1.8 supports the following collections apart from SQL_Latin1_General_CP1_CI_AS:

- Chinese_PRC_CI_AS
- Japanese_CI_AS
- Korean_Wansung_CI_AS

CiscoWorks NCM 1.8 supports UTF-8 non-English Oracle locales.

You can enter the following information in the language that you select:

- Comment fields
- Description fields
- Custom data labels
- Most name and text fields, such as device location and vendor

Note CiscoWorks NCM 1.8 does not support any language other than English when MySQL is used as the back-end database.

You can search on single and multi-byte character sets, as long as the field being searched accepts them. You can also import and export configuration policies that contain single and multi-byte character sets.

For more information on collation, refer to your DBMS documentation.

CHAPTER 2

Upgrading to NCM 1.8 from a Different System

NCM 1.8 must run on a 64-bit operating system.

This chapter describes the procedure for upgrading from NCM 1.4x, 1.5x, or 1.6x running on a standalone NCM application server to NCM 1.8 running on a different standalone NCM application server. If the NCM application server is currently running NCM1.3x, see Upgrading to CiscoWorks NCM 1.8.

For information about upgrading other NCM environments, see the appropriate documentation:

- NCM Multimaster Distributed System

  For information about upgrading NCM in a Distributed System environment, see Upgrade the NCM Mesh in the Configuration Guide for High Availability Distributed System on Oracle or the Configuration Guide for High Availability Distributed System on Microsoft SQL Server . Come back to this chapter when directed to do so in the upgrade procedure.

- NCM Horizontal Scalability

  For information about upgrading NCM in a Horizontal Scalability environment, see Upgrading Horizontal Scalability in the Horizontal Scalability User Guide for CiscoWorks Network Compliance Manager 1.8. Come back to this chapter when directed to do so in the upgrade procedure.

- NCM Satellites

  If you are using NCM Satellites, after installing the current version of NCM, run the "Deploy Remote Agent" task to re-install the upgraded Satellite agent on all of the remote Gateways. For information, see the Upgrading the Satellite section of the Satellite User Guide for CiscoWorks Network Compliance Manager 1.8.

NCM services are not available during the upgrade process. In addition, after you run the NCM Service Pack Installer, you cannot roll back to the previous version of NCM.

This chapter contains the following sections:

Upgrade and Installation Caveats

When installing or upgrading NCM, note the following:

- This documentation supports upgrades of NCM on the same operating system type only. For help moving NCM to a different operating system, contact HP Professional Services.
- The NCM Installer does not perform any sort of version checking. As a result, you could complete installations or upgrades on unsupported platforms.
- If you run a 64-bit NCM full install or a Service Pack install on a 32-bit platform, the NCM Installer will start and then quit without any error message.
- The Windows version of the NCM Installer includes a black CLI window that runs in the background. Do not close this window or the install will end without prompting you. In addition, when performing NCM installs over the network, for example running the `hpna_win.exe` installer from a remote share, you will see the black CLI window for several minutes.

Restoration of Previous Customizations

During the NCM upgrade, the NCM Setup program automatically backs up critical NA files.

After upgrading NCM, the installer automatically restores the following files:

- Device software images from the backup directory are copied to `$NCM_HOME/server/images`.
- Summary reports from the backup directory are copied to `$NCM_HOME/addins`.
- NCM LiveNetwork content files are copied to `$NCM_HOME/content`.
- If you selected the use the previous administrative settings option during installation, the `site_options.rcx` and `adjustable_options.rcx` file from the backup directory are copied to `$NCM_HOME/jre`.
- The SecurID token file is restored.
- The Gateway encryption key is restored.
- The SSL public key certificate is restored.
- The license.dat file is restored if you do not have a new license file.

The following files are backed up. However, they are not restored during the NCM upgrade:

- Most `.rcx` files in the `$NCM_HOME/jre` folder.
  - Aside from the `site_options.rcx` and `adjustable_options.rcx` files, changes in other `.rcx` files will not be preserved.
  - If you have customized the NCM summary reports template or specification, such as adding additional report tabs, manually update the customized settings from the backed up version of the `reporting.rcx` file to the new version of the `reporting.rcx` file.
  - If you changed other `.rcx` files in the previous installation and want to keep those changes after upgrading, add those changes into the new `adjustable_options.rcx` file. You cannot use the previous `.rcx` file to overwrite the new version. Doing so could cause the application to fail.
- `$NCM_HOME/server/ext/jboss/server/default/conf/log4j.xml` file.
  - As of NCM 1.8, the `log4j.xml` file is no longer used. The comparative file is `$NCM_HOME/server/ext/jboss/server/default/deploy/jboss-logging.xml`.

  - To restore previous settings, manually edit the `jboss-logging.xml` file with the customizations in the the `log4j.xml file`. Note that the configuration formats differ between the two files.
- Wrapper configuration files in `$NCM_HOME/server/ext/wrapper/conf`.
  - If you selected the use the previous administrative settings option during installation, the upgrade installer attempts to merge the settings from the backed up version of the `jboss.conf` file to the new `jboss.conf` file. Verify the configuration in the new file.
  - To restore previous settings in other `.conf` files, manually edit the corresponding file after upgrading. You cannot use the previous file to overwrite the new version. Doing so could cause the application to fail.

Upgrade Procedure

The following steps provide an outline for upgrading NCM from a standalone NCM application server to a different standalone NCM application server. In this procedure, Server X identifies the source (existing) NCM application server and Server Y identifies the target (new) NCM application server.

Caution Do not upgrade Oracle or SQL Server while upgrading NCM across application servers. If you need to upgrade the database product for a standalone NCM application server, complete this procedure, and then upgrade the database product as described in Database Upgrades, page 3-3

Step 1 Verify the current NCM version.

If the NCM application server is currently running NCM 1.3x, follow the upgrade procedure in Upgrading to CiscoWorks NCM 1.8 before completing this procedure.

If the NCM application server is currently running NCM 1.4x, 1.5x, or 1.6.x, continue with this procedure.

Step 2 Determine the NCM database name and database user name.

In the NCM console, on the **Admin > System Status** page, locate the DatabaseMonitor row, and then click **Run Now** in that row.

On the **Monitor Results** page, locate the values for `Database catalog` (the database name) and `Database user name`.

Step 3 On Server X, stop all NA services.

Windows: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Stop**:

- TrueControl ManagementEngine
- TrueControl FTP Server
- TrueControl SWIM Server
- TrueControl Syslog Server
- TrueControl TFTP Server

UNIX: Run the following command:

```
/etc/init.d/truecontrol stop
```

Step 4 On Server X, if a gateway is installed on the NCM application server, stop that gateway:

```
/etc/init.d/opswgw-<gatewayName> stop
```

Step 5 On Server X, package (zip or tar) the entire NCM directory to one file that maintains file permissions during transfer.

Windows: For example, if the NCM installation directory is `C:\NCM`, from `C:`, compress the `NCM` folder to a file named `NCM.zip`.

Linux: For example, if the NCM installation directory is `/opt/NCM`, from `/opt`, tar the `NCM` directory to a file named `NCM.tar` by running the following command:

```
tar -cpf NCM.tar NCM
```

Step 6 Back up all of the data in the database. For instructions, see the database documentation or contact your database administrator (DBA).

For MySQL, use a command similar to the following example:

```
mysqldump -u root -p -h 127.0.0.1 --database NCM > NAdump.sql
```

For the MySQL examples in this procedure, the database user name is root, and the database name is NA.

Step 7 Prepare Server Y with a supported version of the operating system in use on Server X.

Step 8 Copy the entire NCM directory from Server X to the same location on Server Y. Retain permissions on the files.

Windows: For example, use an application such as WinSCP to transfer the `NCM.zip` file from Server X to Server Y, and then uncompress or unzip the file into `C:\` on Server Y.

Linux: For example, use the scp command (`scp -rp NCM.tar root@ServerY:/opt`) to transfer the `NCM.tar` file from Server X to Server Y, and then untar the file into `/opt`.

At this point, you have the older NCM client on the newer server.

Step 9 *UNIX only.* Copy the NCM startup files (`/etc/truecontrol` and `/etc/init.d/truecontrol`) from Server X to the same location on Server Y. Retain permissions on the files. For example:

```
scp -rp /etc/truecontrol root@ServerY:/etc
scp -rp /etc/init.d/truecontrol root@ServerY:/etc/init.d
```

Step 10 If you are using the embedded database, do the following:

a. On Server Y, install MySQL using the installer on the NCM Service Pack Installer DVD. Run the correct installer for the operating system type.

b. On Server Y, in MySQL, connect to the database, and then create a new database instance with the same name and user as the NCM database on Server X. For example:

```
mysqldump -u root -p -h 127.0.0.1
CREATE DATABASE NCM
```

c. If the MySQL configuration for the NCM database has been modified on Server X, replicate the configuration changes on Server Y.

MySQL provides configuration files at several levels. You must know which, if any, have been changed. The global configuration file is commonly located as follows:

- *Windows*: `<Drive>:\MySQL\my.ini`
- *UNIX*: `/etc/my.cnf`

Determine which MySQL configuration files have been modified for the NCM database, and then do one of the following:

- Copy these files from Server X to the same location on Server Y. Retain permissions on the files.
- Edit the MySQL configuration files on Server Y to match those on Server X.

d. Copy the database backup file from Server X to Server Y.

   Ensure that the database user has read access to the database backup file.

e. On Server Y, import the data from the NCM database backup into the new database instance created in *step b*. For example:

```
mysql -u root -p NA < NAdump.sql
```

f. On Server Y, delete any existing `*.backup` files from the `$NCM_HOME/server/lib/scripts/Database/Truecontrol` directory.

g. Ensure that the database server is running.

h. On Server Y, run the NCM 1.8 Service Pack Installer as described in Running the CiscoWorks NCM 1.8 Service Pack Installer.

Note If the upgrade fails, save all log files to a location outside the NCM directory structure before re-running the upgrade.

i. On Server Y, if NCM uses a MySQL database, check the MySQL configuration as described in Verify the MySQL Configuration.

Step 11 If Server Y runs the Linux operating system and if NCM uses a MySQL database, verify that the `/etc/hosts` file contains the following line:

```
127.0.0.1      localhost
```

The NCM-installed MySQL requires the localhost line exactly as shown here. To expand the information in the hosts file, add new lines containing the additional definitions.

Step 12 *Optional*. Use the optimized Data Pruning task as described in Data Pruning.

Step 13 On Server Y, install the latest NCM Driver Pack as described in .

Step 14 On Server Y, upgrade any additional NA components as described in .

Step 15 On Server Y, if a gateway was installed on Server X, install the gateway as described in t*he Satellite User Guide for CiscoWorks Network Compliance Manager 1.8*.

Running the NCM 1.8 Service Pack Installer

Before running the NCM Service Pack Installer, ensure that the database server is running.

The NCM Service Pack Installer sets the Java virtual machine (JVM) heap size in relation to the amount of system RAM and the number of processors. Generally speaking, the installer sets the JVM heap size to half of the RAM. (The NCM installer does not explicitly set the size of the young generation, so this value defaults to 1/3 of the JVM heap size.) Note the following exceptions:

- If the heap size is already set to a larger value than the NCM Service Pack Installer would set, the NCM Service Pack Installer does not change that value.
- If the NCM application server has more than 64GB of RAM, the NCM installer sets the JVM heap size to 32GB.
- If HP Network Node Manager i Software is already installed on the NCM application server, the NCM installer sets the JVM heap size to 512MB regardless of the system RAM size. In this case, the NCM installer sets the JVM permanent generation garbage collection (PermGen) to 128MB.

This section describes running the NCM 1.8 service Pack installer on different types of operating systems:

- Running the Service Pack Installer on a Windows Operating System
- Running the Service Pack Installer on a Linux Operating System
- Running the Service Pack Installer on a Solaris Operating System

Running the Service Pack Installer on a Windows Operating System

For upgrading on a Windows platform, insert the NCM Service Pack Installer DVD into the DVD drive and do the following:

Step 1 On the Windows taskbar, click Start, then click Run.

Step 2 Enter: `[drive]:\windows_[nnnn]-[mmddyy]_spi_setup.exe`, where `[drive]` is the letter of your DVD drive, `[nnnn]` is the build number, and `[mmddyy]` is the build date.

Step 3 Click OK.

Step 4 Follow the instructions on the screen.

Running the Service Pack Installer on a Linux Operating System

If you are installing the NCM Service Pack Installer on an NCM Linux server, insert the DVD into the DVD drive and mount it. You must have root access to run the NCM Service Pack Installer.

Step 1 `cd /[DVD_MOUNT_POINT]`, where `[DVD_MOUNT_POINT]` is the location of the DVD drive.

Step 2 `cd linux`

Step 3 Set the environment variable using the following commands: `TZ=UTC` and `export TZ`.

Step 4 `sh linux_[nnnn]-[mmddyy]_spi_setup_64.bin`, where `[nnnn]` is the build number and `[mmddyy]` is the build date.

Step 5 Follow the instructions on the screen.

If you see the following errors in the log file, verify the value of the `TZ` environment variable, and then restart the NCM Service Pack Installer:

```
SQLException while trying to connect to the database.
java.sql.SQLException: ORA-00604: error occurred at recursive SQL level 1
RA-01882: timezone region not found
```

Running the Service Pack Installer on a Solaris Operating System

If you are installing the NCM Service Pack Installer on an NCM Solaris server, insert the DVD into the DVD drive and mount it. You must have root access to run the NCM Service Pack Installer.

Tip On Solaris, the NCM Service Pack Installer supports 64-bit. As a result, on a 64-bit operating system the installer automatically installs 64-bit NCM. The installer also upgrades 32-bit NCm to 64-bit NCM.

Step 1 `cd /[DVD_MOUNT_POINT]` where `[DVD_MOUNT_POINT]` is the location of the DVD drive.

Step 2 cd solaris

Step 3 Set the environment variable using the following commands: `TZ=UTC` and `export TZ`.

Step 4 `sh solaris_[nnnn]-[mmddyy]_spi_setup_64.bin`, where `[nnnn]` is the build number and `[mmddyy]` is the build date.

Step 5 Follow the instructions on the screen.

If you see the following errors in the log file, verify the value of the `TZ` environment variable, and then restart the NCM Service Pack Installer:

```
SQLException while trying to connect to the database.
java.sql.SQLException: ORA-00604: error occurred at recursive SQL level 1
RA-01882: timezone region not found
```

Verify the MySQL Configuration

The following MySQL configuration options affect NCM performance:

- Large device configurations can exceed the default packet size configured for MySQL, resulting in an error similar to the following example:

  ```
  DeviceDataManagementEJB: Exception in addDeviceData -
  com.mysql.jdbc.PacketTooBigException: Packet for query is too large.
  ```

  To avoid this problem, increase the maximum packet size that MySQL accepts to at least 16MB. If the error still occurs after adjusting this value, increase it further, up to a maximum of 1GB.

- Restricting MySQL to a small number of concurrent threads can reduce NCM performance. (On prior versions of NCM, the default number was 10.) To avoid this problem, in the MySQL configuration file, set the number of concurrent threads to 20, which the NCM-installed version of MySQL interprets as “infinite threads.”

To set the MySQL configuration as described here, follow these steps:

Step 1 Determine which file to modify.

If no other applications use this installation of MySQL, you can modify the global configuration file, which is commonly located as follows:

  - *Windows*: *<Drive>*`:\MySQL\my.ini`
  - *UNIX*: `/etc/my.cnf`

If any other application uses this installation of MySQL, determine whether to modify the global configuration or a more-specific configuration.

Step 2 Back up the file identified in step 1.

Step 3 Open the configuration file in a text editor, such as WordPad or vi.

Step 4 To set the MySQL permitted packet size to 16MB, edit the configuration file as follows:

a. Locate the line that contains the `string max_allowed_packet=`.

If this line does not exist, create it in the next step.

b. Increase the allocation by updating this line to read:

```
max_allowed_packet=16776192
```

Step 5 To set infinite thread concurreny, edit the configuration file as follows:

a. Locate the line that contains the string `innodb_thread_concurrency=`.

b. Set infinite thread concurrency by updating this line to read:

```
innodb_thread_concurrency=20
```

Step 6 Save the configuration file.

Step 7 Stop all NCM services:

Windows: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Stop**:

- TrueControl ManagementEngine
- TrueControl FTP Server
- TrueControl SWIM Server
- TrueControl Syslog Server
- TrueControl TFTP Server

UNIX: Run the following command:

```
/etc/init.d/truecontrol stop
```

Step 8 Restart MySQL:

Windows: Open the Services control panel. In the list of services, right-click the MySQL service, and then click **Restart**.

UNIX: Run the following command:

```
/etc/init.d/mysql restart
```

Step 9 Start all NCM services:

Windows: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Start**:

- TrueControl ManagementEngine
- TrueControl FTP Server
- TrueControl SWIM Server
- TrueControl Syslog Server
- TrueControl TFTP Server

UNIX: Run the following command:

```
/etc/init.d/truecontrol restart
```

Data Pruning

The NCM 1.8 Data Pruning task is optimized from that of previous versions of NCM. To take advantage of this optimization, verify that the Data Pruning task is scheduled to run at least weekly

Note In a Distributed System or Horizontal Scalability environment, it is recommended to run the Data Pruning task manually on one NCM application server until the warning message does not appear. At that point, verify that the Data Pruning task is scheduled to run at least weekly on each core.

After upgrading NCM, the first several runs of the Data Pruning task might exceed the configured maximum task time. In this case, you might see the following warning message:

```
com.rendition.pruner.ConfigPruner: The task thread was interrupted. Pruning partially completed.
```

This message indicates that additional records can be pruned. No action is necessary; subsequent runs of the Data Pruning task will clear the additional records.

Tip If the database configuration includes redo logs, ensure that adequate disk space is available for these logs, especially while the warning message appears. The required size depends on the database configuration and the size of the NCM database.

To complete database cleanup faster, do either or both of the following steps:

- Temporarily increase the value of Max Task Length to a value such as 18000 (5 hours). This setting is under Tasks on the Admin > Administrative Settings > Server page in the NA console.

Tip After the warning message no longer appears, reset the Max Task Length to the original value (3600 by default).

- Run the Data Pruning task manually until the warning message does not appear.

Upgrading Additional CiscoWorks NCM Components

The following additional components must be upgraded when upgrading CiscoWorks NCM:

- CiscoWorks NCM High Availability Distributed System—After upgrading to CiscoWorks NCM 1.8, you must update your High Availability Distributed System environment. See the *High Availability Distributed System Configuration Guide for CiscoWorks Network Compliance Manager* for detailed information.
- CiscoWorks NCM Horizontal Scalability—If you are using the CiscoWorks NCM Horizontal Scalability functionality, see the *Horizontal Scalability User Guide for CiscoWorks Network Compliance Manager* for detailed instructions on installing and configuring the Horizontal Scalability software.
- CiscoWorks NCM Satellites—If you are using the CiscoWorks NCM Satellite agent, after installing CiscoWorks NCM 1.8, you must run the Deploy Remote Agent task to re-install the upgraded Satellite agent on all remote Gateways. See the *Satellite User Guide for CiscoWorks Network Compliance Manager* for detailed information.

CiscoWorks NCM AAA Log Reader

If you are using the AAA Log Reader on your AAA server to provide real-time change detection, you must update the AAA Log Reader after installing CiscoWorks NCM 1.8. To do this:

Step 1 Backup the AAA Log Reader directory on your AAA server.

Step 2 Copy the truecontrol-client.jar file located in the AAA folder on the Install CD to the AAA Log Reader directory. Overwrite the existing file.

Step 3 Change the following four options in the agent.rcx file for correct error logging to appear in the aaa_wrapper.log.

Change

```
[option name="log/AAALogReader"]System.out[option]
[option name="log/AAALogReader/level"]0[ooption>
[option name="log/connect"]System.out[option]
[option name="log/connect/level"]75[option]
```

To:

```
[option name="log/External/AAALogReader"]System.out[option]
[option name="log/External/AAALogReader/level"]0[option]
[option name="log/System/Authenticate"]System.out[option]
[option name="log/System/Authenticate/level"]75[option]
```

Note It is recommended that you install the JRE version 1.6.0 on AAA Server. The various JRE installations can be found on the CiscoWorks NCM Core Software DVD at: /add-ons/jre/.

CiscoWorks NCM Syslog Reader

CiscoWorks NCM uses Syslog messages to detect device changes in real-time. Some environments require the use of a Syslog Reader to forward messages from the Syslog server to CiscoWorks NCM. Typically, the Syslog Reader is required only when a central Solaris Syslog server is in use (because Solaris is not RFC-compliant for Syslog).

To upgrade the Syslog Reader:

Step 1 Go to /usr/local/CWNCM/syslogreader/probe.rcx.

Step 2 In the probe.rcx file, edit the following lines:

```
[option name="connect/AppServerURL"]SERVERNAME:1099[/option]
[option name="SyslogReader/LogFile/FileName"]SOMEPATH/FILE[/option]
```

Step 3 Stop the Syslog Reader.

Step 4 Run the **/etc/init.d/truecontrol.syslogreader stop** command.

Step 5 Remove the /usr/local/CWNCM directory.

Step 6 Follow the install instructions in the ReadMe.txt file.

CHAPTER 3

Upgrading to CiscoWorks NCM 1.8

This chapter describes how to upgrade to CiscoWorks NCM 1.8 from previous releases of Ciscoworks NCM.

This chapter contains the following sections:

Note CiscoWorks NCM 1.8 supports direct upgrade from Ciscoworks NCM 1.3.x or higher releases.

Getting Started

This section includes information on upgrading from CiscoWorks NCM 1.3.x or higher releases to CiscoWorks NCM 1.8.

Note CiscoWorks NCM services are not available during the upgrade process. You cannot rollback to the previous version of CiscoWorks NCM after upgrading to CiscoWorks NCM 1.8.

CiscoWorks NCM 1.3.x Users

For CiscoWorks NCM 1.3.x users upgrading to CiscoWorks NCM 1.8, you must:

1. If you are using MySQL 3.23.55 as the database platform, run the MySQL Upgrade Installer to upgrade to MySQL 5.0.58. See Running the MySQL Upgrade Installer, page 3-4 for information on the MySQL Upgrade Installer.
2. Run the CiscoWorks NCM 1.8 Service Pack Installer. See Running the CiscoWorks NCM 1.8 Service Pack Installer, page 3-7 for information on running the CiscoWorks NCM 1.8 Service Pack Installer.

Note To ensure that no settings or files are lost during an upgrade, backup the entire CiscoWorks NCM directory to a safe location before starting the upgrade. The current CiscoWorks NCM upgrade process does not restore the <NCM_Install_Dir>\jre\reporting.rcx file. If you have customized the CiscoWorks NCM Summary Reports template or specification, such as adding additional report tabs, manually update the customized settings from the backed up version of the files to the new installed version of the file.

CiscoWorks NCM 1.4.x, 1.5.x, and 1.6.x Users

For CiscoWorks NCM 1.4.x and greater users, you can upgrade directly to CiscoWorks NCM 1.8. See Installing CiscoWorks NCM 1.8, page 4-1 for information on installing CiscoWorks NCM 1.8.

Upgrading to CiscoWorks NCM 1.8

The following steps provide an outline for single CiscoWorks NCM 1.8 Core upgrade on Windows, Solaris, and Linux platforms:

Step 1 Stop all CiscoWorks NCM services. See Starting/Stopping CiscoWorks NCM Services, page 7-1 for instructions.

Step 2 To ensure that no settings or files are lost during the upgrade, backup the entire CiscoWorks NCM directory to a safe location. For example, if you installed CiscoWorks NCM in c:\cisco\CWNCM, backup the entire directory to a safe location.

Step 3 Backup the CiscoWorks NCM database. See Backing Up the CiscoWorks NCM Database, page 3-12 for information on backing up your database.

Step 4 Run the CiscoWorks NCM 1.8 Service Pack Installer. See Running the CiscoWorks NCM 1.8 Service Pack Installer, page 3-7 for instructions.

Step 5 Install the latest CiscoWorks NCM Driver Pack.

Note the following points while installing or upgrading to CiscoWorks NCM 1.8:

- The CiscoWorks NCM 1.8 Installer does not perform any sort of version checking, therefore, it allows installation and upgrade even on unsupported platforms.
- If you run a 64-bit CiscoWorks NCM full install or a Service Pack install on a 32-bit platform, the CiscoWorks NCM Installer will start and then quit without any error message.
- The Windows version of the CiscoWorks NCM 1.8 Installer includes a black CLI window that runs in the background. Do not close this window or the install will end without prompting you.

Operating System Upgrades

While upgrading to CiscoWorks NCM 1.8, if you are moving from a deprecated operating system to a supported operating system, do the following:

Step 1 Stop CiscoWorks NCM.

Step 2 Backup the CiscoWorks NCM folder. See Backing Up CiscoWorks NCM Files, page 3-13 for instructions.

Step 3 Upgrade the operating system.

Step 4 Restart CiscoWorks NCM and verify that CiscoWorks NCM is working properly.

Step 5 Follow the CiscoWorks NCM 1.8 upgrade procedure.

Note For all operating system upgrades, please refer to the vendor documentation or consult your system support personnel. Cisco is not responsible for issues that might arise during third-party product upgrade.

Database Upgrades

While upgrading to CiscoWorks NCM 1.8, if you are moving from a deprecated version of the database to a supported version of the database, do the following:

Step 1 Stop CiscoWorks NCM.

Step 2 Backup the CiscoWorks NCM database. See Backing Up the CiscoWorks NCM Database, page 3-12 for instructions.

Step 3 Upgrade the database. For MySQL, see Running the MySQL Upgrade Installer, page 3-4.

Step 4 Restart CiscoWorks NCM and verify that CiscoWorks NCM is working properly.

Step 5 Follow the CiscoWorks NCM 1.8 upgrade procedure.

If after upgrading to CiscoWorks NCM 1.8 you experience performance issues, such as the CiscoWorks NCM Home page taking a long time to load, it is recommended that your Oracle DBA perform a re-index of the tables in the CiscoWorks NCM database instance.

Note For all database upgrades, please refer to the vendor documentation or consult your database administrator. Cisco is not responsible for issues that might arise during third-party product upgrades.

Operating System and Database Upgrades

For upgrading both the operating system and the database, do the following:

Step 1 Stop CiscoWorks NCM.

Step 2 Backup the CiscoWorks NCM folder. See Backing Up CiscoWorks NCM Files, page 3-13 for instructions.

Step 3 Backup the CiscoWorks NCM database. See Backing Up the CiscoWorks NCM Database, page 3-12 for instructions.

Step 4 Upgrade the operating system.

Step 5 Upgrade the database.

Step 6 Restart CiscoWorks NCM and verify that CiscoWorks NCM is working properly.

Step 7 Follow the CiscoWorks NCM 1.8 upgrade procedure.

Running the MySQL Upgrade Installer

If you are using MySQL as your CiscoWorks NCM database and upgrading from a NCM release prior to CiscoWorks NCM 1.4, you must run the MySQL Upgrade Installer.

Before you perform the MySQL update, ensure that:

- The existing MySQL 3.23.55 database is working properly with CiscoWorks NCM.
- The existing MySQL 3.23.55 database is installed on one of the following OS platforms:
  - Windows 2000 Server and 2003 Server
  - Red Hat Linux AS 3, Red Hat Linux AS 4, SuSE Linux 9
  - Solaris 10 (Solaris 9 is not supported. You must upgrade to Solaris 10 before upgrading MySQL.)
- CiscoWorks NCM services have been stopped.

Windows Platform

To upgrade to MySQL 5.0.58 on a Windows platform, do the following:

Step 1 Double click the **mysql-5.0.58-[*nnnn*]-[*mmddyy*]-windows.exe** installer file, where [*nnnn*] is the build number and [mmddyy] is the date on which the MySQL Update Installer was built.

Step 2 Click **Next** after reading the introduction.

Step 3 Click **Upgrade Existing MySQL to Version 5.0.58**, and then click **Next**.

Step 4 Ensure that both MySQL Install folder and MySQL Data folder are correctly specified, and click **Next**.

The MySQL Install folder is the folder where the existing MySQL 3.23.55 database is installed. The MySQL Upgrade Installer checks for the existence of the bin\mysql.exe file in this folder for validation.

The MySQL Data folder is the folder where the existing MySQL 3.23.55 stores its database files. The MySQL Upgrade Installer checks for the existence of the mysql\user.frm file in this folder for validation.

Step 5 Enter the root password and port number of the existing MySQL 3.23.55 database, and click **Next**.

The MySQL Upgrade Installer tries to locate the my.ini file in the Windows folder (usually located in C:\Windows or C:\Winnt). If the file is found, the MySQL Upgrade Installer parses it and extracts some MySQL variables. If the my.ini file cannot be located, the MySQL Upgrade Installer tries to connect to the existing MySQL 3.23.55 database using the account root of the given password. It then queries MySQL 3.23.55 for certain variables.

Step 6 The MySQL Upgrade Installer opens a warning dialog box with the following message:

```
Previous MySQL installation (except MySQL data folder) is going to be removed. Make sure
you have backed up the entire MySQL install folder and MySQL data folder before processing
to the next step.
```

Step 7 Click **OK** to continue the installation. Click **Cancel** to cancel the installation. If you click **OK**, the MySQL Upgrade Installer executes the following actions:

- Stops the MySQL 3.23.55 engine.
- Verifies that the given port is available.
- Removes the MySQL Windows service if it exists.
- Deletes all the files and folders (except MySQL data files in the MySQL Data folder) in the MySQL Install folder.

Step 8 Click **Install**. The MySQL Upgrade Installer executes the following actions:

- Installs the MySQL 5.0.58 files.
- Places the my.ini file in the MySQL Install folder.
- Configures the MySQL Windows service.
- Starts MySQL 5.0.58 using the Windows service.
- Verifies the root password provided earlier.
- Runs the database upgrade scripts to upgrade all MySQL 3.23.55 databases in the MySQL Data folder (this could take up to several hours if you have a very large database.)
- Restart MySQL.

Step 9 Click **Done** to complete the MySQL 5.0.58 upgrade.

Linux or Solaris Platform

To upgrade to MySQL 5.0.58 on a Linux or Solaris platform, do the following:

Step 1 Login as root.

Step 2 Copy **mysql-5.0.58-[*nnnn*]-[*mmddyy*]-[*linux*|*solaris*].bin** from the software DVD to the local file system.

Step 3 Run the following command to change the permission of *.bin* file:

```
chmod +x mysql-5.0.58-[nnnn]-[mmddyy]-[linux|solaris].bin
```

where [*nnnn*] is the build number and [*mmddyy*] is the date on which the MySQL Upgrade Installer was built.

Step 4 Run the MySQL Upgrade installer using the following command:

```
./mysql-5.0.58-[nnnn]-[mmddyy]-[linux|solaris].bin
```

Step 5 Press **Enter** after reading the introduction.

Step 6 Select **Upgrade existing MySQL to version 5.0.58**, and press **Enter**.

Step 7 Ensure that both MySQL Install folder and MySQL Data folder are correctly specified.

The MySQL Install folder is the folder where existing MySQL 3.23.55 is installed. The MySQL Upgrade Installer checks the existence of bin/mysql file in this folder for validation.

The MySQL Data folder is the folder where existing MySQL 3.23.55 stores its database files. The MySQL Upgrade Installer checks the existence of mysql/user.frm file in this folder for validation.

Step 8 Enter the root password and port number of the existing MySQL 3.23.55 database.

The MySQL Upgrade Installer tries to locate the /etc/my.cnf file. If this file is found, the MySQL Upgrade Installer parses it and extracts some MySQL variables from it. If /etc/my.cnf cannot be located, the MySQL Upgrade Installer tries to connect to the existing MySQL 3.23.55 database using account root and the given password. It then queries MySQL 3.23.55 for certain variables.

Step 9 The MySQL Upgrade Installer displays the following warning message:

```
Previous MySQL installation (except MySQL data folder) is going to be removed. Make sure
you have backed up the entire MySQL install folder and MySQL data folder before processing
to the next step.
```

Step 10 Select **OK** to continue the installation. Select **Cancel** to cancel the installation. If you clicked **OK**, the MySQL Upgrade Installer executes the following actions:

- Stops the MySQL 3.23.55 engine. If MySQL 3.23.55 cannot be stopped, the MySQL Upgrade Installer displays a warning message. If the **ps -efl|grep mysql|wc -l** command returns 0, it means MySQL has been stopped. If MySQL is not stopped, manually enter the **/etc/init.d/mysql stop** or **kill** command to stop it.
- Verifies that given port is available.
- Deletes the files and folders (except MySQL data files in MySQL Data folder) in the MySQL Install folder.

Step 11 Press **Enter** after reading the Pre-Installation summary. The MySQL Upgrade Installer executes the following actions:

- Installs the MySQL 5.0.58 files.
- Starts MySQL 5.0.58.
- Verifies the root password provided earlier.
- Runs the database upgrade scripts to upgrade all MySQL 3.23.55 databases in the MySQL Data folder (this could take up to several hours if you have very large database).
- Restarts MySQL.

Step 12 Press **Enter** to complete MySQL 5.0.58 upgrade.

Running the CiscoWorks NCM 1.8 Service Pack Installer

This section provides information on running the CiscoWorks NCM 1.8 Service Pack Installer. Before running the CiscoWorks NCM 1.8 Service Pack Installer, ensure that the database server is running.

Restoring Previous Customization

The current CiscoWorks NCM upgrade process does not restore the <CWNCM Install Dir>\jre\reporting.rcx file. If you have customized the CiscoWorks NCM Summary reports template or specification, such as adding additional report tabs, you have to manually update the customized settings from the backed up version of the file to the new installed version of the file.

All settings in the site_options.rcx and adjustable_options.rcx files are preserved and restored automatically. If you want to restore the reporting.rcx file, you must manually edit the new reporting.rcx file.

If you changed other *.rcx* files in the previous installation and want to keep those changes after upgrading, you should add those changes to the new adjustable_options.rcx file. You cannot use the previous .rcx file to overwrite the new version. Doing so could cause the application to fail.

Note All settings in the <CWNCM Install Dir>/server/ext/wrapper/conf/*.conf file and <CWNCM Install Dir>/server/ext/jboss/server/default/conf/log4j.xml file are preserved and restored automatically.

Windows Platform

For upgrading on a Windows platform, insert the CiscoWorks NCM Core Software DVD into the DVD drive and do the following:

Step 1 On the Windows taskbar, choose **Start > Run**.

Step 2 Enter: **`[drive]:\windows_[nnnn]-[mmddyy]_spi_setup.exe`**, where `[drive]` is the letter of your DVD drive, `[nnnn]` is the build number, and `[mmddyy]` is the build date.

Step 3 Click **OK**.

Step 4 Follow the instructions on the screen.

See Upgrading Additional CiscoWorks NCM Components, page 3-10 for information on upgrading other CiscoWorks NCM components, such as CiscoWorks NCM Satellites, CiscoWorks NCM AAA Log Reader, and CiscoWorks NCM Syslog Reader.

Linux and Solaris Platforms

For upgrading on a Linux platform, insert the CiscoWorks NCM Core Software DVD into the DVD drive and mount it. You must have root access to run the CiscoWorks NCM 1.8 Service Pack Installer.

Note On Solaris, the NCM Service Pack Installer supports 64-bit. As a result, on a 64-bit operating system, the installer automatically installs 64-bit NCM. The installer upgrades 32-bit NCM to 64-bit NCM.

Step 1 Enter: **cd /[*DVD_MOUNT_POINT*]**, where [*DVD_MOUNT_POINT*] is the location of the DVD drive.

Step 2 Enter: **cd linux**

Step 3 Set the environment variable using the following commands: **TZ=UTC** and **export TZ**.

Step 4 Enter: **sh linux_[*nnnn*]-[*mmddyy*]_spi_setup_64.bin**, where [*nnnn*] is the build number and [*mmddyy*] is the build date.

Step 5 Follow the instructions on the screen.

For upgrading on a Solaris platform, insert the CiscoWorks NCM Core Software DVD into the DVD drive and mount it. You must have root access to run the CiscoWorks NCM 1.8 Service Pack Installer.

Step 1 Enter: **cd /[*DVD_MOUNT_POINT*]**, where [*DVD_MOUNT_POINT*] is the location of the DVD drive.

Step 2 Enter: **cd solaris**

Step 3 Set the environment variable using the following commands: **TZ=UTC** and **export TZ**.

Step 4 Enter: **sh solaris_[*nnnn*]-[*mmddyy*]_spi_setup.bin**, where [*nnnn*] is the build number and [*mmddyy*] is the build date.

Step 5 Follow the instructions on the screen.

If you see following errors in the Log file, be sure to set the environment variable as indicated above and restart the CiscoWorks NCM 1.8 Service Pack Installer:

```
SQLException while trying to connect to the database.
java.sql.SQLException: ORA-00604: error occurred at recursive SQL level 1
RA-01882: timezone region not found
```

If CiscoWorks NCM was configured to run without root privileges on Linux or Solaris, CiscoWorks NCM will not start after the upgrade. If you are running CiscoWorks NCM as non-root, after installing the CiscoWorks NCM 1.8 Service Pack, you must enter the following command:

```
chown -R $user $CWNCM find $CWNCM -type d -exec ls -ld {} \; |grep '^d..-.' |
awk '{print $9}' | xargs chmod u+x
```

where *$CWNCM* is the root CiscoWorks NCM directory and *$user* is the username with which to start the CiscoWorks NCM Management Engine.

Installing the Latest CiscoWorks NCM Driver Pack

You must install the latest CiscoWorks NCM Driver Pack after you install or upgrade to CiscoWorks NCM 1.8, otherwise you could experience a regression in functionality.

Go to Cisco Software Download Center, http://www.cisco.com/cisco/software/navigator.html, and download the latest CiscoWorks NCM Driver Pack. Install the latest CiscoWorks NCM Driver Pack after installing or upgrading to CiscoWorks NCM 1.8.

Verify the MySQL Configuration

The following MySQL configuration options affect NCM performance:

- Large device configurations can exceed the default packet size configured for MySQL, resulting in an error similar to the following example:

  ```
  DeviceDataManagementEJB: Exception in addDeviceData -
  com.mysql.jdbc.PacketTooBigException: Packet for query is too large.
  ```

  To avoid this problem, increase the maximum packet size that MySQL accepts to at least 16MB. If the error still occurs after adjusting this value, increase it further, up to a maximum of 1GB.

- Restricting MySQL to a small number of concurrent threads can reduce NA performance. (On prior versions of NA, the default number was 10.) To avoid this problem, in the MySQL configuration file, set the number of concurrent threads to 20, which the NA-installed version of MySQL interprets as “infinite threads.”

To set the MySQL configuration as described here, follow these steps:

Step 1 Determine which file to modify.

If no other applications use this installation of MySQL, you can modify the global configuration file, which is commonly located as follows:

- Windows: <Drive>:\MySQL\my.ini
- UNIX: /etc/my.cnf

If any other application uses this installation of MySQL, determine whether to modify the global configuration or a more-specific configuration.

Step 2 Back up the file identified in step 1.

Step 3 Open the configuration file in a text editor, such as WordPad or vi.

Step 4 To set the MySQL permitted packet size to 16MB, edit the configuration file as follows:

a. Locate the line that contains the string max_allowed_packet=.

b. If this line does not exist, create it in the next step.

c. Increase the allocation by updating this line to read:

```
max_allowed_packet=16776192
```

Step 5 To set infinite thread concurreny, edit the configuration file as follows:

a. Locate the line that contains the string innodb_thread_concurrency=.

b. Set infinite thread concurrency by updating this line to read:

```
innodb_thread_concurrency=20
```

Step 6 Save the configuration file.

Step 7 Stop all NCM services:

- Windows: Open the Services control panel. In the list of services, right-click each of the following services, and then click Stop:
  - TrueControl ManagementEngine
  - TrueControl FTP Server
  - TrueControl SWIM Server
  - TrueControl Syslog Server
  - TrueControl TFTP Server
- UNIX: Run the following command:

```
/etc/init.d/truecontrol stop
```

Step 8 Restart MySQL:

- Windows: Open the Services control panel. In the list of services, right-click the MySQL service, and then click Restart.
- UNIX: Run the following command:

```
/etc/init.d/mysql restart
```

Step 9 Start all NCM services:

- Windows: Open the Services control panel. In the list of services, right-click each of the following services, and then click Start:
  - TrueControl ManagementEngine
  - TrueControl FTP Server
  - TrueControl SWIM Server
  - TrueControl Syslog Server
  - TrueControl TFTP Server
- UNIX: Run the following command:

```
/etc/init.d/truecontrol restart
```

Upgrading Additional CiscoWorks NCM Components

The following additional components must be upgraded when upgrading CiscoWorks NCM:

- CiscoWorks NCM High Availability Distributed System—After upgrading to CiscoWorks NCM 1.8, you must update your High Availability Distributed System environment. See the *High Availability Distributed System Configuration Guide for CiscoWorks Network Compliance Manager* for detailed information.
- CiscoWorks NCM Horizontal Scalability—If you are using the CiscoWorks NCM Horizontal Scalability functionality, see the *Horizontal Scalability User Guide for CiscoWorks Network Compliance Manager* for detailed instructions on installing and configuring the Horizontal Scalability software.

- CiscoWorks NCM Satellites—If you are using the CiscoWorks NCM Satellite agent, after installing CiscoWorks NCM 1.8, you must run the Deploy Remote Agent task to re-install the upgraded Satellite agent on all remote Gateways. See the *Satellite User Guide for CiscoWorks Network Compliance Manager* for detailed information.

CiscoWorks NCM AAA Log Reader

If you are using the AAA Log Reader on your AAA server to provide real-time change detection, you must update the AAA Log Reader after installing CiscoWorks NCM 1.8. To do this:

Step 1 Backup the AAA Log Reader directory on your AAA server.

Step 2 Copy the truecontrol-client.jar file located in the AAA folder on the Install CD to the AAA Log Reader directory. Overwrite the existing file.

Step 3 Change the following four options in the agent.rcx file for correct error logging to appear in the aaa_wrapper.log.

Change

```
[option name="log/AAALogReader"]System.out[option]
[option name="log/AAALogReader/level"]0[ooption>
[option name="log/connect"]System.out[option]
[option name="log/connect/level"]75[option]
```

To:

```
[option name="log/External/AAALogReader"]System.out[option]
[option name="log/External/AAALogReader/level"]0[option]
[option name="log/System/Authenticate"]System.out[option]
[option name="log/System/Authenticate/level"]75[option]
```

Note It is recommended that you install the JRE version 1.6.0 on AAA Server. The various JRE installations can be found on the CiscoWorks NCM Core Software DVD at: /add-ons/jre/.

CiscoWorks NCM Syslog Reader

CiscoWorks NCM uses Syslog messages to detect device changes in real-time. Some environments require the use of a Syslog Reader to forward messages from the Syslog server to CiscoWorks NCM. Typically, the Syslog Reader is required only when a central Solaris Syslog server is in use (because Solaris is not RFC-compliant for Syslog).

To upgrade the Syslog Reader:

Step 1 Go to /usr/local/CWNCM/syslogreader/probe.rcx.

Step 2 In the probe.rcx file, edit the following lines:

```
[option name="connect/AppServerURL"]SERVERNAME:1099[/option]
[option name="SyslogReader/LogFile/FileName"]SOMEPATH/FILE[/option]
```

Step 3 Stop the Syslog Reader.

Step 4 Run the **/etc/init.d/truecontrol.syslogreader stop** command.

Step 5 Remove the /usr/local/CWNCM directory.

Step 6 Follow the install instructions in the ReadMe.txt file.

Backing Up the CiscoWorks NCM Database

You cannot rollback to the previous version of CiscoWorks NCM after installing CiscoWorks NCM 1.8. It is recommended that you back up the NCM database before any upgrade.

This section contains the following sub-sections:

- MS-SQL Server Backup Instructions, page 3-12
- MySQL Backup and Restore Instructions, page 3-12

MS-SQL Server Backup Instructions

To back up the MS-SQL Server database:

Step 1 Start Enterprise Manager.

Step 2 Connect to the MS-SQL database server and navigate to your database.

Step 3 Right-click and choose **All Tasks > Backup Database**.

Step 4 Under Destination, if there are any entries highlight them and click **Remove**.

Step 5 Under Destination, click **Add**.

Step 6 Open the file browser.

Step 7 Under File name, enter a filename for your backup. Be sure to provide a new filename or you will overwrite any existing backups.

Step 8 Click **OK** to start the backup procedure. Depending on the size of your database, this could take several minutes.

MySQL Backup and Restore Instructions

To back up the MySQL databases:

Step 1 From the command line prompt in the mysql\bin folder, enter the following command:

```
mysqldump -h<databaseserver> -u<username> -p<password> -r <YourFileName>.sql
<DatabaseName>
```

where:

- *databaseserver* is the ipaddress or hostname of the database server
- *username* is the username to connect to the database server

- *password* is the password to connect to the database server
- *DatabaseName* is the CiscoWorks NCM database name

Example:

```
mysqldump -hNCMDBServer -utc -ptc -r NCM_Backup_04_30_04.sql NCM
```

Step 2 Copy (or move) the file to a backup location.

Step 3 Stop the MySQL service:

- On a Windows platform, choose **My Computer > Control Panel > Administrative Tools > Services**.
- On a Linux or Solaris platform, enter the command **/etc/init.d/mysql stop**

Step 4 Locate the mysql\data folder. It should contain a large ibdata file. For a standard install, this file is located in c:\mysql\data. Copy that entire data folder to a backup location.

Step 5 Restart the MySQL service. This operation can take ten minutes or more for large databases.

Please consult your Oracle database administrator for information on backing up the Oracle databases.

Backing Up CiscoWorks NCM Files

It is recommended that you use a commercial backup/restore utility to backup and restore the entire hard disk of the server that hosts CiscoWorks NCM. This minimizes risks of missed, corrupted, or misplaced files.

Before running the CiscoWorks NCM upgrade, create a full copy of your CiscoWorks NCM folder. During the CiscoWorks NCM upgrade, the CiscoWorks NCM Setup program automatically backs up critical CiscoWorks NCM files to the following directory.

For Windows:

C:\WINDOWS\Temp\Rendition

For Solaris and Linux:

/var/Rendition/

After upgrading to CiscoWorks NCM 1.8, the installer automatically restores the following files:

- Device software images from the backup directory are copied to <CWNCM Install Dir>/server/images.
- Summary reports from the backup directory are copied to <CWNCM Install Dir>/addins.
- CiscoWorks NCM Alert Center content files are copied to <CWNCM Install Dir>/content.
- The site_options.rcx and adjustable_options.rcx files from the backup directory are copied to <CWNCM Install Dir>/jre, if you have selected the Use the Previous Administrative Settings option during installation.
- The SecurID token file is restored.
- The Gateway encryption key is restored.
- The SSL public key certificate is restored.
- The license.dat file is restored if you do not have a new license file.

The following files are backed up. However, they are not restored during the CiscoWorks NCM upgrade:

- All *.rcx* files in the <CWNCM Install Dir>/jre folder.
  - The site_options.rcx and adjustable_options.rcx files will be restored automatically if you have selected the Use the Previous Administrative Settings option during installation. Changes that are made to other *.rcx* files are not preserved.
  - If you want to restore the reporting.rcx file, you must manually edit the new reporting.rcx file.
  - If you changed other *.rcx* files in the previous installation and want to keep those changes after upgrading, you should add those changes into the new adjustable_options.rcx file. You cannot use the previous *.rcx* file to overwrite the new version. Doing so could cause the application to fail.
- <CWNCM Install Dir>/server/ext/jboss/server/default/conf/log4j.xml file—To restore previous settings, you must manually edit this file after upgrading. You cannot use the previous file to overwrite the new version. Doing so could cause the application to fail.
- Wrapper configuration files in <CWNCM Install Dir>/server/ext/wrapper/conf—To restore previous settings in *.conf* files, you must manually edit the corresponding file after upgrading. You cannot use the previous file to overwrite the new version. Doing so could cause the application to fail.

CHAPTER 4

Installing CiscoWorks NCM 1.8

This chapter provides information on installing NCM 1.8 on a new standalone NCM application server..

The following sections provide an outline for single NCM Core installation:

- Prepare the Database
- Install Nmap
- Run the NCM Installer
- Installing the Latest CiscoWorks NCM Driver Pack

Prepare the Database

This section describes the following database options:

- MySQL Database Options
- Oracle Database Options
- Microsoft SQL Server Database Options

MySQL Database Options

On the Linux operating system, verify that the `/etc/hosts` file contains the following line:

```
127.0.0.1     localhost
```

The NCM-installed MySQL requires the localhost line exactly as shown here. To expand the information in the hosts file, add new lines containing the additional definitions.

Make note of the following MySQL Database options during installation:

Step 1 If you want NCM to install MySQL Enterprise Server 5.0.58, when prompted for the folder in which to install MySQL, do not select the NCM Install folder or any sub-folder therein.

Step 2 When prompted whether or not to create a new database or use an existing one, select the Create New Database option. Do not return to the previous step after the database has been created

Note If you want to use an existing NCM database created by a previous NCM installation, select the "using existing database" option. The database will be upgraded to the current version, if applicable.

Oracle Database Options

Oracle database configuration requirements:

- Create a new tablespace dedicated to NCM. For example:

```
CREATE TABLESPACE NADB DATAFILE
'/oracledata/u01/app/oracle/oradata/perfqa02/NADB01.DBF' SIZE 30G REUSE
```

Tip To enable future defragmentation of the NCM tablespace, create the tablespace with automatic segment space management (ASSM). The example command creates the tablespace with ASSM.

- Create an NCM database user that uses the new tablespace. For example:

```
CREATE USER nauser IDENTIFIED BY napass DEFAULT TABLESPACE NADB;
```

- Grant at least the following privileges to the NCM database user:
  - DBA with the ADMIN option
  - CREATE SEQUENCE
  - CREATE SESSION
  - CREATE TABLE
  - CREATE PROCEDURE
  - SELECT ANY DICTIONARY
  - CONNECT
  - CREATE VIEW
  - CREATE PUBLIC DATABASE LINK
  - CREATE DATABASE LINK
  - CREATE USER
  - CREATE ANY PROCEDURE
  - DROP USER
  - DROP PUBLIC DATABASE LINK
  - DROP ANY PROCEDURE
  - CREATE MATERIALIZED VIEW
  - GLOBAL QUERY REWRITE
  - SELECT ANY TABLE
  - UNLIMITED TABLESPACE

For example:

```
GRANT DBA to nauser WITH ADMIN OPTION;
GRANT CREATE SEQUENCE, CREATE SESSION, CREATE TABLE, CREATE PROCEDURE TO nauser;
GRANT SELECT ANY DICTIONARY, CONNECT, CREATE VIEW TO nauser;
GRANT CREATE PUBLIC DATABASE LINK, CREATE DATABASE LINK, CREATE USER TO nauser;

GRANT CREATE ANY PROCEDURE TO nauser;
GRANT DROP USER TO nauser;
GRANT DROP PUBLIC DATABASE LINK TO nauser;
GRANT DROP ANY PROCEDURE TO nauser;
GRANT CREATE MATERIALIZED VIEW, GLOBAL QUERY REWRITE, SELECT ANY TABLE to nauser;
GRANT UNLIMITED TABLESPACE to nauser WITH ADMIN OPTION;
```

- To enable future configuration of the "contains (full text)" search functionality, enable Oracle Text for the database.

Designating Unclustered Oracle During NCM Installation

In an unclustered Oracle environment, note the following database options during installation:

Step 1 When prompted for the Database Admin Login information, enter the database user with access to the NCM tablespace.

Step 2 When prompted to configure the database, select the "Clean database for use by NA" option. Do not return to the previous step after the database has been created.

Note If you want to use an existing NA database created by a previous NA installation, select the "using existing database" option. The database will be upgraded to the current version, if applicable.

Designating Oracle RAC During NCM Installation

In an Oracle RAC environment, note the following database options during installation:

Step 1 When prompted for the Database Admin Login information, enter the database user with access to the NCM tablespace.

Step 2 When prompted to configure the database, select the "Clean database for use by NA" option. Do not return to the previous step after the database has been created.

Note If you want to use an existing NA database created by a previous NCM installation, select the using existing database option. The database will be upgraded to the current version, if applicable.

Step 3 When prompted for database credentials, do the following:

a. In a text editor, open the `$NA_HOME/server/conf/JDBCDrivers.properties` file.

b. Set the `oracle.url` variable in the following format:

oracle.url=jdbc:oracle:thin:@//<*server*>:<*port*>/<*service_name*>

Replace the variables as follows:

– <*server*> is the IP address or fully-qualified hostname of the Oracle RAC cluster.

- *<port>* is the port of the Oracle RAC cluster.
- *<service_name>* is the service name of the Oracle RAC cluster.

c. Save the file.

d. At the NCM installer prompt, enter the following information:

- For the database IP address or hostname, enter the value of *<server>* in the `oracle.url` variable.
- For the database port, enter the value of *<port>* in the `oracle.url` variable.
- For the database SID / Service Name, enter the value of *<service_name>* in the `oracle.url` variable.

Step 4 After NCM installation completes, ensure that the Oracle RAC cluster information in the `$NCM_HOME/server/ext/jboss/server/default/deploy/db_ds.xml` file is current.

Microsoft SQL Server Database Options

SQL Server database configuration requirements:

- Create the NCM database with the server role of public.
- To enable future configuration of the "contains (full text)" search functionality, install and enable the SQL Server Full Text Search service for the database.

Make note of the following Microsoft SQL Server Database options during installation:

Step 1 When prompted for the Database Admin login, if you do not select the Use Windows Authentication option, make sure you have set all privileges at the global level.

Step 2 When prompted whether or not to create a new database or use an existing one, select the "Create New Database" option.

Note If you want to use an existing NCM database created by a previous NCM installation, select the "using existing database" option. The database will be upgraded to the current version, if applicable.

Install Nmap

Nmap enables you to scan networks to determine which hosts are up and the services they offer.

Install Nmap as described in the section appropriate to the operating system of the NCM application server:

- Installing Nmap on a Windows Operating System
- Installing Nmap on a Linux Operating System
- Installing Nmap on a Solaris Operating System

Installing Nmap on a Windows Operating System

The Nmap execution file included with NCM might not be compliant with all Windows versions. Be sure to download the correct Nmap install packages for your Windows versions.

Installing Nmap on a Linux Operating System

To install Nmap on a Linux operation system, follow these steps:

Step 1 cd [$NCM_HOME]/server/ext/nmap

Install the RPM package using the following command:

```
rpm -i <rpm file>
```

For example:

```
cd [$NA_HOME]/server/ext/nmap
rpm -i nmap-3.81-1.i386.rpm
```

Step 2 Create a link to the nmap executable in the $NA_HOME/server/ext/nmap directory:

```
cd [$NCM_HOME]/server/ext/nmap
ln -s /usr/bin/nmap nmap
```

Installing Nmap on a Solaris Operating System

Nmap has several installation prerequisites. Make sure you have the following installed before installing Nmap.

- glib
- gtk
- openssl-0.9.7g
- pcre
- libgcc-3.3 or gcc-3.3.2 (libgcc-3.3 is preferred)

These packages are available at http://sunfreeware.com

To install Nmap on a Solaris operating system, follow these steps:

Step 1 `cd $NCM_HOME/server/ext/nmap`

Step 2 Unzip and add the packages using the following commands:

`gunzip` *<filename>*

`pkgadd -d` *<filename>*

For example:

```
cd [$NCM_HOME]/server/ext/nmap
gunzip nmap-3.81-sol10-sparc-local.gz
pkgadd -d nmap-3.81-sol10-sparc-local
```

Note The Nmap package that comes with NCM might not be compliant with all Solaris versions. Be sure to download the correct Nmap install packages for your Solaris version

Step 3 Create a link to the nmap executable in the `$NA_HOME/server/ext/nmap` directory:

```
cd $NCM_HOME/server/ext/nmap
ln -s /usr/local/bin/nmap nmap
```

Run the NCM Installer

If you are installing NCM on a Windows platform, run the Install Wizard. If you are installing NCM on a Linux or Solaris platform, run the CLI Installer.

The NCM installer sets the Java virtual machine (JVM) heap size in relation to the amount of system RAM and the number of processors. Generally speaking, the installer sets the JVM heap size to half of the RAM. (The NCM installer does not explicitly set the size of the young generation, so this value defaults to 1/3 of the JVM heap size.) Note the following exceptions:

- If the NCM application server has more that 64GB of RAM, the NCM installer sets the JVM heap size to 32GB.
- If HP Network Node Manager i Software is already installed on the NCM application server, the NCM installer sets the JVM heap size to 512MB regardless of the system RAM size. In this case, the NCM installer sets the JVM permanent generation garbage collection (PermGen) to 128MB.

Note Be sure you have ActivePerl 5.8.x (for Windows) or Perl 5.8.x (for Solaris and Linux) installed before installing NCM.

Note If the installation fails, save all log files to a location outside the NCM directory structure before re-running the installation.

This section contains:

Running the Installer on a Windows Operating System

With Administrator privileges, do the following to install NCM:

Step 1 On the Windows taskbar, click Start, and then click Run.

Step 2 Enter: `<drive>:\windows_[nnnn]-[mmddyy]_setup.exe`, where `<drive>` is the letter of your CD-ROM drive and `[nnnn]-[mmddyy]` is the build number.

Step 3 Click OK.

Follow the instructions on the screen.

Note Setup does not work with PC Anywhere. If you attempt to run Setup through PC Anywhere, you cannot view the windows to step through the installation. This also affects uninstalling NA.6

Running the Installer on a Linux Operating System

To install NCM on a Linux server, follow these steps:

Step 1 Log on to the Linux server as the `root` user.

Step 2 If the installer is on physical media, mount that drive:

a. mount /mnt/cdrom

b. cd /mnt/cdrom

Step 3 Change to the directory containing the CLI installer.

On the physical media, change to the `linux` directory.

Step 4 Set the time zone environment variable using the following commands:

TZ=UTC

export TZ

Step 5 Run the installer:

./linux_[nnnn]-[mmddyy]_setup_64.bin

Follow the instructions on the screen.

If you see the following errors in the log file, verify the value of the `TZ` environment variable, and then restart the NCM Service Pack Installer:

```
SQLException while trying to connect to the database.
java.sql.SQLException: ORA-00604: error occurred at recursive SQL level 1
RA-01882: timezone region not found
```

Running the Installer on a Solaris Operating System

The Solaris CLI installer supports 64-bit. As a result:

- The Solaris CLI installer automatically installs 64-bit NCM.
- The Solaris SPI will upgrade 32-bit NA to 64-bit NCM.
- When upgrading to 64-bit NCM, all of the wrapper configuration files (files such as `jboss_wrapper.conf` and `syslog_wrapper.conf`) will be overwritten. Any user-specified settings will be reset. For example, if you had set the `jboss_wrapper.conf` to start NA with 1GB Java Heap memory, the setting will be overwritten to the NCM default.

To install NCM on Solaris, first download the latest Solaris patches from the Sun Web site:

Before installing NCM on a Solaris 10 platform, you must reconfigure the Syslog server on Solaris 10 to not listen for remote Syslog messages on port 514.

Step 1 Edit the `/etc/default/syslogd` file and set `LOG_FROM_REMOTE=NO`.

Step 2 Restart the Syslog server. Enter: `svcadm refresh svc:/system/system-log:default`

Enter the following commands to install NA manually. Be sure to change to the drive on which you want to install NA. At the shell prompt, enter:

Step 1 `su root` [when prompted, enter the password]

Step 2 `cd /cdrom/`

Step 3 Set the environment variable using the following commands: `TZ=UTC` and `export TZ`.

Step 4 sh solaris_[nnnn]-[mmddyy]_setup_64.bin

Follow the instructions on the screen.

Note On Solaris, the NA installer moves the existing /etc/syslog.conf file to /etc/syslog.conf.rm and then restarts the Syslog process using its own configuration.

If you see the following errors in the log file, verify the value of the `TZ` environment variable, and then restart the NCM Service Pack Installer:

```
SQLException while trying to connect to the database.
java.sql.SQLException: ORA-00604: error occurred at recursive SQL level 1
RA-01882: timezone region not found
```

Installing the Latest CiscoWorks NCM Driver Pack

You must install the latest CiscoWorks NCM Driver Pack after you install or upgrade to CiscoWorks NCM 1.8, otherwise you could experience a regression in functionality.

Go to Cisco Software Download Center, http://www.cisco.com/cisco/software/navigator.html, and download the latest CiscoWorks NCM Driver Pack. Install the latest CiscoWorks NCM Driver Pack after installing or upgrading to CiscoWorks NCM 1.8.

CHAPTER 5

Licensing

This chapter contains the following sections:

The information contained in this chapter applies only to new CiscoWorks NCM 1.8 installations. If you are upgrading from a previous release of CiscoWorks NCM, no new license is required.

Understanding Licensing Terms

Table 5-1 describes CiscoWorks NCM licensing terms.

Table 5-1 CiscoWorks NCM Licensing Terms

Licensing Term	Description
Product Authorization Key (PAK)	The PAK is printed on the software claim certificate included in product packaging. Use the PAK and LMHOSTID to get your license file from Cisco.com. You can purchase incremental licenses for additional device support. For each incremental license that you purchase, you will receive a PAK. You must use that PAK to obtain a license file.
License file	To register your product on the product licensing area of Cisco.com, you need to provide the following details: • LMHOSTID • PAK Upon successful registration you will receive a license file.

Licensing Your Product During Installation

After installing CiscoWorks NCM 1.8, you should register the product and obtain a license file.

To register your product, you must do the following:

Step 1 From the command line, run the command **/<*NCM_ROOT*>/server/ext/wrapper/bin/lmutil lmhostid** to determine the LMHOSTID.

Step 2 Log into following Cisco.com URL with your username and password:

http://www.cisco.com/go/license/index.html

Note You must be a registered user of Cisco.com to log in. Logging in allows your Cisco user profile information to automatically populate many of the product registration fields. Login is case sensitive.

Step 3 Register the CiscoWorks NCM product with Cisco.com using the LMHOSTID and PAK.

You might want to request a license without installing CiscoWorks NCM. The NCM **flexlmhostid** is same as the Windows and Linux MAC address or the Solaris system hostid. Run the following commands to get the MAC or host id depending on the platform.

- Windows: **ipconfig /all**
- Linux: **ifconfig -a**
- Solaris: **hostid**

Installing the CiscoWorks NCM License File

Licenses are issued separately for CiscoWorks NCM products, such as CiscoWorks NCM Core, High Availability Distributed Systems, and Cisco Satellite (or Gateway), based on the device count.

Evaluation licenses are not included in the software DVD. To get an evaluation license, you must do the following:

Step 1 Log into the following Cisco.com URL with your username and password:

http://www.cisco.com/go/license/index.html

Note You must be a registered user of Cisco.com to log in. Logging in allows your Cisco user profile information to automatically populate many of the product registration fields. Login is case sensitive.

Step 2 If you do not have a Product Authorization Key (PAK), click the **Click Here for Available Licenses** link.

Product License Registration page will appear.

Step 3 Click **CiscoWorks Network Compliance Manager**.

Step 4 Enter the registration information to register your CiscoWorks NCM Core Evaluation product.

Registration of your CiscoWorks NCM Core evaluation software is required for you to obtain a license file that will be necessary to complete the software installation. Ensure that you enter your email address correctly as your license file will be emailed to you.

Evaluation licenses expire 90 days after installation. If a NCM server has both an evaluation and permanent license for the same product, the evaluation license is ignored.

Installing the CiscoWorks NCM License with the CiscoWorks NCM Software

To install a CiscoWorks NCM license file with the CiscoWorks NCM software:

Step 1 Save the *.lic* license file on the server in a separate directory.

Note Make sure there are no spaces in the directory path name.

Step 2 During the CiscoWorks NCM install process, the install wizard will prompt for the license file directory. Point the install wizard to the directory where the *.lic* file is saved.

Installing the CiscoWorks NCM License After Installing CiscoWorks NCM Software

To install a CiscoWorks NCM license file after installing the CiscoWorks NCM software, do the following:

Step 1 Ensure that the CiscoWorks NCM software has been installed and configured on the server. See Installing CiscoWorks NCM 1.8, page 4-1 for instructions.

Step 2 Save the *.lic* license file to the directory where CiscoWorks NCM is installed.

Step 3 Restart the CiscoWorks NCM server:

- On Windows platform: Restart the service TrueControl NCM License server
- On Solaris or Linux platforms: enter `/etc/init.d/truecontrol restart`

Step 4 Open a supported version of a web browser.

Step 5 In the **Location** or **Address** field, enter the appropriate URL to access the CiscoWorks NCM server.

Step 6 Log into the CiscoWorks NCM server as system administrator.

Step 7 Choose **Admin > About CiscoWorks Network Compliance Manager**.

Step 8 Click **View License Information**.

The updated license status will be displayed.

Step 9 If the updated license information is not visible, copy the information in the *.lic* file and paste it in the text box.

Step 10 Click the **Update License** button.

A new license file is created with a unique name in the \CWNCM root directory. If you choose to copy the license file, enter a filename that does not already exist, otherwise you will overwrite the existing license file.

When CiscoWorks NCM starts, a license server parses the license files and caches the information. You must restart the CiscoWorks NCM server when new license files are added.

Licensing High Availability Distributed Systems

For High Availability Distributed System, both High Availability Distributed System and CiscoWorks NCM Core licenses are required, with a license count equal to or greater than your total device inventory. Inactive devices do not count toward this number.

For non-High Availability Distributed Systems, a CiscoWorks NCM Core license is required for each CiscoWorks NCM Core server in the system.

Each CiscoWorks NCM Core server must be able to manage the entire device inventory in the event that one or more CiscoWorks NCM Core servers go off-line and devices need to be assigned to different managed CiscoWorks NCM Cores. As a result, any on-line CiscoWorks NCM Core server will have license capacity to manage the devices inventory.

Note Install the CiscoWorks NCM Core and High Availability Distributed System licenses only on the Primary Master server. You do not need to install licenses on other High Availability Distributed System servers.

License Error Messages

If a CiscoWorks NCM server has multiple licenses installed, the device count allowed is the sum of all valid licenses. If the device count exceeds the number of valid licenses, you will not be able to log into CiscoWorks NCM. The login screen will display a License Error message.

For information on CiscoWorks NCM license configuration settings and License Monitor messages, see Chapter 1 in the *User Guide for CiscoWorks Network Compliance Manager 1.8*.

If you experience a problem with CiscoWorks NCM licensing, remove all existing evaluation and expired license files from the CiscoWorks NCM root directory and reinstall the CiscoWorks NCM license.

CHAPTER 6

Uninstalling CiscoWorks NCM and MySQL

This chapter contains the following sections:

Uninstalling CiscoWorks NCM on Windows Platform

To uninstall CiscoWorks NCM on a Windows platform:

Step 1 Choose **Start > Programs > CiscoWorks Network Compliance Manager > Uninstall CiscoWorks Network Compliance Manager**.

Step 2 Click **Uninstall**.

Step 3 When the uninstall program is done, click **Finish**.

A message appears saying that you must reboot. The installation folder is removed when you reboot the system.

Step 4 (Optional) You can delete the files in the following folder:

c:\windows\Temp\Rendition

Note The CiscoWorks NCM database is not removed when you uninstall CiscoWorks NCM. If you manually delete the database, you must ensure that the database files are removed before trying to re-install CiscoWorks NCM.

If you upgraded to a newer version of CiscoWorks NCM on a Windows platform, the CiscoWorks NCM Uninstaller does not remove the FTP service. After uninstalling CiscoWorks NCM, you must enter the **sc delete TrueControlFTP** command from the command line prompt to delete the FTP service.

Uninstalling CiscoWorks NCM on Linux or Solaris Platforms

To uninstall CiscoWorks NCM on Linux or Solaris platforms:

Step 1 Navigate to the <CWNCM_Install_Directory>/UninstallerData directory (for example, /opt/CWNCM/UninstallerData).

Step 2 Enter the following command:

```
#./Uninstall_CiscoWorks_Network_Compliance_Manager
```

There are files left in other locations to preserve your settings, logs, and scripts in case you reinstall CiscoWorks NCM. If you want to completely purge CiscoWorks NCM from your system, manually delete all files (for example: `# rm -rf /opt/CWNCM`).

Step 3 (Optional) You can delete the following folder:

/var/Rendition

Manually Uninstalling CiscoWorks NCM on Windows

While uninstalling CiscoWorks NCM, if the uninstaller makes no progress for over 10 minutes, stop the uninstaller process and do the following:

Step 1 Run the following commands to stop all CiscoWorks NCM services:

```
{$CWNCM_HOME}\server\ext\wrapper\bin\UninstallAAAWrapper-NT.bat
{$CWNCM_HOME}\server\ext\wrapper\bin\UninstallJBossWrapper-NT.bat
{$CWNCM_HOME}\server\ext\wrapper\bin\UninstallSWIMWrapper-NT.bat
{$CWNCM_HOME}\server\ext\wrapper\bin\UninstallSyslogWrapper-NT.bat
{$CWNCM_HOME}\server\ext\wrapper\bin\UninstallTFTPWrapper-NT.bat
```

Step 2 Delete the CiscoWorks NCM folder.

Step 3 Delete the following Windows registry keys if they exist:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Rendition Networks\TrueControl
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrueControlJBoss
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrueControlAAA
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrueControlJBossSWIM
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrueControlJBossSyslog
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrueControlJBossTFTP
```

Step 4 Manually delete the %WINDIR%\temp\Rendition folder.

Note %WINDIR% is usually located in C:\WINDOWS or C:\WINNT. However, it might reside on a different drive.

Uninstalling MySQL 5.0.58 (MySQL Installer)

If MySQL 5.0.58 was installed by the MySQL Installer:

- On a Windows platform, double-click Uninstall_MySQL.exe (<MySQL Install Dir>\Uninstall_MySQL\Uninstall MySQL.exe) and follow the instructions in the MySQL Uninstaller.
- On a Linux or Solaris platform, run **<*MySQL Install Dir*>/Uninstall_MySQL/Uninstall_MySQL** and follow the instructions in the MySQL Uninstaller.

Note The MySQL data folder will not be removed.

Uninstalling MySQL 5.0.58 (CiscoWorks NCM Installer)

If MySQL 5.0.58 was installed by the CiscoWorks NCM Installer:

On a Windows platform:

Step 1 Double click <MySQL Install Dir>\bin\remove-service.bat, where <MySQL Install Dir> is the location where MySQL is installed.

Step 2 Backup the MySQL data folder.

Step 3 Manually delete the MySQL Install directory.

On a Linux or Solaris platform:

Step 1 Run **/etc/init.d/mysql stop**

Step 2 Backup the MySQL data folder.

Step 3 Run **rm -rf /etc/init.d/mysql /etc/my.cnf <*MYSQL Install Dir*>**, where <MySQL Install Dir> is the location where MySQL is installed.

Uninstalling MySQL 3.23.55

Caution Uninstalling the MySQL 3.23.55 database permanently deletes your historical data. There is no undo.

To uninstall MySQL 3.23.55 on a Windows platform:

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

Step 2 Right-click **MySQL** and select **Stop**.

Step 3 Choose **Start > Run**, then enter **cmd**.

Step 4 Enter `c:\<mysql_install_folder>\bin\mysqld-max-nt.exe --remove`

Step 5 In the Services window, verify that the MySQL Service is removed. If it is still listed as disabled, close all programs and restart your computer, then check the Services window again.

Step 6 In the Windows Control Panel, double-click **Add/Remove Programs**.

Step 7 Select **MySQL Servers and Clients** and click **Remove**.

Step 8 Choose **Start > Run**, and then enter `cmd` to launch a command window.

Step 9 Enter: `cd c:\`

Step 10 Enter: `del c:\mysql`

To uninstall MySQL 3.23.55 on a Linux or Solaris platform:

Step 1 Login as Root.

Step 2 Run the following command:

```
/etc/init.d/mysql stop
```

Step 3 Backup the MySQL data folder.

Step 4 Enter the following command:

```
rm -rf /etc/init.d/mysql /etc/my.cnf [<MYSQL Install Dir>]
```

where <MYSQL Install Dir> is the directory where MySQL is installed.

CHAPTER 7

Starting/Stopping CiscoWorks NCM Services

This chapter contains the following sections:

Windows Platform

To start/stop CiscoWorks NCM services on a Windows platform:

Step 1 Choose **Start > Programs > Administrative Tools > Services**.

Step 2 Start/stop the following CiscoWorks NCM services:

- TrueControl AAA Agent
- TrueControl Management Engine
- TrueControl SWIM Server
- TrueControl Syslog Server
- TrueControl TFTP Server
- TrueControl NCM License Server

Note Use Windows Services to start/stop MySQL.

Linux and Solaris Platform

To start/stop CiscoWorks NCM services on Linux or Solaris platform, login as root and enter the following command:

```
/etc/init.d/truecontrol <command>
```

Options for this command include:

- start
- stop
- restart
- status

Note Use `/etc/init.d/mysql` to start/stop MySQL.

System Status Page

If you do not know the name of the existing CiscoWorks NCM database, before shutting down CiscoWorks NCM do the following:

Step 1 Choose **Admin > System Status**.

The System Status page appears.

Step 2 In the **Monitor Name column**, locate **DatabaseMonitor**.

Step 3 Click the **View Details** option in the Actions column.

The database information is displayed.

APPENDIX A

IPv6 Readiness

CiscoWorks NCM is a robust network element management and automation tool. CiscoWorks NCM communicates with the network elements via numerous protocols and authentication methods to gather information. CiscoWorks NCM then parses the information, normalizing it in a searchable and presentable format.

CiscoWorks NCM supports IPv6, both as transport and as parsed searchable and presentable bits of IPv6 specific information. CiscoWorks NCM's adoption of IPv6 is focused on providing:

- Transparent access to network elements via IPv4 or IPv6
- Information on network element IPv6 configurations
- IPv6 support across CiscoWorks NCM features

Installation

CiscoWorks NCM installs and automatically detects network provisioning on the server. The available protocol determines what protocol CiscoWorks NCM uses for communicating to elements and CiscoWorks NCM listening servers. This includes:

- IPv4 only
- IPv6 only
- Dual stack environments (whether native or using a transition mechanism)

If CiscoWorks NCM is installed on a server that is to be updated to support IPv6, the following procedure is recommended:

1. Shutdown CiscoWorks NCM.
2. Add IPv6 support to the server.
3. Restart CiscoWorks NCM.
4. Check the Admin options for various servers to ensure correct IPv6 address discovery.

Supported Platforms

CiscoWorks NCM IPv6 functionality has been verified on the following platforms:

- Windows Server 2008 64-bit
- Linux RH AS5 64-bit

- Solaris 10

CiscoWorks NCM supports IPv6 connections to DBMS. This includes MS-SQL 2005 and MS-SQL 2008.

Network Services

CiscoWorks NCM has several network services that will appropriately listen on IPv4-only, IPv6-only, and dual stack environments. Some of the network services are:

- Web Server (TCP 80 and 443)—Clients using IPv6-enabled OS and browser can access CiscoWorks NCM via IPv6.
- TFTP Server (UDP 69)—Network elements can upload or download information via TFTP IPv6.
- TELNET Server (TCP 23)—Network elements can upload or download information via TELNET IPv6. Clients accessing the CiscoWorks NCM CLI can do it via TELNET IPv6.
- SSH/SCP Server (TCP 22)—Network elements can upload or download information via SSH/SCP IPv6. Clients accessing the CiscoWorks NCM CLI can do it via SSH IPv6.
- SYSLOG Server (UDP 514)—Network elements reporting change can do it via SYSLOG IPv6.

CiscoWorks NCM functions that instruct network elements to access these services will correctly determine which protocol to use based on a number of factors.

Clients

CiscoWorks NCM uses numerous protocols for intra-communication and communicating with network elements. These include:

- HTTP (TCP 80)—Access network elements
- HTTP (TCP 443)—Access network elements
- FTP (TCP 21)—Access network elements
- SNMP (UDP 161)—Access network elements
- Telnet (TCP 23)—Access network elements
- SSH/SCP (TCP 22)—Access network elements
- SYSLOG (UDP 514)—Send logging message
- SMTP (TCP 25)—Send email

IPv6 Presentation

The CiscoWorks NCM user interface supports IPv6 notation. This includes correct understanding, parsing, input, and display of IPv6 addresses. CiscoWorks NCM provides unique searching features for searching the IPv6 addresses within the system.

Development Environment

CiscoWorks NCM relies heavily on Java JDK 1.6 for network support of IPv6. For more information on Java's support and interpretation of the IPv6 standards, refer to: http://java.sun.com.

CiscoWorks NCM Features Supporting IPv6

The following CiscoWorks NCM features support IPv6:

- Detect Network Device
- Discover Driver
- Device Reservation
- Take Snapshot
- Configure Syslog
- Deploy Passwords
- Reboot Device
- Run Command Script
- Run Diagnostics
- Synchronize Startup and Running
- Update Device Software
- Import
- Deduplication
- Check Policy Compliance
- Resolve FQDN
- Searching
- Reporting
- Real time change management
- Work Flow
- CLI and API

Drivers

CiscoWorks NCM architecture includes a driver layer between the CiscoWorks NCM Core and the managed network elements. This layer abstracts information from network elements, interprets it, and then forwards the information to CiscoWorks NCM. CiscoWorks NCM has IPv6 driver dependencies. As a result, not all drivers support all features of IPv6. Primary adoption includes the Cisco family of network elements.

Currently, the following CiscoWorks NCM components do not support IPv6:

- Overlapping IPs—Satellite Gateways do not support IPv6.
- Dynamic IPv6 addresses—CiscoWorks NCM does not gather or track information on device elements or dynamically assigned IPv6 addresses (for example, link local and multicast).
- IPv6 ACLs—The ACL specific feature does not parse or process IPv6 ACLs, though functionality to search, add, delete, and edit IPv6 ACLs exists.
- Nmap—Using Nmap with the CiscoWorks NCM Detect Network Device feature does not work.
- High Availability Distributed System and Horizontal Scalability—Dual stack is supported, however with the replication/RMI using IPv4-only.
- Topology Diagramming—Topology diagramming does not support IPv6.

APPENDIX B

Troubleshooting

This appendix contains the following sections:

Restoring Databases

To restore SQL server databases:

Step 1 Backup the database that you want to restore.

Step 2 Launch Enterprise Manager.

Step 3 Connect to the SQL database server and navigate to your database.

Step 4 Right click and choose **All Tasks > Restore Database**.

Step 5 Click the **Restore: From Device** button.

Step 6 Click **Select Devices**.

Step 7 Click **Add**.

Step 8 Open the file browser under File name and select the file you want to restore.

Step 9 Click **OK**.

Step 10 Click the **Options** tab.

Step 11 Click **Force Restore Over Existing Database**.

Step 12 Click **OK**.

If you receive an error message, such as “Database is in use”, you need to either stop your JBoss server or go to the Options tab and change the names of the physical files listed to a different name.

To restore MySQL databases, there are two methods. One of the methods is to restore using the copied files. This method restores all MySQL databases that were on the server at the time of the backup. To do this:

Step 1 Make a backup of the mysql\data directory.

Step 2 Choose **My Computer > Control Panel > Administrative Tools > Services** and stop the MySQL service.

Step 3 Copy all the files that were backed up from the mysql\data directory back into the mysql\data directory.

Step 4 Restart the MySQL service.

Note This method should only be used if CiscoWorks NCM is the only application using the database server.

Another method is to restore MySQL databases using the .sql backup file. To do this:

Step 1 Make a backup of the MySQL database.

Step 2 Edit the *.sql* file. Add the following line to the top of the file:

```
SET FOREIGN_KEY_CHECKS=0;
```

Step 3 Navigate to the mysql\bin directory and enter the following command to get to the MySQL command interface:

```
mysql -h<hostname> -u<username> -p<password>
```

Step 4 Enter the following commands in the MySQL command interface. (Note that MySQL needs forward slashes '/' in path names.)

```
drop database <DatabaseName>;
create database <DatabaseName>;
use <DatabaseName>;
source <BackupFileName>.sql;
grant all privileges on <DatabaseName>.* TO <username>
identified by '<password>';
```

Port in Use

CiscoWorks NCM communicates with devices using a combination of protocols and ports. If any one of the ports is in use by another application or service, you must stop that application or service to ensure a successful CiscoWorks NCM upgrade.

Protocols, Databases, and Ports

CiscoWorks NCM communicates with devices using a combination of the following protocols, databases, and ports. If you use a given protocol, CiscoWorks NCM requires access to the corresponding port. Specifically, if CiscoWorks NCM communicates with devices protected by firewalls, these ports must be open.

Table B-1 Protocols and Ports Used by CiscoWorks NCM

Protocol/Database/Port	From/To
CiscoWorks NCM Server (running the Mgmt Engine, Syslog, TFTP) and Network devices	
Telnet (port 23)	From CiscoWorks NCM server to network devices.
SSH (port 22)	From CiscoWorks NCM server to network devices.
TFTP (port 69/udp)	From network devices to CiscoWorks NCM server.
Syslog (port 514/udp)	From network devices to CiscoWorks NCM server. You can change the CiscoWorks NCM Syslog port.
SNMP (port 161/udp)	From CiscoWorks NCM server to network devices.
Oracle (port 1521)	From CiscoWorks NCM server to an Oracle database. In a Distributed System configuration, the Oracle processes connect to each other on port 1521.
TCP (Port 1099)	In a Distributed System configuration, the CiscoWorks NCM Cores communicate with each other on port 1099 when TCP protocol is used.
UDP (Port 4443)	In a Distributed System configuration, the CiscoWorks NCM Cores communicate with each other on port 4443 when UDP protocol is used.
SQL Server (port 1433)	From a CiscoWorks NCM server to a SQL Server database. In a Distributed System configuration, the SQL Server databases communicate with each other on port 1433.
MySQL (port 3306)	From a CiscoWorks NCM server to a MySQL database.
jboss (ports 4712, 4713, and 4714)	jboss transaction management
jboss (ports 5445 and 5455)	jboss Messaging service
CiscoWorks NCM server and the AAA Log Reader	
JNDI (port 1099)	From AAA Log Reader to CiscoWorks NCM server. You can change this by editing the CiscoWorks NCM configuration files.

Table B-1 Protocols and Ports Used by CiscoWorks NCM (continued)

Protocol/Database/Port	From/To
RMI (port 1098)	From AAA Log Reader to CiscoWorks NCM server. You can change this by editing the CiscoWorks NCM configuration files.
RMI (object port 4444)	From AAA Log Reader to CiscoWorks NCM server. You can change this by editing the CiscoWorks NCM configuration files.
RMI (object port 8083)	CiscoWorks NCM also uses RMI between CiscoWorks NCM clients and the CiscoWorks NCM Management Engine, and between the CiscoWorks NCM Management Engines in separate CiscoWorks NCM Cores. CiscoWorks NCM clients can include: • CiscoWorks NCM Syslog Server • CiscoWorks NCM Connectors • AAA Log Reader • Syslog Reader • Customer-written API scripts (See the *CiscoWorks NCM 1.8 API Reference Guid*e for information.)
CiscoWorks NCM server and the Software Image Management Server	
HTTPS (port 6099)	From CiscoWorks NCM server to Software Image Management server.
Gateway	
TunnelPort (2001)	From Satellite Gateway to Core Gateway. The Core Gateway listens for tunnel connections.
ProxyPort (3002)	From CiscoWorks NCM Core to Core Gateway and from Satellite agent to Satellite Gateway.
IdentPort (4040)	From CiscoWorks NCM Core to the Core Gateway.
AdminPort (9090)	From Satellite Gateway to Core Gateway. The Satellite Gateway uses all ports that the CiscoWorks NCM Core uses for managing devices (from the Satellite Gateway to the device: 22, 23, 514, 80, and 443).
RpcPort (8443)	From the Satellite Gateway to the management agent (Tomcat, Syslog, TFTP, and so on).
CiscoWorks NCM Server and the CiscoWorks NCM client	
HTTPS (port 443)	From CiscoWorks NCM client to CiscoWorks NCM server. You can change this by editing the CiscoWorks NCM configuration files.
TACACS+ (port 49)	From CiscoWorks NCM client to CiscoWorks NCM server.

Table B-1 Protocols and Ports Used by CiscoWorks NCM (continued)

Protocol/Database/Port	From/To
Telnet (port 23 - Windows or 8023 - Solaris/Linux)	From CiscoWorks NCM client to CiscoWorks NCM server. This can be changed from the Administrative Settings option. See Chapter 2, "Configuring Administrative Settings," in the *CiscoWorks NCM 1.8 User Guide* for information on assigning ports.
SSH (port 22 - Windows or 8022 - Solaris/Linux)	From CiscoWorks NCM client to CiscoWorks NCM server. This can be changed from the Administrative Settings option. See Chapter 2, "Configuring Administrative Settings," in the *CiscoWorks NCM 1.8 User Guide* for information on assigning ports.

Other ports include:

- FTP—Port 21
- SCP—Port 22
- Rlogin—Port 513
- RADIUS—1812
- LDAP—3268
- Twist—1032

Configuring the CiscoWorks NCM Syslog Server

The following configuration settings are available for the CiscoWorks NCM Syslog Server:

- The interface to listen for Syslog messages. The default is to listen on all interfaces.
- The UDP port to listen for Syslog messages. The default is 514.
- A hostname to forward Syslog messages. Syslog forwarding is off by default.
- The UDP port to forward Syslog messages. The default is 514.

To configure the above settings, edit the $CWNCM/jre/adjustable_options.rcx file and add the following lines between the <option> and </option> tags:

```
<option name="syslog/listener_address">192.168.1.12</option>
<option name="syslog/listener_port">514</option>
```

To enable Syslog forwarding, add the following:

```
<array name="syslog/handlers">
  <value>com.hp.nas.syslog.NASSyslogHandler</value>
  <value>com.hp.nas.syslog.NASSyslogForwarder</value>
</array>

<option name="syslog/forward_host">10.1.2.3</option>
<option name="syslog/forward_port>514</option>
```

Note If you remove the NASSyslogHandler from the array of Syslog handlers, NCM will only forward Syslog messages. NCM will not initiate snapshots of devices when Syslog messages are received.

User Authentication Crypto Key Exception

It is possible that after upgrading to CiscoWorks NCM 1.5, you will not be able to access any of the menu items under Administrative Settings. This is due to a corrupted encryption option in the site_options.rcx file.

Workaround:

Step 1 Go to the <*CWNCM_Install_Dir*>/jre directory.

Step 2 Backup the current *site_options.rcx* file.

Step 3 Open the site_options.rcx file and locate all encrypted text options by searching for "EncryptedText".

Step 4 Remove the value for all encrypted text options if it is not empty. In the following example, you would delete the information between </comment> and </option>.

Before:

```
<option name="twist/password"><title>Twist Password</title>
<section>Opsware Server Automation System Authentication</
section><size>30</size><type>EncryptedText</type><comment>Web Services Data Access
Engine Password for finding connected servers.
</comment>encrypted:sQAHLgjGjdGIbvNB18NEoQ==</option>
```

After:

```
<option name="twist/password"><title>Twist Password</title>
<section>OpswareServer Automation System Authentication</
section><size>30</size><type>EncryptedText</type><comment> Web Services Data Access
Engine Password forfinding connected servers.</comment></option>
```

Step 5 Save the file.

Step 6 Login to CiscoWorks NCM.

Step 7 On the menu bar under Admin, select Administrative Settings and click User Authentication. Scroll down to the "TACACS+ / RADIUS Authentication" section.

Step 8 For the TACACS+ or RADIUS Secret option, enter the shared secret for the CiscoWorks NCM host configured on the TACACS+ or RADIUS server.

Step 9 Scroll down to the "Server Automation Authentication" section.

Step 10 For the Twist Password option, enter the Server Automation password to use when locating connected servers.

Step 11 Click the Save button.

Step 12 Click the Device Access tab.

Step 13 Scroll down to the "Bastion Host Settings" section.

Step 14 For the Default Bastion Host Password option, enter the password of the Bastion Host to use for Telnet and/or SSH access.

Step 15 Click Save.

MySQL Upgrade Installer

When troubleshooting the MySQL Upgrade Installer, keep in mind the Log files are in the sub-folder log in the MySQL Install folder.

In some very rare cases, my.ini (/etc/my.cnf) cannot be located and the MySQL variables cannot be queried successfully from MySQL engine. You may be asked to confirm the previous MySQL variables. Please refer to your MySQL 5.0 Reference Manual for detailed description of these variables.

- bind-address—IP address to bind to.
- innodb_data_file_path—Paths to individual data files and their sizes. The full directory path to each data file is acquired by concatenating innodb_data_home_dir to the paths specified here. The file-sizes are specified in megabytes, hence the 'M' after the size specification above. InnoDB also understands the abbreviation 'G', 1G meaning 1024M. Starting from 3.23.44 you can set the file-size bigger than 4 GB on those operating systems which support big files. On some operating systems, files must be < 2 GB. The sum of the sizes of the files must be at least 10 MB.
- innodb_data_home_dir—The common part of the directory path for all InnoDB data files. If you do not mentioned this option in`my.cnf' the default is the datadir of MySQL. You can specify this also as an empty string, in which case you can use absolute file paths in innodb_data_file_path.
- innodb_log_file_size—Size of each log file in a log group in megabytes. Sensible values range from 1M to 1/nth of the size of the buffer pool specified below, where n is the number of log files in the group. The bigger the value, the less checkpoint flush activity is needed in the buffer pool, saving disk I/O. But bigger log files also mean that recovery will be slower in case of a crash. The combined size of log files must be < 4 GB on 32-bit computers.
- max_binlog_size—If a write to the binary (replication) log exceeds the given value, rotate the logs. You cannot set it to less than 1024 bytes, or more than 1 GB. The default is 1 GB.

CiscoWorks NCM 1.5 Upgrade

If the CiscoWorks NCM 1.5 upgrade failed, check the following files for detailed error messages:

- <CWNCM_Install_Dir> CWNCM_InstallLog.log
- All files in <CWNCM_Install_Dir>/server/log

If the CiscoWorks NCM 1.5 upgrade is successful, but CiscoWorks NCM 1.5 does not run, check the following:

- <CWNCM_Install_Dir> CWNCM_InstallLog.log file—If this file is truncated, this indicates that CiscoWorks NCM was not allocated enough disk space. Please contact your System Administrator to resolve disk space or other hardware issues.
- <CWNCM_Install_Dir>/jre folder—If JRE is installed successfully, the folder should contain approximately 600 files. An installation failure will result in less than 100 files. This could occur if Windows Explorer was not closed or other applications were running during the CiscoWorks NCM upgrade. You must close Windows Explorer and all other applications before running the CiscoWorks NCM 1.5 Service Pack Installer.

Running a multi-million record update can take a long time and you might think the upgrade has hung. This may not be the case. Before you cancel the upgrade installer, check the log files. The file is located in <CWNCM_Install_Dir> /server/Log/install_SP_UpgradeDatabase.log.

Using Gateways

When upgrading NCM where Gateways are used, after the upgrade run the "Deploy Remote Agent" task to re-install the upgraded Satellite agent on all of the remote Gateways. For information on configuring the Satellite functionality, see the Satellite User Guide for CiscoWorks Network Compliance Manager 1.8.

INDEX

S

U

V

W