



Installation Guide for Cisco Application Networking Manager 5.2

February 2012

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-26573-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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

Installation Guide for Cisco Application Networking Manager 5.2

© 2012 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface v

CHAPTER 1

Preparing to Install Application Networking Manager 1-1

- ANM Overview 1-1
- Server Requirements 1-3
- Client Requirements 1-5
- ANM Software Licensing Requirements 1-5
- Becoming the Root User 1-5

CHAPTER 2

Installing Application Networking Manager Server Software 2-1

- Information About Installing the ANM Server Software 2-1
- Information About ANM High Availability 2-2
- Installing ANM in Standalone Mode 2-2
- Installing ANM in HA Mode 2-3
- Uninstalling Application Networking Manager 2-6
 - Uninstalling ANM in Standalone Mode 2-6
 - Uninstalling ANM From HA Mode 2-7

CHAPTER 3

Upgrading the Application Networking Manager Server Software 3-1

- Information About Upgrading ANM Server Software 3-1
- Preparing to Upgrade ANM Server 3-3
- Installing the ANM Software Upgrade 3-3
 - Upgrading a Standalone ANM Server 3-4
 - Upgrading ANM HA Servers 3-6

CHAPTER 4

Getting Started with Application Networking Manager 4-1

- Acquiring and Uploading a Cisco Application Networking Manager License 4-1
- Uploading Site-Specific Certificate/Key Pair Files for Server Authentication 4-3
- Logging In To Cisco Application Networking Manager 4-3
 - Using the Firefox Web Browser to Access ANM 5.2 4-5
- Managing Cisco Application Networking Manager Licenses 4-6
- Changing Configuration Attributes After Installing Cisco Application Networking Manager 4-6

Example ANM Standalone Configuration Session 4-7
 Example ANM HA Configuration Session 4-8
 Example ANM Advanced Options Configuration Session 4-9
 ANM Ports Reference 4-9

CHAPTER 5

Troubleshooting Problems with Application Networking Manager Installation 5-1

Difficulties with Product Installation 5-1
 Login Problems After Installation 5-2
 Resetting the ANM Admin Password 5-2
 Restarting ANM 5-3
 Obtaining the Install Session Log 5-5
 Obtaining the Upgrade Session Log 5-5
 Starting Cisco Application Networking Manager 5-5
 Stopping Cisco Application Networking Manager 5-7
 Checking Why ANM Does Not Start 5-7
 Changing the Web Idle Session Timeout 5-8
 Reconfiguring After HA Installation 5-8
 Backing Up and Restoring Data in Standalone Mode 5-9
 Backing Up Data in Standalone Mode 5-9
 Restoring Data in Standalone Mode 5-10
 Backing Up and Restoring Data in HA Mode 5-11
 Backing Up Data in HA Mode 5-12
 Restoring Data in HA Mode 5-12

APPENDIX A

Red Hat Operating System Installation Tips A-1

Information About Installing Red Hat for Use with ANM A-1
 Red Hat Installation Procedure A-1

INDEX



Preface

Date: 9/18/12

This preface describes the audience, organization, and conventions of the *Installation Guide for Cisco Application Networking Manager 5.2*. It also provides information on how to obtain related information.

This preface included the following topics:

- [Audience, page v](#)
- [Organization, page v](#)
- [Related Documentation, page vi](#)
- [Conventions, page vi](#)
- [Obtaining Documentation and Submitting a Service Request, page vii](#)

Audience

This publication is for experienced system and network administrators who have specific knowledge in the following areas:

- Networking and data communications
- Network security
- Router and switch configuration

Organization

This publication is organized as follows:

Chapter	Description
Chapter 1, “Preparing to Install Application Networking Manager”	Identifies the information you must know before installing ANM.
Chapter 2, “Installing Application Networking Manager Server Software”	Provides step-by-step directions for installing ANM.
Chapter 3, “Upgrading the Application Networking Manager Server Software”	Provides step-by-step directions for upgrading ANM.

Chapter	Description
Chapter 4, “Getting Started with Application Networking Manager”	Provides step-by-step directions for configuring ANM.
Chapter 5, “Troubleshooting Problems with Application Networking Manager Installation”	Provides information for troubleshooting issues or problems you might encounter when installing and setting up ANM.
Appendix A, “Red Hat Operating System Installation Tips”	Describes the recommended Red Hat operating system installation procedure.

Related Documentation

In addition to this installation guide, the Application Networking Manager (ANM) documentation set includes the following publications. You can access the ANM documentation on www.cisco.com at: http://www.cisco.com/en/US/products/ps6904/tsd_products_support_series_home.html.

- *User Guide for the Cisco Application Networking Manager 5.2*—Includes complete information about ANM functionality and detailed procedures for its use. Contains all of the information found in online help; available either on [cisco.com](http://www.cisco.com) or from the ANM online help.
- Context-sensitive online help—Help topics for all pages in the UI (also provides access to a PDF file of the user guide). Select an option from the ANM GUI and click **Help**.
- *Release Note for the Cisco Application Networking Manager (Software Version 5.x)*—Includes resolved and open defects and any pertinent release specific information.
- *Supported Devices Table for the Cisco Application Networking Manager 5.2*—Includes complete supported network element and firmware versions for ANM.
- *Installation Guide for the Cisco Application Networking Manager 5.2 Virtual Appliance*—Includes complete information about ANM virtual appliance functionality, installation, configuration, and administration procedures.
- *API Reference Guide for Cisco Application Networking Manager 5.2*—Includes information about ANM Web Services, which provides APIs that support the operations for Application Control Engine (ACE) modules and appliances, Cisco Content Services Switch (CSS), and Cisco Content Switching Module (CSM) devices (for restrictive APIs) with all available releases.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	boldface font
Variables for which you supply values	<i>italic font</i>
Displayed session and system information	screen font
Information you enter	boldface screen font
Variables you enter	<i>italic screen font</i>
Menu items and button names	boldface font

Item	Convention
Selecting a menu item in paragraphs	Option > Network Preferences
Selecting a menu item in tables	Option > Network Preferences

**Note**

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

**Caution**

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

All documentation on ANM uses the following terms when referring to ACE modules and appliances:

- ACE = Any ACE network element (module or appliance)
- ACE appliance = Only ACE appliances
- ACE module = Only ACE modules

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 a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



CHAPTER 1

Preparing to Install Application Networking Manager

Date: 9/18/12

This chapter describes what you need to know and steps you need to take before installing or upgrading ANM.

For detailed hardware and Cisco IOS requirements, see the *Supported Devices Table for Application Networking Manager 5.2* at the following URL:

http://www.cisco.com/en/US/products/ps6904/products_device_support_tables_list.html



Note

This guide describes how to install and administer the Cisco ANM server software only. For information about installing the ANM Virtual Appliance software on a VMware virtual machine, see the *Installation Guide for Cisco Application Networking Manager 5.2 Virtual Appliance*.

This chapter includes the following sections:

- [ANM Overview, page 1-1](#)
- [Server Requirements, page 1-3](#)
- [Client Requirements, page 1-5](#)
- [ANM Software Licensing Requirements, page 1-5](#)
- [Becoming the Root User, page 1-5](#)

ANM Overview

ANM is a client/server application that enables you to perform all the following functions:

- Configure, monitor, and troubleshoot the functions of data center devices.
- Create policies for operations, applications owners, and server administration staff to activate and suspend network-based services without knowledge of, or ability to, change network configuration or topology.
- Manage the following product types:
 - Cisco Application Control Engine (ACE) module or appliance
 - Cisco Global Site Selector (GSS)
 - Cisco Content Services Switch (CSS)

- Cisco Catalyst 6500 Virtual Switching System (VSS) 1440
 - Cisco Catalyst 6500 series switch
 - Cisco 7600 series router
 - Cisco Content Switching Module (CSM)
 - Cisco Content Switching Module with SSL (CSM-S)
 - VMware vCenter Server
- Allow activation/suspension of VIP answers and DNS rules for the GSS.
 - The server runs on a dedicated Linux machine where you will need to install Red Hat Enterprise Linux. The client runs on supported versions of Internet Explorer or Firefox web browsers. A pair of ANM servers can be configured to run in High Availability mode.

ANM is available in two versions, allowing you to install it either on a dedicated server or on a VMware virtual machine as shown in [Figure 1-1](#). The capabilities and functions of the ANM software are the same regardless of which application you use. This guide uses the following terms to reference the two ANM applications:

- ANM server—Dedicated server with ANM server software and Red Hat Enterprise Linux (RHEL) operating system installed on it.
- ANM Virtual Appliance—VMware virtual appliance with ANM server software and Cisco Application Delivery Engine Operating System (ADE OS) installed on it. Cisco distributes ANM Virtual Appliance in Open Virtual Appliance (.OVA) format. For information about installing this type of ANM application, see the [Installation Guide for Cisco Application Networking Manager 5.2 Virtual Appliance](#).

Figure 1-1 ANM Server Deployment

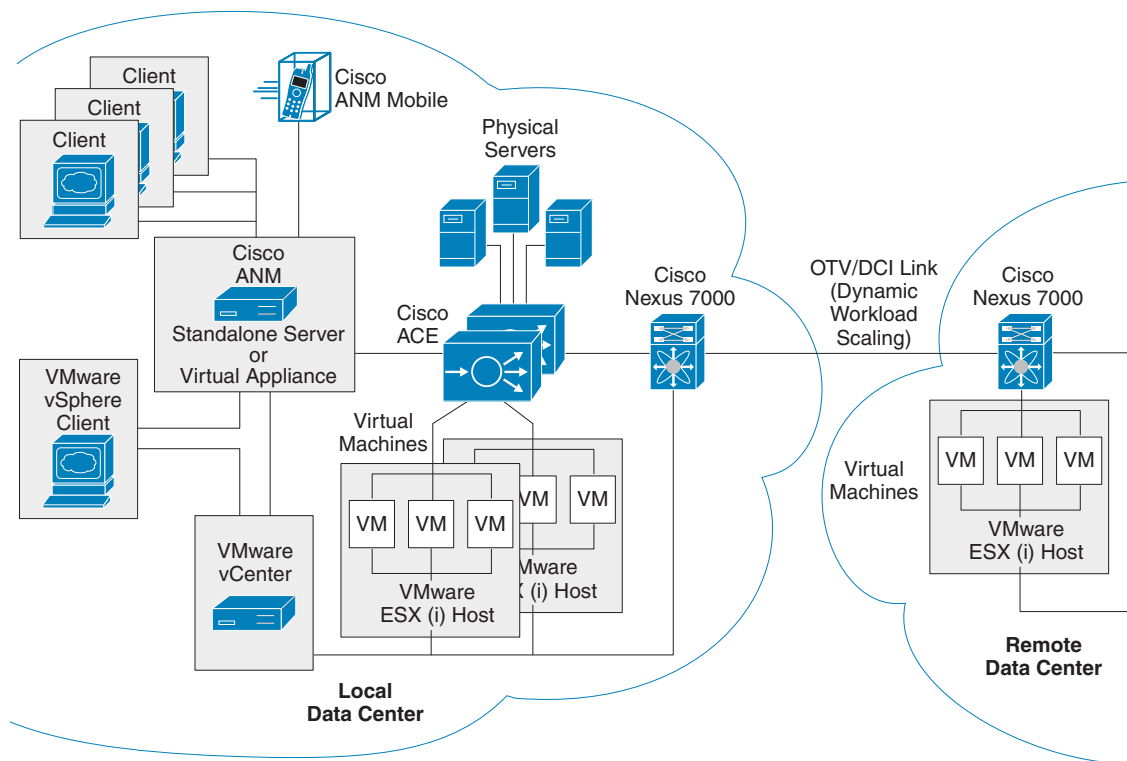


Figure 1-1 shows the following ANM and ACE features:

- VMware integration—Feature that enables ANM and the ACE to be integrated with VMware, allowing you to create and manage server farms for application delivery that consist of real servers that are a combination of physical servers and VMware virtual machines (VMs).
- Dynamic Workload Scaling—ACE feature that permits on-demand access to remote resources, such as VMs, that you own or lease from an Internet service provider (or cloud service provider). This feature uses Cisco's Nexus 7000 series switches with Overlay Transport Virtualization (OTV), which is a Data Center Interconnect (DCI) technology used to create a layer 2 link over an existing IP network between geographically distributed data centers.

For more information, see the “[Dynamic Workload Scaling Overview](#)” section in the *User Guide for the Cisco Application Networking Manager 5.2*.



Note Dynamic Workload Scaling requires ACE module or appliance software Version A4(2.0) or later and the Cisco Nexus 7000 series switch.

- ANM plug-in for vCenter Server—Plug-in on an ANM server or ANM Virtual Appliance that permits access to ANM's ACE server load-balancing functions from a VMware vSphere Client. For more information, see the “[Using ANM With Virtual Data Centers](#)” section in the *User Guide for the Cisco Application Networking Manager 5.2*.
- ANM Mobile—Feature that enables supported mobile devices to access to your ANM server or ANM Virtual Appliance, allowing you to manage the network objects in much the same way you do from an ANM client. Using a mobile device, you can run ANM Mobile as a native application or inside the mobile device's browser.

For more information, see [Chapter 19, “Using ANM Mobile”](#) in the *User Guide for the Cisco Application Networking Manager 5.2*.

Server Requirements

You install ANM server on an RHEL server only. ANM 5.1 supports the following RHEL operating system versions:

- RHEL 5 (base server) Update 3 (5.3) 32-bit or 64-bit Server Edition (Linux 2.6 kernel)
- RHEL 5 (base server) Update 4 (5.4) 32-bit or 64-bit Server Edition (Linux 2.6 kernel)
- RHEL 5 (base server) Update 5 (5.5) 32-bit or 64-bit Server Edition (Linux 2.6 kernel)
- RHEL 5 (base server) Update 6 (5.6) 32-bit or 64-bit Server Edition (Linux 2.6 kernel)

With ANM 4.1 and later releases, 64-bit Server Edition (Linux 2.6 Kernel) support is added (see the “[Information About Upgrading ANM Server Software](#)” section on page 3-1). The upgrade procedure is similar to the procedures as described in the RHEL 5.x upgrade (RHEL 5.3, 5.4, 5.5, or 5.6). The primary difference when you are not upgrading RHEL is that you do not have to back-up the data from the ANM server. This is because you are not upgrading the operating system software and the data that was previously configured on the ANM server remains intact.

During an ANM installation, MySQL (Sun's RDBMS) is automatically installed. If your system contains a different version of MySQL than the one used by ANM, it will be replaced with the version used by ANM during installation.

**Tip**

If you are installing RHEL 5 servers for the first time, to avoid installation failures or incompatibilities, see the [“Red Hat Operating System Installation Tips”](#) section on page A-1.

Your server must also meet the following minimum requirements:

**Note**

No external software or libraries are needed to install ANM.

Your server must also meet the following minimum requirements:

- A dedicated Linux server for ANM.
- A *minimum* of 2-GB random access memory (RAM); we recommend 4 GB RAM as a minimum for optimum performance.
- A *minimum* of 120-GB hard drive.
- Disk space requirements for ANM components as listed in [Table 1-1](#).

**Note**

Because ANM can potentially span multiple partitions, the disk requirements are listed on a directory basis. The partition that contains the specified directory must have at least the specified amount of free space indicated in [Table 1-1](#).

Table 1-1 ANM Disk Space Requirements

Directory	Disk Requirement
/opt/CSCOanm	2 GB
/var/lib/anm	45 GB

- 3-GHz Pentium III CPU or equivalent (dual processor supported; application is multithreaded but performance/capacity increase has not been specified).
- CD-ROM drive.
- 100-Mbps Ethernet interface for a single ANM configuration.
- One ANM server license for the active or primary server that you can download to the machine after installation by using the product authorization key (PAK).

If you are installing ANM with fault-tolerant high availability (HA), ensure that you have the following:

- Two full-duplex 100-Mbps Ethernet interfaces
- Two hosts with unique hostnames
- Primary IP addresses of both hosts configured on the same subnet (requirement)
- Secondary IP addresses (used as heartbeats) of both hosts configured on the same subnet (requirement)
- An additional ANM server license for the standby or backup server

**Note**

For more information about high availability functions, see the [“Installing ANM in HA Mode”](#) section on page 2-3.

Client Requirements

Each client accessing ANM running on a Linux server must meet the following minimum requirements:

- IBM-compatible computer with 2-GHz or faster Pentium processor
- At least 1-GB minimum RAM

The client must run one of the following operating systems:

- Windows 7
- Windows Vista with Service Pack 1
- Windows XP Professional with Service Pack 2
- Red Hat Enterprise Linux 5 (base server)

The client requires one of the following browsers:

- Microsoft Internet Explorer as follows:
- IE 7.0 on Windows XP Professional with Service Pack 2 or Windows Vista with Service Pack 1
- IE 8.0 on Windows XP Professional with Service Pack 2, Windows Vista with Service Pack 1, or Windows 7
- Firefox 3.6 on Windows XP Professional with Service Pack 2, Windows Vista with Service Pack 1, Windows 7, or Red Hat Enterprise Linux 5

**Note**

All browsers require that you enable cookies, JavaScript/scripting, Adobe Flash Player 9, and popup windows. Whenever ANM software is changed (upgrade or downgrade), end clients will need to clear their browser cache of each client.

ANM Software Licensing Requirements

Beginning with ANM software Version 5.2, the ANM software image includes a 90-day evaluation period that is activated when you install the software. This feature allows you to begin using ANM immediately after installing the software. You must install the permanent software license before the 90-day evaluation period expires to continue using ANM. When the time remaining to the evaluation period is down to 10 days, ANM issues daily reminders that the evaluation period is coming to an end and that you need to install the permanent license.

For more information about ANM software licenses, see the [“Acquiring and Uploading a Cisco Application Networking Manager License”](#) section on page 4-1

Becoming the Root User

To install ANM, you must be logged in as the root user on the server where you want to install ANM.

**Caution**

As the root user, you can adversely affect your operating environment if you are unaware of the effects of the commands that you use. If you are a relatively inexperienced Linux user, limit your activities as the root user to the tasks described in this publication.

From the Linux command line, log in as the root user by entering the following at the prompts:

> **login:** root

> **Password:** *root-password*

If you are already logged in, but not as the root user, use the **su** command to change your login to root:

su -

Password: *root-password*



CHAPTER 2

Installing Application Networking Manager Server Software

Date: 9/18/12

This chapter describes how to install or uninstall the Application Networking Manager (ANM) software on the server. This chapter includes the following sections:

- [Information About Installing the ANM Server Software, page 2-1](#)
- [Information About ANM High Availability, page 2-2](#)
- [Installing ANM in Standalone Mode, page 2-2](#)
- [Installing ANM in HA Mode, page 2-3](#)
- [Uninstalling Application Networking Manager, page 2-6](#)

Information About Installing the ANM Server Software

You can install ANM on the server in either high availability or standalone mode. High availability (or *fault tolerance*) ensures that your network services and applications are always available.

During the ANM installation, the following items are installed:

- MySQL (a Sun RDBMS)—If your system contains a different version of MySQL than the one used by ANM, it is replaced with the version used by ANM during installation.
- Linux System Users—The following ANM user accounts are created on the Linux filesystem: `anm` and `anm-mysql`.

You can enable HTTP during installation. By default, the HTTP enable field displays [False]. You enable HTTP by changing that value to **True**. If HTTP is disabled during installation, you can enable HTTP by entering the `/opt/CSCOanm/bin/anm-tool configure` command at the command line.

For more information, see the “Changing Configuration Property Values” section in the online help or Chapter 18, “[Troubleshooting Cisco Application Networking Manager Problems](#)” of the *User Guide for the Cisco Application Networking Manager 5.2*.

Information About ANM High Availability

ANM high availability (HA) consists of two peer hosts, an active (primary) and a standby (secondary or backup host). Both peers in an ANM HA system *must* be running the same version of ANM.

Each host must have at least two network interfaces:

- A primary interface, which is normally used to access the host.
- A heartbeat interface, which is used as a redundant network element in case the primary host fails. The heartbeat interfaces of the two hosts must be connected through a crossover Ethernet connection, which must be a physical connection, configured on its own (private) subnet.

ANM does not configure the primary and heartbeat IP addresses for the primary (Node 1) and secondary (Node 2) ANM servers. You must manually configure these addresses. Typically, the heartbeat IP address is not on the same subnet as the subnet that connects the nodes to your network.

Guidelines and Restrictions

This topic includes the following guidelines and restrictions:

- The heartbeat interfaces on Node 1 and Node 2 should be configured on a private subnet that only includes each node's individual IP addresses.
- You must designate eth0 as the primary interface and eth1 as the heartbeat interface. For more information about high availability, see the [“Installing ANM in HA Mode” section on page 2-3](#).
- When you install ANM, you need to provide values for high availability parameters. Because there are no default values for the high availability parameters, you cannot specify *interactive=0* during installation.
- The parameter *interactive=0* conflicts with *ha=1* and should *not* be used during the installation.
- Both peers in an ANM HA system must be running on the same software version of ANM as well as the same underlying operating system, either 32-bit or 64-bit Server Edition (Linux 2.6 Kernel). Do not attempt an ANM HA pair between a 32-bit and 64-bit Server Edition (Linux 2.6 Kernel) running system.

Installing ANM in Standalone Mode

You can install ANM on the server in standalone mode. During the installation of ANM, you must specify an admin password.


Guidelines and Restrictions

The ANM software image includes a 90-day evaluation period, which means that you can begin using ANM immediately without installing a license. However, you must install the permanent licenses before the evaluation period expires to continue using ANM (see the [“Acquiring and Uploading a Cisco Application Networking Manager License” section on page 4-1](#)).

Prerequisites

Ensure that your system meets the requirements listed in the [“Server Requirements” section on page 1-3](#).

Procedure

-
- Step 1** Insert the CD-ROM into the drive of the Linux server and mount to the /cdrom directory from the command line.
- Step 2** After you have logged in, change to the /cdrom directory or the directory to which you mounted the CD.
- Step 3** From the Linux command line, log in as the root user as described in the [“Becoming the Root User” section on page 1-5](#).
- Step 4** (Optional) Change the access mode of the installation file by entering the following command:
chmod a+x anm-5.2.bin
- Step 5** Start the installation script by entering the following command:
./anm-5.2.bin [--interactive=0|1] [--admin-password=admin-password]
 The **--interactive** keyword specifies whether there is an interaction during ANM installation. Enter **0** to specify that there will be no possible interaction. Enter **1** to specify that there will be an interaction. The default value is **1**. Note that *admin-password* is required only for noninteractive mode.
 The installation begins and status messages appear on your login window. When Done appears, the installation script has finished.
- Step 6** (Optional) From the command line, install the license on the ANM server by entering the following command:
/opt/CSCOanm/bin/anm-license install /path/ANMxxxxxxxxxxxxxxxxx.lic
 where *path* is the location of the license file and *ANMxxxxxxxxxxxxxxxxx.lic* is the name of the license file.
-  **Note** ANM includes a 90-day evaluation period that does not require a license (see [Guidelines and Restrictions](#)).
-
- Step 7** Unmount the CD-ROM, and then continue to the [“Getting Started with Application Networking Manager” section on page 4-1](#).
-

Installing ANM in HA Mode

You can install ANM on the server in HA mode, which requires two hosts. One host takes an *active* role and the other host takes a *standby* role. The active host provides ANM functionality. If something happens to the active host, the standby takes over after a brief delay. All active sessions are lost when the standby server takes over; therefore, you need to log in again. To install ANM in HA mode, complete the following steps on *both* servers. To prepare for the questions that are part of the installation, see the [“Information About ANM High Availability” section on page 2-2](#).

Guidelines and Restrictions

This topic includes the following guidelines and restrictions:

- The ANM software image includes a 90-day evaluation period, which means that you can begin using ANM immediately without installing a license. However, you must install the permanent licenses before the evaluation period expires to continue using ANM (see the [“Acquiring and Uploading a Cisco Application Networking Manager License” section on page 4-1](#)).

- During the installation of ANM 5.2, you must specify an admin password. Because you are installing ANM in HA mode, you must also specify a MySQL password.



Note The MySQL password *must* be the same on both HA nodes.

- [Table 2-1](#) describes the installation parameters. Use these parameters as described in the “[Installing ANM in HA Mode](#)” section on page 2-3.



Note All parameter values shown in [Table 2-1](#) must be identical on both servers except for the HA Node ID parameter.

Table 2-1 ANM High Availability Installation Parameter Descriptions

Installation Parameter	Description
Database Password	Password for the MySQL database.
HA Node 1 Uname	Name of Node 1, which can be returned by entering the uname -n command on the host.
HA Node 2 Uname	Name of Node 2, which can be returned by entering the uname -n command on the host.
HA Node 1 Primary IP	IP address that Node 1 uses for normal (nonheartbeat related) communication. This IP address must be on the same subnet as the primary IP address of Node 2.
HA Node 2 Primary IP	IP address that Node 2 uses for normal (nonheartbeat related) communication. This IP address must be on the same subnet as the primary IP address of Node 1.
HA Node 1 Heartbeat IP	IP address associated with the crossover network interface of Node 1. This IP address must be on the same subnet as the heartbeat IP address of Node 2. Typically, this subnet is private.
HA Node 2 Heartbeat IP	IP address associated with the crossover network interface of Node 2. This IP address must be on the same subnet as the heartbeat IP address Node 1. Typically, this subnet is private.
HA Virtual IP	Virtual IP address that is associated with the active host. This IP address must be on the same subnet as the primary IP addresses of both Node 1 and Node 2. You manually create the IP address during the ANM HA installation. We recommend that the IP address be in the same subnet of the primary IP address of the active/standby node.
HA Node ID	Predetermined node ID of the node, which must be either 1 or 2.

Prerequisites

Ensure that your HA system hosts meet the requirements listed in the “[Server Requirements](#)” section on page 1-3.

Procedure

- Step 1** Insert the CD-ROM into the drive of the Linux server and mount to the /cdrom directory.
- Step 2** From the command line, change to the /cdrom directory or the directory to which you mounted the CD.
- Step 3** Log in as the root user as described in the [“Becoming the Root User”](#) section on page 1-5.
- Step 4** (Optional) Change the access mode of the installation file by entering the following command:

```
chmod a+x anm-5.2.bin
```

- Step 5** Start the installation script by entering the following command:

```
./anm-5.2.bin --ha=1
```

The `--ha=1` keyword specifies this as an HA installation. The default value for HA is 0. HA installations are interactive; if you enter `--interactive=0`, the installation will fail. The installation begins and status messages appear in your login window.

An HA installation requires that two hosts be configured. You must configure the hosts identically, but you can have unique hostnames (except for the node ID).



Caution

Each host must have a unique hostname, or an error will result. You can use the `uname -n` command to verify that the names are unique.

- Step 6** When you see a series of prompts that request information, do the following:
- Enter the MySQL database password in the space provided.
 - Enter the name of Node 1 in the space provided.
 - Enter the name of Node 2 in the space provided.
 - Enter the IP address of the primary network interface card (NIC) on Node 1 in the space provided.
 - Enter the IP address of the primary NIC on Node 2 in the space provided.
 - Enter the IP address of the HeartBeat NIC on Node 1 in the space provided.
 - Enter the IP address of the HeartBeat NIC on Node 2 in the space provided.
 - Enter the virtual IP address of the Node 1–Node 2 pair in the space provided.
 - Enter the node ID of the node that you are configuring in the space provided. For Node 1, enter **1**. For Node 2, enter **2**.
 - Wait for the Done prompt to appear, at which point the installation script has finished.
 - (Optional) Install the ANM license on the ANM server by entering the following command:


```
/opt/CSCOanm/bin/anm-license install /path/ANMxxxxxxxxxxxxxxxxx.lic
```

 where *path* is the location of the license file and *ANMxxxxxxxxxxxxxxxxx.lic* is the name of the license file.



Note

ANM includes a 90-day evaluation period that does not require a license (see [Guidelines and Restrictions](#)).

- Step 7** Unmount the CD-ROM and repeat the previous steps on the other HA host. After your standby host is installed, continue to the [“Getting Started with Application Networking Manager”](#) section on page 4-1.

**Note**

Some ANM processes will run on a standby ANM host. For more information, see the “Configuring High Availability” chapter in the online help or in the *User Guide for the Cisco Application Networking Manager 5.2*.

Uninstalling Application Networking Manager

This section describes how you can uninstall the ANM application from the standalone or HA-mode.

Guidelines and Restrictions

This topic includes the following guidelines and restrictions:

- Make sure that you uninstall ANM before you install it again.
- During the uninstall process, you are given the opportunity to save the current list of ANM users to the server. If you plan to reinstall ANM and utilize the same users, save the list of users.
- Uninstalling ANM also uninstalls MySQL.

This section includes the following topics:

- [Uninstalling ANM in Standalone Mode, page 2-6](#)
- [Uninstalling ANM From HA Mode, page 2-7](#)

Uninstalling ANM in Standalone Mode

You can uninstall the Application Networking Manager application from the standalone mode.

Prerequisites

This topic includes the following prerequisites:

- Make sure that your current working directory is *not* `/opt/CSCOanm` or one of its subdirectories when performing the uninstall. Uninstalling ANM results in the `/opt/CSCOanm` directory being removed.
- Cisco recommends that you back up your current license file and ANM configuration before uninstalling ANM (see the “[Backing Up and Restoring Data in Standalone Mode](#)” section on [page 5-9](#)).
- If you are using the ANM plug-in to integrate ANM with VMware vCenter Server, make sure that the plug-in is unregistered before you uninstall ANM. For information about using ANM with VMware vCenter Server and unregistering the plug-in, see the *User Guide for the Cisco Application Networking Manager 5.2* and Appendix B, “[Using ANM With Virtual Data Centers](#)”.

Procedure

-
- Step 1** From the Linux command line, log in as the root user as described in the “[Becoming the Root User](#)” section on [page 1-5](#).
- Step 2** Uninstall ANM by entering the following command:
- ```
/opt/CSCOanm/bin/anm-tool uninstall
```
- Step 3** Type **Yes** when you are prompted for confirmation to uninstall.

- Step 4** When prompted to preserve the current list of ANM users, enter one of the following:
- **Yes**—The current list of users is saved on the server for use with the subsequent ANM installation.
  - **No**—The current list of users is not saved.



**Note** These users are the `anm` and `anm-mysql` Linux user accounts that are created on the Linux filesystem during the installation of ANM; they are not the user accounts that are used to log in to ANM. If you have local custom scripts based on the user IDs of these Linux user accounts, you should preserve them to avoid having to remap them after performing an ANM upgrade.

When the uninstallation is complete, the `/opt/CSCOanm` directory, RPMs, and application files are deleted.

## Uninstalling ANM From HA Mode

You can uninstall the Application Networking Manager application from the HA mode.

### Prerequisites

This topic includes the following prerequisites:

- Make sure that your current working directory is *not* `/opt/CSCOanm` or one of its subdirectories when performing the uninstall. Uninstalling ANM results in the `/opt/CSCOanm` directory being removed.
- We recommend that you back up your current license file and ANM configuration before uninstalling ANM (see the “[Backing Up and Restoring Data in HA Mode](#)” section on page 5-11).
- If you are using the ANM plug-in to integrate ANM with VMware vCenter Server, make sure that the plug-in is unregistered before you uninstall ANM. For information about using ANM with VMware vCenter Server and unregistering the plug-in, see the *User Guide for the Cisco Application Networking Manager 5.2* and Appendix B, “[Using ANM With Virtual Data Centers](#).”

### Procedure

- Step 1** From the Linux command line, log in as the root user as described in the “[Becoming the Root User](#)” section on page 1-5.
- Step 2** From the standby server, uninstall ANM by entering the following command:
- ```
/opt/CSCOanm/bin/anm-tool uninstall
```
- Step 3** From the active server, uninstall ANM by entering the following command:
- ```
/opt/CSCOanm/bin/anm-tool uninstall
```
- Step 4** Type **Yes** when you are prompted for confirmation to uninstall.
- Step 5** When prompted to preserve the current list of ANM users, enter one of the following:
- **Yes**—The current list of users is saved on the server for use with the subsequent ANM installation.
  - **No**—The current list of users is not saved.



---

**Note** These users are the anm and anm-mysql Linux user accounts that are created on the Linux filesystem during the installation of ANM; they are not the user accounts used to log in to ANM. If you have local custom scripts based on the user IDs of these Linux user accounts, you should preserve them to avoid having to remap them after performing an ANM upgrade.

---

When the uninstallation is complete, the /opt/CSCOanm directory RPMs and application files are deleted.

---



# CHAPTER 3

## Upgrading the Application Networking Manager Server Software

**Date:** 9/18/12

This chapter describes how to upgrade the Application Networking Manager server software to ANM 5.2. This chapter includes the following sections:

- [Information About Upgrading ANM Server Software, page 3-1](#)
- [Preparing to Upgrade ANM Server, page 3-3](#)
- [Installing the ANM Software Upgrade, page 3-3](#)

### Information About Upgrading ANM Server Software

This section provides information about upgrading to ANM server software Version 5.2 from a previous version.



**Note**

To ensure that all network elements (both staged and imported) are migrated, you must deploy network elements that are not yet imported (staged objects). Otherwise, you can choose to import any staged network elements after the upgrade completes.

[Table 3-1](#) shows the upgrade path that you must follow when upgrading to ANM software Version 5.2.

**Table 3-1** Upgrade Paths for ANM 5.2



| Current Release             | Previous Releases                     |
|-----------------------------|---------------------------------------|
| Upgrade to ANM server 5.2.1 | From ANM server 5.1 or 5.2 only.      |
| Upgrade to ANM server 5.2   | From ANM server 5.1 only.             |
| Upgrade to ANM server 5.1   | From ANM server 4.1, 4.2 or 4.3 only. |
| Upgrade to ANM server 4.3   | From ANM server 4.1 or 4.2 only.      |
| Upgrade to ANM server 4.2   | From ANM server 4.1 only.             |

**Table 3-1** Upgrade Paths for ANM 5.2 (continued)

| Current Release                         | Previous Releases                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Upgrade to ANM server 4.1               | <p>From ANM 3.0, ANM 3.1 and ANM 3.2 only.</p> <p><b>Note</b> If you need to upgrade to ANM 3.0 before upgrading to ANM 4.1, when you upgrade the ANM software to version 3.0, the network elements that were already imported into ANM software versions 2.2, 2.1(1), 2.1, or 2.0 will properly migrate. If you need to upgrade to ANM 3.1 before upgrading to ANM 4.1, when you upgrade the ANM software to version 4.1 the network elements that were already imported into ANM software 3.0 will properly migrate.</p> <p><b>Note</b> ANM 3.2 can be upgraded from ANM 3.0 or ANM 3.1.</p> |
| Upgrade to ANM 3.0, ANM 3.1 and ANM 3.2 | <p>From ANM 1.2, requires an intermediate upgrade to ANM 2.2, 2.1(1), 2.1, or 2.0. See the Installation Guide for Application Networking Manager 2.2 and 2.1 for details.</p> <p><b>Note</b> We recommend that you initially upgrade to ANM 2.2 before you upgrade to ANM 3.0 as described in this document.</p>                                                                                                                                                                                                                                                                               |


Table 3-2 contains a list of features and their status after the upgrade has occurred. For explanations and information about these features, see the *User Guide for the Cisco Application Networking Manager 5.2*.

**Table 3-2** Post Upgrade Feature Status

| Feature                                         | Upgrade | Upgrade Status                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network Elements                                | Y       | All imported network elements are migrated.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Staged objects (those that were never deployed) | N       | <p>If you are upgrading to ANM 3.0 before upgrading to ANM 4.x and then to ANM 5.2, staged objects do not migrate to ANM 3.0 from previous versions of ANM. Perform network element import to add network elements.</p> <p> <b>Note</b> Before the upgrade, ensure that staged objects are deployed or the data will be lost.</p>                                                                                                                               |
| Building Blocks                                 | Y       | <p>Building Blocks are migrated.</p> <p> <b>Note</b> Beginning with ANM software Version 5.1, the building block feature by default is hidden. If you have used the building block feature in the past and want to continue using it after upgrading to ANM 5.1, you must enable it. For more information, see the “<a href="#">Enabling the Building Block Feature</a>” section in the <i>User Guide for the Cisco Application Networking Manager 5.2</i>.</p> |
| Role Based Access Control (RBAC)                | Y       | Username, roles, domains, and all relationships are maintained.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |



**Table 3-2 Post Upgrade Feature Status (continued)**

| Feature                                         | Upgrade | Upgrade Status                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network Elements                                | Y       | All imported network elements are migrated.                                                                                                                                                                                                                                                                                                                                                                        |
| Staged objects (those that were never deployed) | N       | <p>If you are upgrading to ANM 3.0 before upgrading to ANM 4.x and then to ANM 5.2, staged objects do not migrate to ANM 3.0 from previous versions of ANM. Perform network element import to add network elements.</p> <p> <b>Note</b> Before the upgrade, ensure that staged objects are deployed or the data will be lost.</p> |
| User-roles                                      | Y       | Custom roles will be retained.                                                                                                                                                                                                                                                                                                                                                                                     |
| Monitoring Data                                 | N       | All monitoring data, including historical data, is lost during an upgrade. For more information, see the <a href="#">“Preparing to Upgrade ANM Server”</a> section on page 3-3.                                                                                                                                                                                                                                    |

## Preparing to Upgrade ANM Server

If you enabled HTTP on ANM before the upgrade, it is still enabled after the upgrade. If you prefer to use HTTPS to make your connection more secure, change the properties file and restart ANM.

If you restore the ANM database from a backup repository and a virtual context that is in the repository has been removed from the network element, ANM removes that context from the database and the context does not appear in the ANM user interface.

During the upgrade process, the entire ANM configuration and the ANM user/domain settings are upgraded. Monitoring data is lost during an upgrade. If you want to save the monitoring data, use the Historical Data Export feature (Monitor > Settings > Historical Data Export) to export the current monitoring data to an external data store *before* you perform an upgrade.

## Installing the ANM Software Upgrade

The procedures in this section show how to upgrade ANM in either standalone mode or high availability (HA) mode, which allows you to perform the following tasks:

- Restore the upgraded ANM server using an ANM backup from another ANM server or ANM Virtual Appliance.
- Upgrade the Red Hat operating system during the ANM upgrade process.

### Guidelines and Restrictions

This topic includes the following guidelines and restrictions:

- During the ANM upgrade, MySQL is automatically installed. If your system contains a different version of MySQL than the one used by ANM, it is replaced with the version used by ANM during installation.
- You can use backup file taken from a 32-bit Server Edition when upgrading to ANM 5.2 operating in a 64-bit Server Edition either in standalone or HA mode.

- At the end of the upgrade process, you must install the ANM license that is applicable to the upgraded server. If the backup you use during the upgrade process belongs to a different host, you must install the appropriate license because an ANM license is tied to the server's MAC address.



**Caution** As the root user, you can adversely affect your operating environment if you are unaware of the effects of the commands that you use. If you are an inexperienced Linux user, you should limit your activities as the root user to the tasks described in this procedure.

### Prerequisites

The ANM server being upgraded to ANM software Version 5.2 must be using ANM software Version 5.1.

This section includes the following topics:

- [Upgrading a Standalone ANM Server, page 3-4](#)
- [Upgrading ANM HA Servers, page 3-6](#)

## Upgrading a Standalone ANM Server

This procedure shows how to use the long method to upgrade the software from ANM 5.1 to ANM 5.2 on an ANM server operating in standalone mode. The procedure includes an optional step to upgrade the Red Hat operating system.

### Procedure

- Step 1** Log into the server as the root user (see the “[Becoming the Root User](#)” section on page 1-5) and create an ANM backup to restore the ANM inventory at the end of the upgrade procedure by doing one of the following:
- To create a backup from ANM server, enter the following command from the ANM server command line:  

```
/opt/CSCOanm/bin/anm-tool backup path/backup_filename
```

 where *path/backup\_filename* is the name of the backup, including the path information.
  - To create a backup from ANM Virtual Appliance, enter the following command from the ANM Virtual Appliance ADE-OS command line:  

```
anm-tool save-inventory disk:backup_filename
```

 where *backup\_filename* is the name of the backup that is saved to disk: on ANM Virtual Appliance.



**Note** The special characters allowed in the file name are as follows:  
 ! , @ , \$ , % , ^ , \_ , + , = , { , } , [ , ] , : , , , (comma) , ?.

- Step 2** Copy the backup file to a safe, remote (nonlocal) location, such as a different computer, a USB flash or external drive, or CD-RW disk.
- Step 3** Uninstall ANM by entering the following command:  

```
/opt/CSCOanm/bin/anm-tool uninstall
```

- Step 4** When prompted to preserve the current list of ANM users, enter one of the following:
- **Yes**—The current list of users is saved on the server for use with the subsequent ANM installation.
  - **No**—The current list of users is not saved.



---

**Note** These users are the `anm` and `anm-mysql` Linux user accounts that are created on the Linux filesystem during the installation of ANM; they are not the user accounts that are used to log in to ANM. If you have local custom scripts based on the user IDs of these Linux user accounts, you should preserve these user accounts to avoid having to remap them after performing an ANM upgrade.

---

When the uninstallation is complete, the `/opt/CSCOanm` directory RPMs and application files are deleted.

- Step 5** (Optional) Install Red Hat Enterprise Linux following the procedure described in the [“Red Hat Operating System Installation Tips”](#) section on page A-1. Skip this step if you are upgrading the ANM server software only.
- Step 6** Copy the ANM backup file that you created in [Step 1](#) to the ANM server.
- Step 7** Insert the ANM 5.2 CD-ROM into the drive of the Linux server and mount to the `/cdrom` directory.
- Step 8** Change your directory to the `/cdrom` directory or the directory to which you mounted the CD and start the upgrade by entering the following command:

```
./anm-5.2.bin upgrade path/backup_filename
```

where `path/backup_filename` is the path and filename of the backup that you copied to the ANM server.

The installation and upgrade begins and status messages appear on your login window. When the Done prompt appears, the upgrade script has finished, which includes restoring the ANM inventory using the backup.

- Step 9** Unmount the CD-ROM.
- Step 10** If the backup file used to restore the ANM server configuration was created on another ANM server or on ANM Virtual Appliance, perform the following steps:
- a. Install the appropriate license for the server. Skip this step if the backup was created from the server you just upgraded (see the [“Using ANM License Manager to Manage ANM Server or Demo Licenses”](#) section in the *User Guide for the Cisco Application Networking Manager 5.2* or in the online help).
  - b. If the port information and configuration attributes of the backup are different than the values of the original ANM server configuration, you need to modify the port information and configuration attributes to match the original ANM server configuration (see the [“Changing Configuration Attributes After Installing Cisco Application Networking Manager”](#) section on page 4-6).
  - c. If the backup was created on an ANM server configured to operate in HA mode, you must set the configuration to standalone mode by doing the following:
    1. Enter the following command:

```
/opt/CSCOanm/bin/anm-tool -ha=0 configure
```

A series of prompts appears.
    2. At the “Check existing configuration files?” prompt, enter **n** (no). Leave all other options at their default values unless you need to modify any of them.
    3. At the “Commit these values?” prompt, enter **y** (yes).

- Step 11** Clear the browser cache on all client devices before accessing the ANM GUI to avoid possible issues with the GUI function buttons being inaccessible.
- 

#### Related Topics

- [Installing the ANM Software Upgrade, page 3-3](#)
- [Upgrading ANM HA Servers, page 3-6](#)

## Upgrading ANM HA Servers

This procedure shows how to upgrade the software from ANM 5.1 to ANM 5.2 on two ANM servers operating in high availability mode and includes an optional step for upgrading the Red Hat operating system.

#### Procedure

---

- Step 1** Log into your current running version of ANM and make sure that active and standby ANM servers are synchronized. See the ANM context sensitive online help for more information.
- Step 2** From the standby ANM server, log into the server as the root user (see the [“Becoming the Root User” section on page 1-5](#)) and perform the following steps:

- a. Create an ANM backup to restore the ANM inventory at the end of the upgrade procedure by entering the following command from the ANM server command line:

```
/opt/CSCOanm/bin/anm-tool backup path/backup_filename
```

where *path/backup\_filename* is the name of the backup, including the path information.



**Note** We recommend that you use a backup created from the server being upgraded; however, you can use a backup created from another ANM server or ANM Virtual Appliance running the same version ANM.

---

- b. Copy the backup file to a safe, remote (nonlocal) location, such as a different computer, a USB flash or external drive, or CD-RW disk.
- c. Uninstall ANM by entering the following command:

```
/opt/CSCOanm/bin/anm-tool uninstall
```

- d. When prompted to preserve the current list of ANM users, enter one of the following:
- **Yes**—The current list of users is saved on the server for use with the subsequent ANM installation.
  - **No**—The current list of users is not saved.



**Note** These users are the `anm` and `anm-mysql` Linux user accounts that are created on the Linux filesystem during the installation of ANM; they are not the user accounts that are used to log in to ANM. If you have local custom scripts based on the user IDs of these Linux user accounts, you should preserve these user accounts to avoid having to remap them after performing an ANM upgrade.

---

When the uninstall is complete, the /opt/CSCOanm directory and all associated RPM's and application files are deleted.

- e. (Optional) Install Red Hat Enterprise Linux following the procedure described in the “[Red Hat Operating System Installation Tips](#)” section on page A-1. Skip this step if you are upgrading the ANM server software only.
- f. Copy the ANM backup file that you created in Step 2a to the ANM server.

**Step 3** From the active ANM server, log into the server as the root user and perform the following steps:

- a. Repeat Steps 2a to 2f.
- b. Insert the ANM 5.2 CD-ROM into the drive of the Linux server and mount to the /cdrom directory.
- c. Change your directory to the /cdrom directory or the directory to which you mounted the CD by entering the following command:

```
./anm-5.2.bin upgrade path/backup_filename
```

where *path/backup\_filename* is the path and filename of the backup that you copied to the ANM server.

The installation and upgrade begins and status messages appear in your login window. When the Done prompt appears, the upgrade script has finished, which includes restoring the ANM inventory using the backup.

- d. If the backup you used during the upgrade process belongs to a different host, install the appropriate license for the server. Skip this step if the backup was created on the server you just upgraded.
- e. Unmount the CD-ROM.

**Step 4** From the standby ANM server, repeat Steps 3b to 3e to upgrade the standby server.

**Step 5** Clear the browser cache on all client devices before accessing the ANM GUI to avoid possible issues with the GUI function buttons being inaccessible.

---

#### Related Topics

- [Installing the ANM Software Upgrade, page 3-3](#)
- [Upgrading a Standalone ANM Server, page 3-4](#)





## CHAPTER 4

# Getting Started with Application Networking Manager

---

**Date:** 9/18/12

This chapter describes how to set up your Cisco Application Networking Manager (ANM) server. After completing the procedures in this chapter, ANM is ready for you to import network devices to monitor and manage. For details about using ANM, including how to import network devices, see the [User Guide for the Cisco Application Networking Manager 5.2](#).

This chapter includes the following sections:

- [Acquiring and Uploading a Cisco Application Networking Manager License, page 4-1](#)
- [Uploading Site-Specific Certificate/Key Pair Files for Server Authentication, page 4-3](#)
- [Logging In To Cisco Application Networking Manager, page 4-3](#)
- [Managing Cisco Application Networking Manager Licenses, page 4-6](#)
- [Example ANM Standalone Configuration Session, page 4-7](#)
- [Example ANM HA Configuration Session, page 4-8](#)
- [Example ANM Advanced Options Configuration Session, page 4-9](#)
- [ANM Ports Reference, page 4-9](#)

## Acquiring and Uploading a Cisco Application Networking Manager License

Beginning with ANM software Version 5.2, the ANM software image includes a 90-day evaluation period that is activated when you install the software. This feature allows you to begin using ANM immediately after installing the software; however, you must install the permanent software license before the 90-day evaluation period expires to continue using ANM.



### Note

This section describes how to install an ANM license using the CLI; however, after you acquire the license, you can choose to install a license using the ANM license manager providing you install the license prior to the expiration of the 90-day evaluation period (see the [“Using ANM License Manager to Manage ANM Server or Demo Licenses”](#) section in the *User Guide for the Cisco Application Networking Manager 5.2* or the ANM online help). If the evaluation period has expired, you must use the CLI to install the license.

Before you can acquire an ANM license, you must be a registered Cisco.com user and you must have the service license authorization key (PAK) that was shipped with your software CD. For more information, see the “Understanding ANM License Information” section in the “Administering the Cisco Application Networking Manager” chapter of the online help or the *User Guide for the Cisco Application Networking Manager 5.2*.

**Note**

The license installation script reinitializes ANM. If you have performed an HA upgrade, it may also take some time for the system to determine which host is the active host. It may take several minutes before you can log in to ANM after the installation or upgrade.

**Procedure**

**Step 1** From Cisco.com, go to <http://www.cisco.com/go/license>. You are asked to log into Cisco.com. If you are not a registered user, you are given a number of options including the option to log in without registering. Once logged in, you are prompted to enter the product authorization key (PAK).

**Step 2** Enter the product authorization key (PAK) exactly as it appears on the label that accompanied the Cisco Information Packet. If you are unable to locate the PAK, contact your Cisco support team or click on the link for a demonstration license.

**Note**

A demo license is valid for 90 days after it is issued. After 90 days, the product will require a standard license.

**Step 3** Follow the instructions for registration on the license website. After you finish registering, a message appears that confirms your registration, and an e-mail that contains the license/key file is sent to you at the e-mail address that you provided during product registration.

**Step 4** After you receive your software license key by e-mail, save the e-mail and the license file (.lic) that is attached to the e-mail to a temporary directory on your hard drive for safekeeping.

**Step 5** (Optional) Copy the file from the temporary directory to your ANM server.

**Step 6** From the command line, install the license on the ANM server by entering the following command:

```
/opt/CSCOanm/bin/anm-license install /path/ANMxxxxxxxxxxxxxxxxx.lic
```

where *path* is the location of the license file and *ANMxxxxxxxxxxxxxxxxx.lic* is the name of the license file.

You can install either the ANM-SERVER-50-K9 license or the ANM-DEMO license, which expires in 90 days.

**Step 7** Log in to ANM and under the Administration tab, choose **ANM Management > License Management** to verify that the installed license is listed.

**Note**

For more information about licenses, see the “Managing Cisco Application Networking Manager Licenses” section on page 4-6.



# Uploading Site-Specific Certificate/Key Pair Files for Server Authentication

This section describes how to install a third party certificate/key pair that is used to authenticate your ANM server. The ANM software installation process includes a self-signed certificate/key pair for this purpose; however, you can choose not to use it by installing a third party certificate/key pair.

**Caution**

Installing a third-party certificate/key pair overwrites the self-signed certificate/key pair included with the ANM software. There is no documented way to revert to the self-signed certificate/key pair after you install a third party certificate/key pair.

**Guidelines and Restrictions**

This topic includes the following guidelines and restrictions:

- You can install a third-party certificate/key pair at any time, not just during the installation of ANM.
- In HA mode, you must perform this procedure on both ANM servers.

**Procedure**

**Step 1** If necessary, copy the certificate and key pair files from the temporary directory to your ANM server.

**Step 2** From the command line, install the certificate and key pair by entering the following command:

```
/opt/CSCOanm/bin/anm-certificate install certificate key [key-password]
```

where *certificate* is the name of the certificate file that you are installing, *key* is the name of the certificate key pair file, and the optional *key-password* is the key password, which is required only if the key is encrypted.

## Logging In To Cisco Application Networking Manager

You access ANM features and functions through a web-based interface. The ANM login window allows you to log into the ANM server, change the password for your account, and obtain online help by clicking **Help**.

**Procedure**

**Step 1** Log in to ANM by doing one the following:

- To log in after a new installation, in your browser address field, enter **https://host** or **http://host** depending on whether or not you enabled non-SSL HTTP during the installation of ANM.

**Note**

You can omit the port numbers from the URL because ANM uses the default web ports for HTTP and HTTPS, which are 80 and 443 respectively.

**Caution**

If you want to log in using HTTP, you must change the properties file. See the [“Changing Configuration Attributes After Installing Cisco Application Networking Manager”](#) section on page 4-6 for more information. Remember that if you enable HTTP, you are making your connection to ANM less secure.

- To log in after an upgrade, in your browser address field, enter **https://host:10443** or **http://host:10080** depending on which port was enabled in the previous release. An upgrade uses the user specified web ports of 10443 and 10080; you must explicitly enter these port numbers.

**Note**

All browsers require that you enable cookies, JavaScript/scripting, Adobe Flash Player 9, and popup windows. If you reinstall a later ANM release, make sure that you delete the cookies and clear the browser cache.

For example, enter **https://192.168.10.10**. The login window appears.

The username is “admin” by default and the password is the one that you provided during the installation.

**Note**

The ANM 5.2 client supports use with Firefox 3.6 on Windows XP, Windows Vista, or Windows 7. When you use Firefox 3.x to log in and access ANM for the first time, the Firefox web browser displays a warning that the site is untrusted. When Firefox displays this warning, follow the prompts to add a security exception and download the self-signed certificate from the ANM server. After you complete this procedure, Firefox accepts the ANM server as a trusted site both now and during all future login attempts. See the [“Using the Firefox Web Browser to Access ANM 5.2”](#) section on page 4-5 for details.

**Step 2** In the User Name field, enter **admin**.

The admin account was created when ANM was installed. After you log in, you can create additional user accounts. For more information about setting up user accounts, see the [User Guide for the Cisco Application Networking Manager 5.2](#).

**Step 3** In the Password field, enter the password that you used for installing ANM.

**Step 4** Click **Login**.

**Caution**

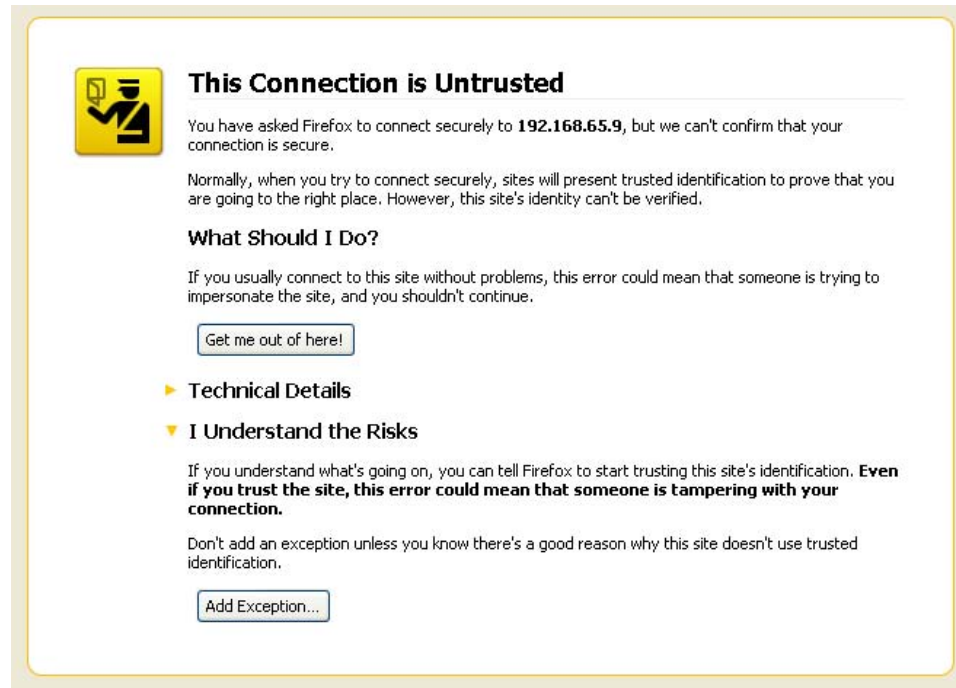
ANM installation takes 90 seconds for initialization to be completed. When the login window appears, make sure that you wait at least 90 seconds before you log in. Failure to wait a minimum of 90 seconds may result in an error.

When you log in, the default page that appears is the ANM Homepage. You can choose the default page that you access after logging in to ANM. By default, the ANM Homepage is the first page that appears after you log in. From the ANM Homepage, you can specify a different page that appears as the default page after you log in. See the [User Guide for the Cisco Application Networking Manager 5.2](#) for details, including how to use ANM to import and manage your network devices.

## Using the Firefox Web Browser to Access ANM 5.2

The ANM 5.2 client supports use with Firefox 3.6 on Windows XP, Windows Vista, or Windows 7. When you use Firefox 3.6 or later releases to log in and access ANM for the first time, the Firefox web browser displays a warning that the site is untrusted (see [Figure 4-1](#)).

**Figure 4-1** Firefox 3.6 Untrusted Connection Warning



When Firefox displays this warning, follow the prompts to add a security exception and download the self-signed certificate from the ANM server. After you complete this procedure, Firefox accepts the ANM server as a trusted site both now and during all future login attempts.

### Procedure

- 
- Step 1** In the This Connection Is Untrusted window, click **I Understand the Risks**.
- Step 2** Click **Add Exception** to add a security exception to the Firefox web browser.  
The Add Security Exception popup window appears identifying the location of the ANM server.
- Step 3** In the Add Security Exception popup window, click **Get Certificate**.  
Firefox retrieves the ANM self-signed certificate and the window's Confirm Security Exception button becomes active.
- Step 4** Click **Confirm Security Exception**.  
Firefox recognizes the ANM server as a trusted site and the ANM Login window appears.
-

# Managing Cisco Application Networking Manager Licenses

Table 4-1 describes the available ANM licenses, which are available at no charge.

**Table 4-1 ANM Licence Descriptions**

| License Name     | Description                                                                                                                                              |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| ANM-DEMO or DEMO | Used for demonstration purposes. It lasts for 90 days from the issue day of the license and allows you to use all features.                              |
| ANM-SERVER-50-K9 | Used to allow access to the ANM server. Beginning with ANM 4.1, ANM does not perform a license version number check; it accepts any version ANM license. |

## Guidelines and Restrictions

You must install a license before the end of the 90-day evaluation period to continue using ANM. To install the license during the evaluation period, you can use either of the following methods:

- Use the ANM license manager (see the “[Using ANM License Manager to Manage ANM Server or Demo Licenses](#)” section in the *User Guide for the Cisco Application Networking Manager 5.2* or in the online help).
- Use the CLI (see the “[Acquiring and Uploading a Cisco Application Networking Manager License](#)” section on page 4-1).

To install a license after the evaluation period has expired, you must use the CLI.

For more information about the evaluation period, see the “[ANM Software Licensing Requirements](#)” section on page 1-5.

## Changing Configuration Attributes After Installing Cisco Application Networking Manager

You can modify the ANM server software configuration attributes that you specified when installing the software. The configuration attributes include the following:

- HTTP Port of Web Services
- HTTP operating state (enable/disable) for Web Services
- HTTPS Port of Web Services
- HTTPS operating state (enable/disable) for Web Services
- Idle session timeout in msec

For details about modifying the software configuration, see the “[Changing ANM Configuration Property Values](#)” section in the *User Guide for the Cisco Application Networking Manager 5.2* or the ANM online help. This section also contains configuration examples.

## Example ANM Standalone Configuration Session

The following is an example of a configuration session for an ANM standalone system. The values shown in the brackets are the currently configured values.

```
/opt/CSCOanm/bin/anm-tool configure
Configuring ANM

Checking ANM configuration files
 Keep existing ANM configuration? [y/n]: n
 Creating config file (/opt/CSCOanm/etc/cs-config.properties)

Enable HTTP for Web Server [true]:
Inbound Port for HTTP traffic to ANM Default [80]:
Enable HTTPS for Web Server [true]:
Inbound Port for HTTPS traffic to ANM Default [443]:

These are the values:
Enable HTTP for Web Server: true
Inbound Port for HTTP traffic to ANM Default: 80
Enable HTTPS for Web Server: true
Inbound Port for HTTPS traffic to ANM Default: 443

Commit these values? [y/n/q]: y
Committing values ... done
 Keeping existing configuration: /opt/CSCOanm/lib/java/thirdparty/ctm_config.txt

Stopping services
 Stopping monit services (/etc/monit.conf) ... (0)
 Stopping monit ... Stopped
 Stopping heartbeat ... Stopped

Installing system configuration files
 Backing up //opt/CSCOanm/etc/my-local.cnf

Setting service attributes
 Enabling mysql for SELinux
setsebool: SELinux is disabled.
 Service monit is started by OS at boot time

Starting mysql ... Started
mysql status ... Ready

Configuring mysql
 Checking mysql user/password
 Setting mysql privileges
 Disabling mysql replication

Starting services
 Starting monit ...Starting monit daemon with http interface at [*:2812]
 Started
```

## Example ANM HA Configuration Session

The following is an example of a configuration session for an ANM HA system. Standalone systems will not contain any HA properties but will include a limited property value configuration. The values shown in the brackets are the currently configured values.

```

/opt/CSCOanm/bin/anm-tool configure
Configuring ANM

Checking ANM configuration files
Keep existing ANM configuration? [y/n]: n
Creating config file (/opt/CSCOanm/etc/cs-config.properties)

Enable HTTP for Web Server [false]: true
Inbound Port for HTTP traffic to ANM Default [80]: 80
Enable HTTPS for Web Server [true]:
Inbound Port for HTTPS traffic to ANM Default [443]:
Database Password [nI4ewPbmV51S]: passme
HA Node 1 UName []: anm49.cisco.com
HA Node 2 UName []: anm50.cisco.com
HA Node 1 Primary IP [0.0.0.0]: 10.77.240.126
HA Node 2 Primary IP [0.0.0.0]: 10.77.240.100
HA Node 1 HeartBeat IP [0.0.0.0]: 10.10.10.1
HA Node 2 HeartBeat IP [0.0.0.0]: 10.10.10.2
HA Virtual IP [0.0.0.0]: 10.77.240.101
HA Node ID [1 or 2] []: 1

These are the values:
Enable HTTP for Web Server: true
Inbound Port for HTTP traffic to ANM Default: 80
Enable HTTPS for Web Server: true
Inbound Port for HTTPS traffic to ANM Default: 443
Database Password: passme
HA Node 1 UName: anm49.cisco.com
HA Node 2 UName: anm50.cisco.com
HA Node 1 Primary IP: 10.77.240.126
HA Node 2 Primary IP: 10.77.240.100
HA Node 1 HeartBeat IP: 10.10.10.1
HA Node 2 HeartBeat IP: 10.10.10.2
HA Virtual IP: 10.77.240.101
HA Node ID [1 or 2]: 1

Commit these values? [y/n/q]: y
Committing values ... done
Keeping existing configuration: /opt/CSCOanm/lib/java/thirdparty/ctm_config.txt

Stopping services
Stopping monit services (/etc/monit.conf) ... (0)
Stopping monit ... Stopped
Stopping heartbeat ... Stopped

Installing system configuration files

Setting service attributes
Enabling mysql for SELinux
Service monit is started by OS at boot time

Starting mysql ... Started

Configuring mysql
Checking mysql user/password

```

```

Setting mysql privileges
Enabling mysql replication
Setting up database
executing /opt/CSCOanm/lib/install/etc/dcmdb.sql ... done

Starting services
Starting monit ... Started

```

## Example ANM Advanced Options Configuration Session

The following is an example of a configuration session for an ANM advanced options. The values shown in the brackets are the currently configured values.

```

/opt/CSCOanm/bin/anm-tool --advanced-options=1 configure
Configuring ANM
Checking ANM configuration files
 Keep existing ANM configuration? [y/n]: n
 Creating config file (/opt/CSCOanm/etc/cs-config.properties)

Enable HTTP for Web Server [false]:
Inbound Port for HTTP traffic to ANM Default [80]:
Enable HTTPS for Web Server [true]:
Inbound Port for HTTPS traffic to ANM Default [443]:
HTTP Port of Web Services [8080]:
Enable HTTP for Web Services [false]:
HTTPS Port of Web Services [8443]:
Enable HTTPS for Web Services [false]:
Idle session timeout in msec [1800000]:
Change the memory available to ANM process [low|high] [low]:

These are the values:
Enable HTTP for Web Server: false
Inbound Port for HTTP traffic to ANM Default: 80
Enable HTTPS for Web Server: true
Inbound Port for HTTPS traffic to ANM Default: 443
HTTP Port of Web Services: 8080
Enable HTTP for Web Services: false
HTTPS Port of Web Services: 8443
Enable HTTPS for Web Services: false
Idle session timeout in msec: 1800000

Change the memory available to ANM process [low|high]: low
Commit these values? [y/n/q]: y
Committing values ... done
 Keeping existing configuration: /opt/CSCOanm/lib/java/thirdparty/ctm_config.txt
Stopping services
 Stopping monit services (/etc/monit.conf) ... (0)

```

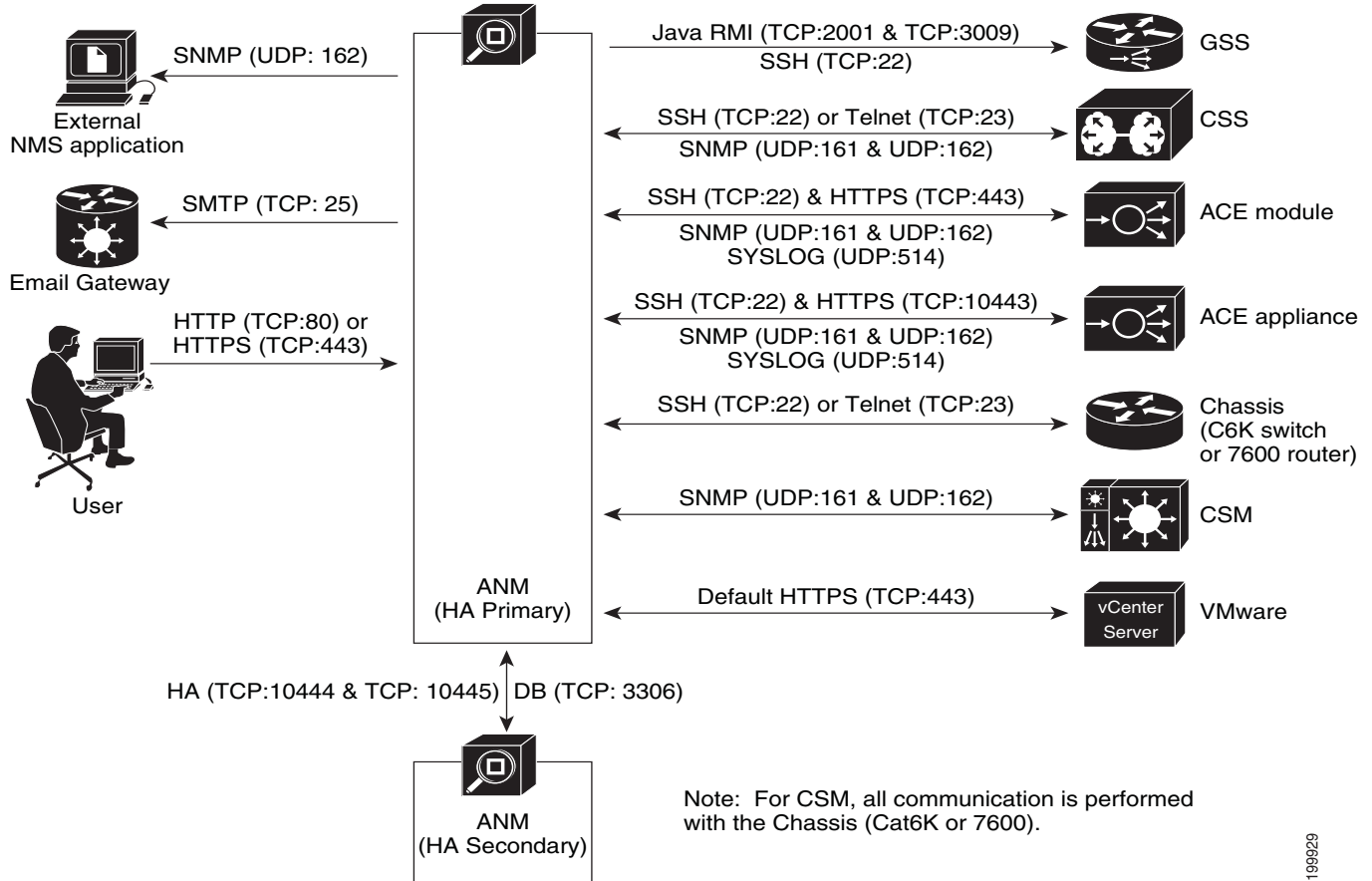
## ANM Ports Reference

ANM uses specific ports for its processes. [Figure 4-2](#) illustrates a typical ANM server deployment in a network. This illustration identifies the protocols and ports used by the different network devices in a typical deployment.

- [Table 4-2](#) lists the ports used for ANM client (browser) or ANM server and ANM high availability communication.

- Table 4-3 lists the ports used for communication between ANM and managed devices.

Figure 4-2 ANM Server Deployment



199929



**Table 4-2** Ports Used by ANM in a Network Deployment<sup>1</sup>

| Port                        | Description                                                                                       |
|-----------------------------|---------------------------------------------------------------------------------------------------|
| TCP (80)                    | Default port if ANM is configured for access using HTTP (using anm-installer).                    |
| TCP (443)                   | Default port if ANM is configured for access using HTTPS (using default install option).          |
| TCP (3306)                  | MySQL Database system (ANM HA installation opens this port to communicate with the peer ANM).     |
| TCP (10444) and TCP (10445) | ANM License Manager (ANM HA installation opens these two ports to communicate with the peer ANM). |
| TCP (25)                    | Port used by ANM server to communicate to Email Gateway through SMTP.                             |
| UDP (162)                   | Port used by ANM server to send out trap notification to external NMS application.                |
| HTTPS (8443) or HTTP (8083) | The web service ports used by ANM Web Service North-Bound API.                                    |

1. We highly recommend that you run ANM on a stand-alone device. However, if you run ANM on a shared device, note that ANM locally opens the following ports for internal communication:

TCP Ports: 8980, 10003, 10004, 10023, 10443, 40000, 40001, 40002, 40003  
 UDP Ports: 6120, 10003

**Table 4-3** Ports Used by ANM for Communication with Managed Devices

| Device Type                                                       | Port                            | Description                                                                                                                            |
|-------------------------------------------------------------------|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Chassis (Catalyst 6500 Series switch or Cisco 7600 Series router) | SSH (TCP:22) or Telnet (TCP:23) | Discover chassis configuration.                                                                                                        |
| ACE (appliance or module)                                         | HTTPS (TCP:443)                 | For ACE module: XML/HTTPS interface on the device used to discover, configure, and monitor using specific <b>show</b> CLI commands.    |
|                                                                   | HTTPS (TCP:10443)               | For ACE appliance: XML/HTTPS interface on the device used to discover, configure, and monitor using specific <b>show</b> CLI commands. |
|                                                                   | SSH (TCP: 22)                   | Discovery and configuration of ACE licenses, certificates/keys (crypto) licensing, scripts, and checkpoints.                           |
|                                                                   | SNMP (UDP: 161 & UDP:162)       | Monitor ACE through SNMP requests (UDP: 161) and receive trap notifications (UDP: 162).                                                |
| CSM                                                               | SNMP (UDP: 161 & UDP:162)       | Monitor CSM through SNMP requests (UDP: 161) and receive trap notifications (UDP: 162).                                                |

**Table 4-3** Ports Used by ANM for Communication with Managed Devices (continued)

| Device Type           | Port                            | Description                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSS                   | SSH (TCP:22) or Telnet (TCP:23) | Discover chassis configuration.                                                                                                                                                                                                                                                                                                                                |
|                       | SNMP (UDP: 161 & UDP:162)       | Monitor CSS through SNMP requests (UDP: 161) and receive trap notifications (UDP: 162)                                                                                                                                                                                                                                                                         |
| GSS                   | SSH (TCP:22)                    | Discover chassis configuration and monitoring operational status of DNS rules and VIP answers.                                                                                                                                                                                                                                                                 |
|                       | RMI (TCP:2001 & TCP:3009)       | Activate/suspend DNS rules and VIP answers.                                                                                                                                                                                                                                                                                                                    |
| VMware vCenter Server | HTTPS (TCP:443)                 | ANM communicates with the vCenter Server and vSphere Client using HTTPS and default port 443, if you are using the plug-in that is available to integrate ANM with a VMware virtual data center environment.<br><br><b>Note</b> For more information about using ANM with VMware, see the <i>User Guide for the Cisco Application Networking Manager 5.2</i> . |



# CHAPTER 5

## Troubleshooting Problems with Application Networking Manager Installation

---

**Date:** 9/18/12

This chapter describes how to troubleshoot problems with Cisco Application Networking Manager (ANM) and includes the following sections:

- [Difficulties with Product Installation, page 5-1](#)
- [Login Problems After Installation, page 5-2](#)
- [Starting Cisco Application Networking Manager, page 5-5](#)
- [Stopping Cisco Application Networking Manager, page 5-7](#)
- [Checking Why ANM Does Not Start, page 5-7](#)
- [Changing the Web Idle Session Timeout, page 5-8](#)
- [Reconfiguring After HA Installation, page 5-8](#)
- [Backing Up and Restoring Data in Standalone Mode, page 5-9](#)
- [Backing Up and Restoring Data in HA Mode, page 5-11](#)

### Difficulties with Product Installation

Installation difficulties can result from ANM back-end installation interactions with preexisting Linux Red Hat Package Manager components (RPMs). RPM libtool is a well-known example as shown in the following error message:

```
Installing libcurl7112-7.11.2-8.cf.rhel4.i386.rpm, heartbeat-2.0.2-1.i386.rpm,
libtool-libs-1.5.6-4.EL4.1.i386.rpm, heartbeat-pils-2.0.2-1.i386.rpm,
net-snmp-libs-5.1.2-11.EL4.6.i386.rpm, heartbeat-stonith-2.0.2-1.i386.rpm
```

```
error: Failed dependencies:
```

```
libtool-libs = 1.5.6-4.EL4.1.c4.4 is needed by (installed)
libtool-1.5.6-4.EL4.1.c4.4.i386
```

```
Error: rpm install failed (1536)
```

```
Done
```

Finished

To work around this problem, enter the `rpm -e RPM1 RPM2` command where *RPM1*, *2*, and so on to denote the name of each RPM that you want removed. Once you have verified that all unwanted RPMs are removed, retry the installation.

## Login Problems After Installation

If you experience problems logging in to ANM after installing the product, there may be several reasons:

- After installation, you attempt to log in and receive an error message that there is no ANM server license installed on the machine. See the [“Acquiring and Uploading a Cisco Application Networking Manager License” section on page 4-1](#) for more information on using your PAK to get a license file.
- ANM can take some time to fully initialize. As a worst (but unlikely) case, you might need to wait up to 5 minutes for initialization to complete. Choose the case that most likely resembles the problem you are having:
  - If, after waiting, you cannot log into the ANM login window, you might need to restart ANM. See the [“Restarting ANM” section on page 5-3](#).
  - If the login window will not display, you can collect installation data by running the standalone Lifeline package. You can then send that package to your technical support representative. See the [“Checking Why ANM Does Not Start” section on page 5-7](#).
  - If you have lost or cannot remember your password, you can reset the ANM admin password by following the steps in the [“Resetting the ANM Admin Password” section on page 5-2](#).

## Resetting the ANM Admin Password

This section describes how to reset the ANM admin password and includes these topics:

- [Resetting the ANM admin Password in Standalone Mode, page 5-2](#)
- [Resetting the ANM admin Password in HA Mode, page 5-3](#)



**Note** Resetting the ANM admin password also resets the default organization authentication type to use local ANM authentication. For more information and a detailed procedure, see the [“Administering the Cisco Application Networking Manager” chapter in the \*User Guide for the Cisco Application Networking Manager 5.2\*](#).

### Resetting the ANM admin Password in Standalone Mode

You can reset the admin password in standalone mode.

#### Procedure

- 
- Step 1** From the Linux command line, log in as the root user on the ANM host, as described in the [“Becoming the Root User” section on page 1-5](#).
  - Step 2** Change your directory to `/opt/CSCOanm/etc` from the command line by entering `cd /opt/CSCOanm/etc`.

**Step 3** To reset the password, from the command line, enter the following command:

```
echo admin-password > .resetPassword
```

where *admin-password* is your new admin password.



---

**Note** Make sure that you insert a period before `resetPassword` as shown in [Step 3](#).

---

**Step 4** Restart ANM. For more information, see the “[Restarting ANM](#)” section on page 5-3.

**Step 5** After ANM displays the login window, log in using the admin user and whatever password you specified in [Step 3](#).

---

## Resetting the ANM admin Password in HA Mode

You can reset the admin password in HA mode. You cannot log in to ANM and perform a failover from the Admin page on the user interface. You must be on the standby host and want it to become the active host.

### Procedure

---

**Step 1** Log in as the root user on the ANM standby host, as described in the “[Becoming the Root User](#)” section on page 1-5.

**Step 2** To change your directory to `/opt/CSCOanm/etc`, from the command line, enter the following command:  

```
cd /opt/CSCOanm/etc
```

**Step 3** To reset the password, from the command line, enter the following command:

```
echo admin-password > .resetPassword
```

where *admin-password* is the new admin password.



---

**Note** Be sure to insert a period before `resetPassword` as shown in [Step 3](#).

---

**Step 4** To switch your HA hosts, from the command line enter the following command:

```
/opt/CSCOanm/bin/anm-ha active
```

**Step 5** Restart ANM. For more information, see the “[Restarting ANM](#)” section on page 5-3.

**Step 6** After ANM displays the login window, log in using the admin user and whatever password you specified in [Step 3](#).

---

## Restarting ANM

You can restart ANM.

### Procedure

---

**Step 1** From the Linux command line, change to the **root** by entering the `% su -` command.

- Step 2** To restart ANM, from the command line, enter the `/opt/CSCOanm/bin/anm-tool restart-services` command.
- Step 3** To check the ANM process status, from the command line, enter the `/opt/CSCOanm/bin/anm-tool info-services` command.
- Step 4** Check that the status that appears next to the following list for the six processes all display as running or changed:
- `anm`—Data Center Manager, which holds the GUI back-end, remote managed objects (RMO), and logging services. Note the following operating requirements for the ANM process:
    - The ANM process reads and manipulates the `/var/log/messages*` files in the `adm` group.
    - The ANM process listens to specific reserved ports (less than port 1023) using port forwarding in the iptables as follows:
      - `http(80)`—Listens at 8980
      - `https(443)` —Listens at 10443
      - `snmptrap(162)` —Listens to 6120
 See the “ANM Ports Reference” section on page 4-9 for details on how ANM uses specific ports for its processes.
  - `ip-disc`—IP Discovery, which handles IP address discovery.
  - `dal`—Device Access Layer, which handles communication and generates CLI commands to the network element.
  - `licman`—License Manager, which handles network element and server licensing.
  - `anm-fw-mon`—Firewall Monitor, which handles the firewall status and port forwarding at the firewall level.
  - `MySQL`— ANM database process, which manages the configuration and event management databases.




---

**Note** In HA mode, the processes `anm`, `dal`, and `ip-disc` are not running on the standby node.

---




---

**Note** You might need to repeat [Step 3](#) and [Step 4](#) a few times while the processes go from initializing to running or changed. It can take up to 5 minutes to complete the initialization.

---

- Step 5** Log into ANM after all five processes have a status of running or changed.
- If all five processes do not eventually have a status of running or changed, or if it is still not possible to log in even though the processes have the desired status, try reinstalling ANM.
- To reinstall ANM, follow the procedure in the “[Information About Installing the ANM Server Software](#)” section on page 2-1.
- If you still cannot log in to ANM, contact the Technical Assistance Center. Before doing so, you need the following information:
- `/var/log/messages` log file.
  - Lifeline file, which is created by entering the `/opt/CSCOanm/bin/anm-sysinfo -a` command as root, and is found at `/tmp/anm-lifeline.tar.gz`.

- Log of the install session. See the [“Obtaining the Install Session Log”](#) section on page 5-5 for the procedure.

## Obtaining the Install Session Log

To obtain the install session log, copy the `/var/lib/anm/console/anm-install.txt` file and forward it to your Cisco technical support representative.

This file is created during the installation and contains useful information.



### Note

In the unlikely event that you cannot find the `anm-install.txt` in the `/var/lib/anm` directory, then you can find it in the `/tmp` directory with the name `anm-install.txt.xxxx` where `xxxx` represents a 4-digit number.

## Obtaining the Upgrade Session Log

To obtain the upgrade session log, copy the `/var/lib/anm/console/anm-upgrade.txt` file and forward it to your Cisco Technical Support team.

This file is created during the upgrade and contains useful information.



### Note

In the unlikely event that you cannot find the `anm-install.txt` in the `/var/lib/anm` directory, then you can find it in the `/tmp` directory with the name `anm-install.txt.xxxx` where `xxxx` represents a 4-digit number.

# Starting Cisco Application Networking Manager

You can start ANM after it has been stopped (see the [“Stopping Cisco Application Networking Manager”](#) section on page 5-7).

### Procedure

- Step 1** From the Linux command line, log in as the root user as described in the [“Becoming the Root User”](#) section on page 1-5. You are presented with a prompt.
- Step 2** To start ANM, enter the following command:
- ```
/opt/CSCOanm/bin/anm-tool start-services
```
- Step 3** (Optional) After ANM has started, you can check the status of ANM processes by entering the following command:

```
/opt/CSCOanm/bin/anm-tool info-services
```

The following example illustrates the status of the processes for a standalone ANM:

```
/opt/CSCOanm/bin/anm-tool info-services  
The monit daemon 4.8.1 uptime: 0m
```

```
Process 'dcm'                running  
Process 'dal'                running  
Process 'ip-disc'           running
```

```

Process 'licman'                running
Process 'anm-fw-mon'           running
Process 'mysql'                running
System 'rjeyacha-lnx'         running

```

Java Processes:

```

licman      : Running (8721) [2009-11-17 23:21:06]
dcm         : Running (8734) [2009-11-17 23:21:06]
dal        : Running (8723) [2009-11-17 23:21:06]
ip-disc    : Running (8732) [2009-11-17 23:21:06]

```

Other Processes:

```

anm-fw-mon: Running (8738) [2009-11-17 23:21:06]
mysql     : Running (8605) [2009-11-17 23:20:58]

```

The following example illustrates the status of the processes for an active node in ANM HA mode:

```

/opt/CSCOanm/bin/anm-tool info-services
The monit daemon 4.9 uptime: 13h 14m

```

```

Process 'heartbeat'            running
Process 'dcm'                  running
Process 'dal'                   running
Process 'ip-disc'              running
Process 'licman'               running
Process 'anm-fw-mon'           running
Process 'mysql'                running
System 'anm50.cisco.com'       running

```

Java Processes:

```

licman      : Running (11874) [2010-08-30 23:52:36]
dcm         : Running (21307) [2010-08-31 05:44:13]
dal        : Running (21314) [2010-08-31 05:44:13]
ip-disc    : Running (21145) [2010-08-31 05:44:09]

```

Other Processes:

```

anm-fw-mon: Running (11858) [2010-08-30 23:52:36]
mysql     : Running (28565) [2010-08-31 11:06:13]

```

Process on the standby server.

The following example illustrates the status of the processes for a standby node in ANM HA mode:

```

/opt/CSCOanm/bin/anm-tool info-services
The monit daemon 4.8.1 uptime: 21h 16m

```

```

Process 'dcm'                  running
Process 'dal'                   running
Process 'ip-disc'              running
Process 'licman'               running
Process 'anm-fw-mon'           running
Process 'mysql'                running
System 'rjeyacha-lnx'         running

```

Java Processes:

```

licman      : Running (21345) [2009-11-19 00:18:24]
dcm         : Running (21380) [2009-11-19 00:18:24]
dal        : Running (21364) [2009-11-19 00:18:24]
ip-disc    : Running (21347) [2009-11-19 00:18:24]

```



```
Other Processes:
anm-fw-mon: Running (21367) [2009-11-19 00:18:24]
mysql      : Running (21456) [2009-11-19 00:18:26]
```

Stopping Cisco Application Networking Manager

You can stop ANM.

Procedure

-
- Step 1** From the Linux command line, log in as the root user as described in the [“Becoming the Root User”](#) section on page 1-5.
- Step 2** Enter the `/opt/CSCOanm/bin/anm-tool stop-services` command at the prompt to stop ANM.
-

Checking Why ANM Does Not Start

If ANM does not start after an installation or upgrade, use the standalone Lifeline package to collect data to forward to your support team.

Make sure that you have an ANM server license installed on your machine. See the [“Acquiring and Uploading a Cisco Application Networking Manager License”](#) section on page 4-1 for more information on using your PAK to get a license file.

Procedure

-
- Step 1** From the Linux command line, log in as the root user as follows:



Caution

As the root user, you can adversely affect your operating environment if you are unaware of the effects of the commands that you use. If you are an inexperienced Linux user, you should limit your activities as the root user to the tasks described in this procedure.

- If you are not logged in, log in as the root user by entering the following:

```
>login: root
```

```
>Password: root-password
```

- If you are already logged in, but not as the root user, use the `su -` command to change your login to root by entering the following:

```
# su -
```

```
# Password: root-password
```

- Step 2** If this is an ANM HA system, enter the `/opt/CSCOanm/bin/anm-ha check` command on both hosts to check for common configuration errors.

An example of output that finds no errors is as follows:

```

# /opt/CSCOanm/bin/anm-ha check
ANM config: local = (1 rh23.cisco.com 192.168.65.23 12.12.12.2)
ANM config: peer = (2 rh25.cisco.com 192.168.65.25 12.12.12.1)
ANM config: VIP = 192.168.65.88
Info: Interface: eth0 192.168.65.23/255.255.255.128
Info: Interface: eth1 12.12.12.2/255.255.255.0

Verifying ...

Detected 0 warning(s)
Detected 0 error(s)
ANM configuration seems reasonable
Done.

```

Although this command may not find a problem, it is not a comprehensive check and errors may still exist. If after entering the command an error is detected, you need to fix the problem. Also, if the output of this command includes a warning, you need to determine whether the warning is explainable and can be fixed. For example, the reason you cannot perform a **ping** command on the peer host may be because the peer host is down.

- Step 3** Collect critical data that can be forwarded to your support representative by entering the `/opt/CSCOanm/bin/anm-sysinfo -a` command.
- This command creates the `/tmp/anm-lifeline.tar.gz` file.
- Step 4** Forward this file to your support representative.
-

Changing the Web Idle Session Timeout

To change the web idle session timeout settings, see the [“Changing Configuration Attributes After Installing Cisco Application Networking Manager”](#) section on page 4-6 and the [“Example ANM Advanced Options Configuration Session”](#) section on page 4-9.

Reconfiguring After HA Installation

If you receive errors when attempting to change the HA properties configuration values after installing ANM, check the node ID to be sure the active and standby values are not reversed.

Backing Up and Restoring Data in Standalone Mode

You can back up a standalone ANM server configuration and restore it if necessary.



Caution

During the backup and restore procedures, you must log in as the root user. As the root user, you can adversely affect your operating environment if you are unaware of the effects of the commands that you use. If you are an inexperienced Linux user, you should limit your activities as the root user to the tasks described in the procedures.

Guidelines and Restrictions

If you restore the ANM database from a backup repository and a virtual context that is in the repository has been removed from the network element, ANM removes that context from the database and the context does not appear in the ANM user interface.

This section includes the following topics:

- [Backing Up Data in Standalone Mode, page 5-9](#)
- [Restoring Data in Standalone Mode, page 5-10](#)

Backing Up Data in Standalone Mode

You can back up your standalone ANM server data.

Prerequisites

MySQL must be running to perform the backup.

Procedure

-
- Step 1** From the Linux command line, log in as the root user as follows:
- If you are not logged in, log in as the root user:

```
>login: root
```



```
>Password: root-password
```
 - If you are already logged in, but not as the root user, use the **su -** command to change your login to root:

```
# su -
```



```
# Password: root-password
```
- Step 2** Verify that the ANM server is running by entering the following command:

```
/opt/CSCOanm/bin/anm-tool info-services
```
- Step 3** Back up the ANM configuration by entering the following command:

```
/opt/CSCOanm/bin/anm-tool backup backup_filename
```


where *backup_filename* is the name of the ANM backup file.

- Step 4** Copy the backup file to a safe, remote (nonlocal) location, such as a different computer, a USB flash or external drive, or CD-RW disk.
-

Restoring Data in Standalone Mode

You can restore your standalone ANM server configuration data.

Guidelines and Restrictions

This topic includes the following guidelines and restrictions:

- You must restore the data on the same version of ANM server on which you performed the backup. Restoring data to a different version of the ANM server is not supported. Data backed up from a Linux running the 32-bit Server Edition can be restored on a Linux running the 64-bit Server Edition and vice versa providing both are on the same version of ANM.
- The restore procedure includes using a backup of your current ANM server configuration to restore the ANM configuration. You can also use a backup file that you created from another ANM server (operating in standalone or HA mode) or from ANM Virtual Appliance to restore the ANM configuration.

For information about creating a backup from an ANM Server, see the [“Backing Up Data in Standalone Mode” section on page 5-9](#).

For information about creating a backup from ANM Virtual Appliance that you use on an ANM server, see the [“Installing the ANM Software Upgrade” section on page 3-3](#)).



Note If you use a backup that you created from another ANM server or from ANM Virtual Appliance to restore the ANM server configuration, at the end of the upgrade process, you must install the appropriate ANM on the server because the license is tied to an ANM server’s MAC address.

Procedure

- Step 1** From the Linux command line, log in as the root user as follows:
- If you are not logged in, log in as the root user:


```
>login: root
>Password: root-password
```
 - If you are already logged in, but not as the root user, use the **su -** command to change your login to root:


```
# su -
# Password: root-password
```
- Step 2** Verify that the ANM server is running by entering the following command:
- ```
/opt/CSCOanm/bin/anm-tool info-services
```

- Step 3** If the backup file to be used to restore the ANM server resides on a remote device (such as a network server, USB flash, external drive, or CD-RW disk), copy the backup file to the ANM server.
- Step 4** Restore the data by entering the following command:
- ```
/opt/CSCOanm/bin/anm-tool restore [path/]backup_filename
```
- The command arguments are as follows:
- *path/*—(Optional) Path to the backup file. The path is not required if you copied the backup file to the bin directory where the restore script resides.
 - *backup_filename*—Name of the backup file to use to restore the ANM server configuration.
- ANM automatically restarts.
- Step 5** If the backup file used to restore the ANM server configuration was created on another ANM server or on ANM Virtual Appliance, perform the following steps:
- a. Install the appropriate license for the server. Skip this step if the backup was created from the server you just upgraded (see the “[Using ANM License Manager to Manage ANM Server or Demo Licenses](#)” section in the *User Guide for the Cisco Application Networking Manager 5.2* or in the online help).
 - b. If the port information and configuration attributes of the backup are different than the values of the original ANM server configuration, you need to modify the port information and configuration attributes to match the original ANM server configuration (see the “[Changing Configuration Attributes After Installing Cisco Application Networking Manager](#)” section on page 4-6).
 - c. If the backup was created on an ANM server configured to operate in HA mode, you must set the configuration to standalone mode by doing the following:
 1. Enter the following command:

```
/opt/CSCOanm/bin/anm-tool -ha=0 configure
```

A series of prompts appears.
 2. At the “Check existing configuration files?” prompt, enter n (no). Leave all other options at their default values unless you need to modify any of them.
 3. At the “Commit these values?” prompt, enter y (yes).

Backing Up and Restoring Data in HA Mode

You can back up an HA ANM server configuration and restore it if necessary.



Caution

During the backup and restore procedures, you must log on as the root user. As the root user, you can adversely affect your operating environment if you are unaware of the effects of the commands that you use. If you are an inexperienced Linux user, you should limit your activities as the root user to the tasks described in the procedures.

Guidelines and Restrictions

If you restore the ANM database from a backup repository and a virtual context that is in the repository has been removed from the network element, ANM removes that context from the database and the context does not appear in the ANM user interface.

This section includes the following topics:

- [Backing Up Data in HA Mode, page 5-12](#)
- [Restoring Data in HA Mode, page 5-12](#)

Backing Up Data in HA Mode

You can back up your ANM server data when you have two servers operating in HA mode.

Prerequisites

MySQL must be running to perform the backup.

Procedure

-
- Step 1** From the Linux command line of the active ANM server, log in as the root user as follows:
- If you are not logged in, log in as the root user:


```
>login: root
```

```
>Password: root-password
```
 - If you are already logged in, but not as the root user, use the **su** - command to change your login to root:


```
# su -
```

```
# Password: root-password
```
- Step 2** Verify that the ANM server is running by entering the following command:
- ```
/opt/CSCOanm/bin/anm-tool info-services
```
- Step 3** Back up the ANM configuration by entering the following command:
- ```
/opt/CSCOanm/bin/anm-tool backup backup_filename
```
- where *backup_filename* is the name of the ANM backup file.
- Step 4** Copy the backup file to a safe, remote (nonlocal) location, such as a different computer, a USB flash or external drive, or CD-RW disk.
- Step 5** Repeat Steps 1 to 4 on the standby ANM server.
-

Restoring Data in HA Mode

You can restore ANM server configuration data.

Guidelines and Restrictions

This topic includes the following guidelines and restrictions:

- You must restore the data on the same version of the ANM server on which you performed the backup. Restoring data to a different version of the ANM server is not supported. Data backed up from a Linux running the 32-bit Server Edition can be restored on a Linux running the 64-bit Server Edition and vice versa if both are on the same version of ANM.
- At the end of the restore process, you must install the ANM license that is applicable to the upgraded server. If the backup you use during the restore process belongs to a different host, you must install the appropriate license because an ANM license is tied to the MAC address of a server.

Procedure

- Step 1** From the Linux command line of the active and standby ANM servers, log in as the root user as follows:
- If you are not logged in, log in as the root user:

```
>login: root
```



```
>Password: root-password
```
 - If you are already logged in, but not as the root user, use the **su -** command to change your login to root:

```
# su -
```



```
# Password: root-password
```
- Step 2** Verify that both ANM servers are running by entering the following command on both servers:

```
/opt/CSCOanm/bin/anm-tool info-services
```
- Step 3** From the standby ANM server, stop the server by entering the following command:

```
/opt/CSCOanm/bin/anm-tool stop-services
```
- Step 4** From the active ANM server, perform the following steps:
- a. If the backup file to be used to restore the ANM server resides on a remote device (such as a network server, USB flash, external drive, or CD-RW disk), copy the backup file to the ANM server.
 - b. Restore the data on the server by entering the following command:

```
/opt/CSCOanm/bin/anm-tool restore [path/]backup_filename
```

The command arguments are as follows:

 - path*—(Optional) Path to the backup file. The path is not required if you copied the backup file to the bin directory where the restore script resides.
 - backup_filename*—Name of the backup file to use to restore the ANM server configuration.

ANM automatically restarts.
 - c. If the backup used to restore the server was made on the same server, skip to [Step 5](#). If the backup file used to restore the ANM server configuration was created on another ANM server or on ANM Virtual Appliance, then perform the following tasks:
 1. Reinstall the ANM license that was originally installed on the server (see the [“Using ANM License Manager to Manage ANM Server or Demo Licenses”](#) section in the *User Guide for the Cisco Application Networking Manager 5.2* or in the online help).

2. If the port information and configuration attributes of the backup are different than the values of the original ANM server configuration, you must modify the port information and configuration attributes to match the original ANM server configuration (see the [“Changing Configuration Attributes After Installing Cisco Application Networking Manager”](#) section on page 4-6).

- Step 5** From the standby ANM server, perform the following steps:
- a. Start the standby server by entering the following command:
`/opt/CSCOanm/bin/anm-tool start-services`
 - b. Repeat Steps 4a. to 4c.
-



APPENDIX **A**

Red Hat Operating System Installation Tips

Date: 9/18/12

This appendix describes the recommended Red Hat operating system installation procedure in three parts and includes the following sections:

- [Information About Installing Red Hat for Use with ANM, page A-1](#)
- [Red Hat Installation Procedure, page A-1](#)



Note

The screen captures included in this Appendix are from RHEL Update 2 (5.2). You may find slight variations in screen text when using the other supported versions of RHEL Linux 5 (for example, RHEL 5 Update 6). When in doubt, consult the RHEL documentation at <http://www.redhat.com/docs/> for the latest information.

Information About Installing Red Hat for Use with ANM

The procedures in this section are intended as a supplement *only* and are not meant to replace Red Hat system requirements and end-to-end installation procedures. Use the procedures in this appendix to avoid library conflicts between ANM and Red Hat Enterprise Linux 5 or 5.5 (base server) that might arise when you select certain optional software packages available with the RHEL installation. The Red Hat Enterprise Linux (RHEL) documentation can be found online at <http://www.redhat.com/docs/>.



Note

If you are installing ANM for the first time on a server where it has never been installed, you *must* install one of the supported Red Hat Enterprise Linux operating systems specified in the “[Server Requirements](#)” section on page 1-35.

Red Hat Installation Procedure

The RHEL installation procedure is divided into three parts. The entire procedure should take approximately one hour, depending on any starts and stops you might require. The installation parts are described in [Table A-1](#).

Table A-1 RHEL Installation Sequence

Task	Steps
1. Media check and server partitioning—Allows you to inspect the integrity of the physical installation media (CD-ROMs or DVDs), and to make any adjustments to the partitioning of your Linux environment before installation.	“Media Check and Server Partitioning” section on page A-2, Steps 1 through 25.
2. Operating system installation—Allows you to install the operating system and any selected libraries and software packages.	“Operating System Installation” section on page A-10, Steps 27 through 30.
3. Setup Agent guided startup—Allows you to enable, disable, or adjust firewall and other security settings.	“Setup Agent Guided Startup” section on page A-11, Steps 31 through 35.



Note We do not recommend that you skip any of these steps even if you plan to make adjustments after the installation of ANM.

Prerequisites

This topic includes the following prerequisites:

- You have all the RHEL CD-ROMs or DVDs that you purchased or onto which you copied the installation files from the Red Hat website.
- You have verified all system requirements listed in the RHEL documentation at <http://www.redhat.com/docs/> and in the “Preparing to Install Application Networking Manager” section on page 1-1.
- You are logged in to your server as root as described in the “Becoming the Root User” section on page 1-5.

The RHEL installation is one procedure, that for ease of understanding, is divided into three parts and labeled accordingly, as described in [Table A-1](#).

Media Check and Server Partitioning

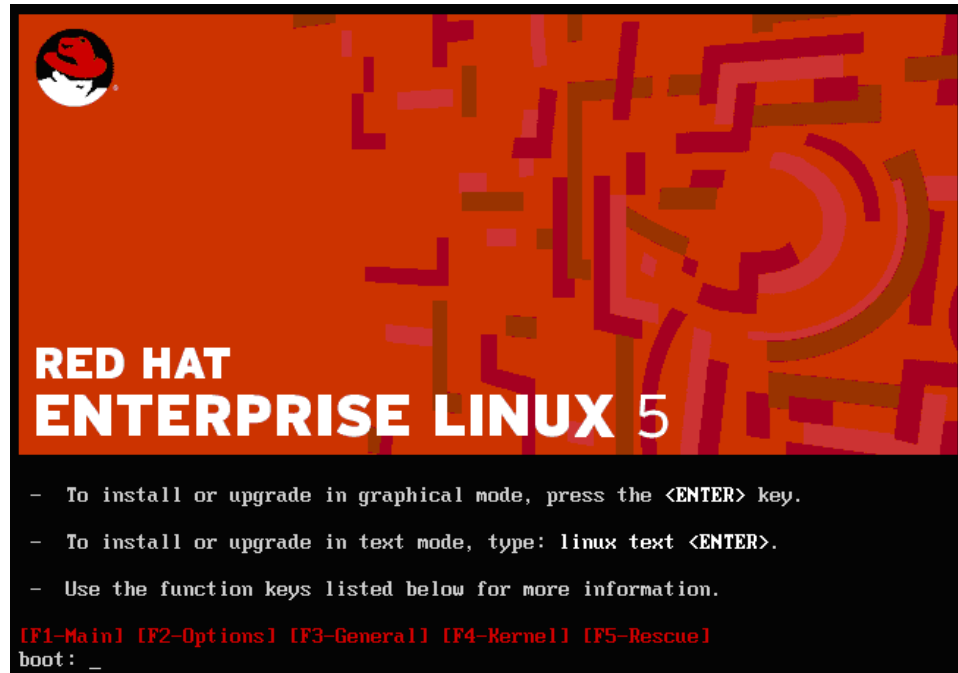
-
- Step 1** Insert the first installation CD-ROM or DVD into the server CD-ROM/DVD drive.
- Step 2** Restart the server. This should begin the installation program depending on the BIOS settings that you have set for our Linux server.



Note If the installation does not begin after you restarted the server, you may have to stop the program and readjust the BIOS settings for your Linux server. See your system administrator for assistance.

After approximately a minute, the installer window appears as shown in [Figure A-1](#).

Figure A-1 Red Hat Enterprise Linux 5 Installer Window



Step 3 From the installer window, choose the GUI (graphical mode) by pressing **Enter**.



Note If you do not choose one of the options that are shown in [Figure A-1](#), the installation defaults to graphical mode.

The CD Found window appears. You are offered the choice of testing the CD media before installation.

Step 4 In the CD Found window, do one of the following:

- Click **OK** to begin testing the media before installation (recommended), and go to [Step 5](#).
- Click **Skip** to skip the media test and start the installation (not recommended unless you are reinstalling or have already tested all installation media), and go to [Step 10](#).

Step 5 In the Media Check window, Click **Test** to test the CD-ROM or DVD in the drive.

As the check process begins, a smaller Media Check window with progress bar displays the percentage of the check completed. The check process takes approximately 3 minutes. When the check process is done, the Media Check Results window appears.

Step 6 In the Media Check window, do one of the following:

- Proceed to [Step 7](#) if the Media Check Results window displays a message indicating the CD-ROM or DVD has passed the check.
- Exit the installation and work with your system administrator to do what is needed to get new media so that you can install RHEL safely if a message appears indicating the CD-ROM or DVD did not pass the check.

Step 7 In the Media Check Results window, click **OK** to return to the Media Check window.

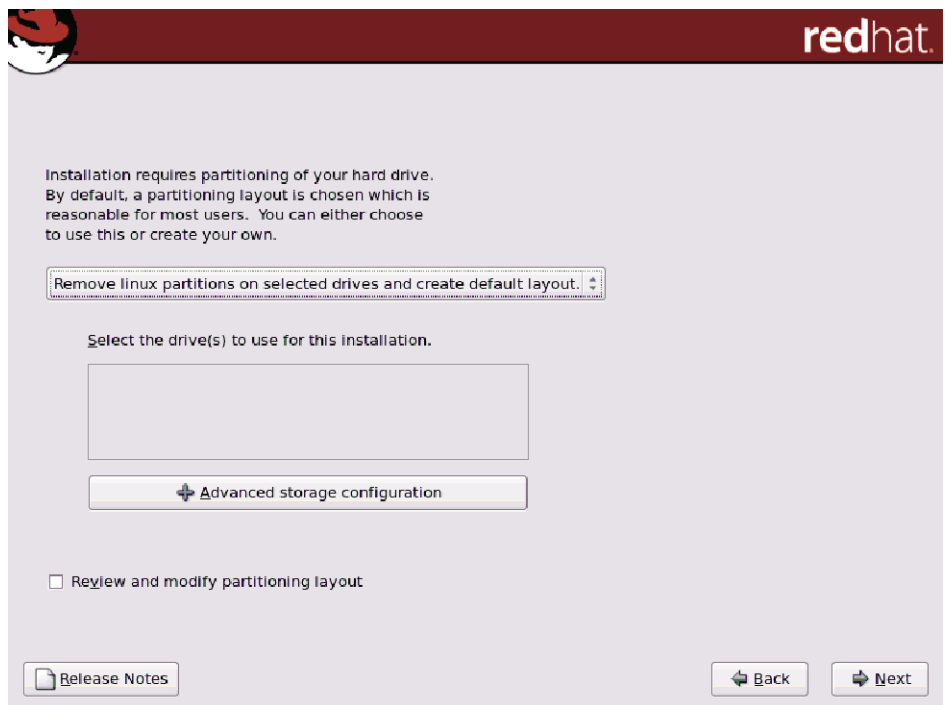
- Step 8** In the Media Check window, click **Eject CD** to eject the CD-ROM or DVD and insert another for testing. The Media Check window with a progress bar appears as described in [Step 5](#).
- Step 9** Repeat [Steps 6](#) through [8](#) until you have tested all installation media. A confirmation window appears stating that all media has been tested.
- Step 10** In the confirmation window, click **Next** to continue with preinstallation setup tasks. The language and keyboard selection windows appear.
- Step 11** Click **English** for both windows. The Installation Number window appears requesting you enter an installation number. If the version of RHEL you are installing was purchased with additional packages, you most likely received an installation number. The procedures in this appendix require that you do *not* install additional software packages or Web server. Even if you have an installation number, it is important that you do not enter it by clicking **Skip** as noted in [Step 12](#).



Note Even if you have an installation number, do not enter it when prompted. If you enter an installation number you could inadvertently install additional packages that might conflict with the software libraries that are automatically installed with ANM.

- Step 12** In the Installation Number window, click **Skip**. A warning window appears.
- Step 13** Click **OK**. A partitioning window appears as shown in [Figure A-2](#).

Figure A-2 Red Hat Enterprise Linux 5 Partitioning Window



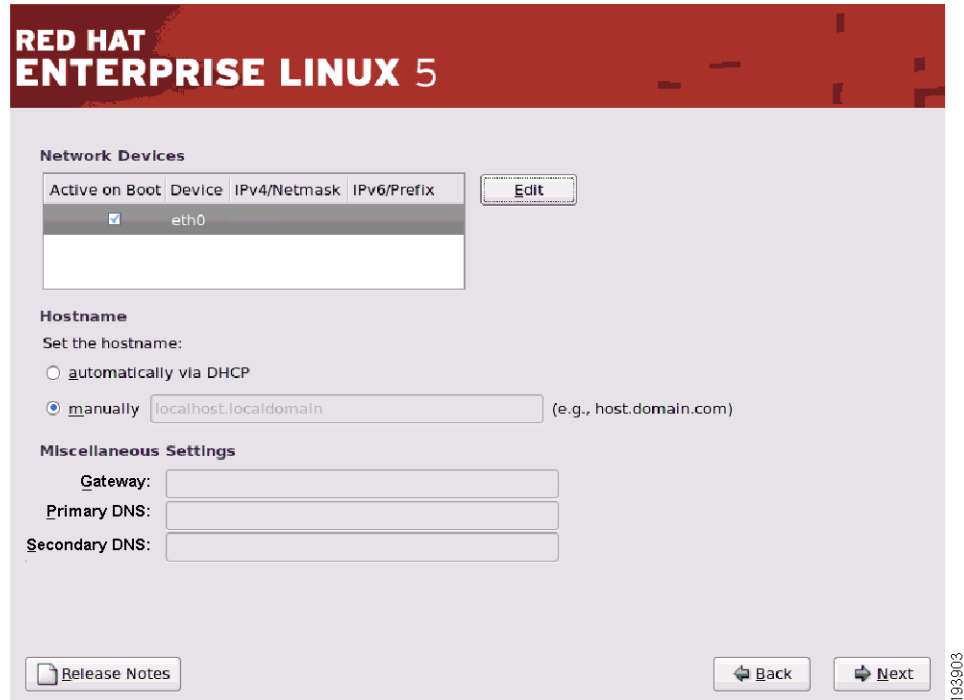
From the partitioning window, you can remove existing partitions if any or modify an existing hard drive layout to accommodate RHEL. Partitioning, which is the default, causes a reformatting of your hard drive.

Step 14 Click **Remove Linux partitions on selected drive and create default layout**. A dialog box displays “Are you sure that you want to do this?” because this action will reformat your drive and delete all previous setup partitions.

Step 15 Click **Yes**.

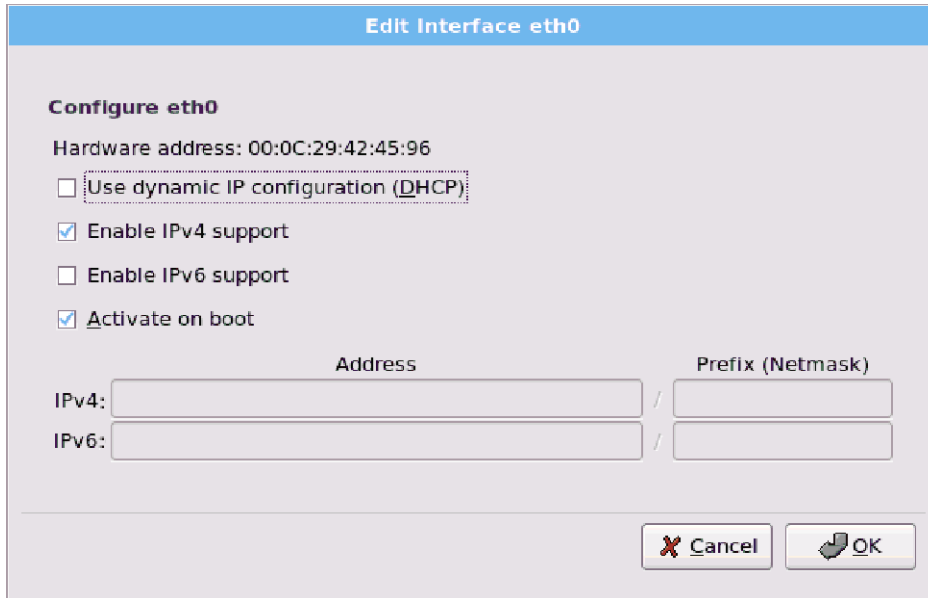
The Network Devices/Hostname/Miscellaneous Settings window appears as shown in [Figure A-3](#). The installation program automatically detects any network devices that you have and displays them in the Network Devices list.

Figure A-3 Network Devices, Hostname, and Miscellaneous Settings Window



- Step 16** In the Network Devices/Hostname/Miscellaneous Settings window, click **Edit**.
The Edit Interface eth0 window appears as shown in [Figure A-4](#).

Figure A-4 *Edit Interface eth0 Window*



- Step 17** In the Edit Interface eth0 window, check the **Enable IPv4 support** checkbox and the **Activate on boot** checkbox.



Note Make sure the Use dynamic IP configuration and Enable IPv6 support checkboxes are unchecked.

The IPv4 IP Address and Prefix (Netmask) fields in the lower portion of the window displayed in [Figure A-4](#) are no longer be grayed out.

- Step 18** In the IPv4 IP Address and Prefix (Netmask) fields, enter the IPv4 IP address and netmask.
Step 19 Click **OK**.

The Network Devices/Hostname/Miscellaneous Settings window appears.

Step 20 In the Network Devices/Hostname/Miscellaneous Settings window, check the **Manually** check box to enter the server settings for ANM, (see [Figure A-5](#)).

Figure A-5 Network Devices, Hostname, and Miscellaneous Settings Window

**RED HAT
ENTERPRISE LINUX 5**

Network Devices

Active on Boot	Device	IPv4/Netmask	IPv6/Prefix	Edit
<input checked="" type="checkbox"/>	eth0			

Hostname

Set the hostname:

automatically via DHCP

manually (e.g., host.domain.com)

Miscellaneous Settings

Gateway:

Primary DNS:

Secondary DNS:

193903

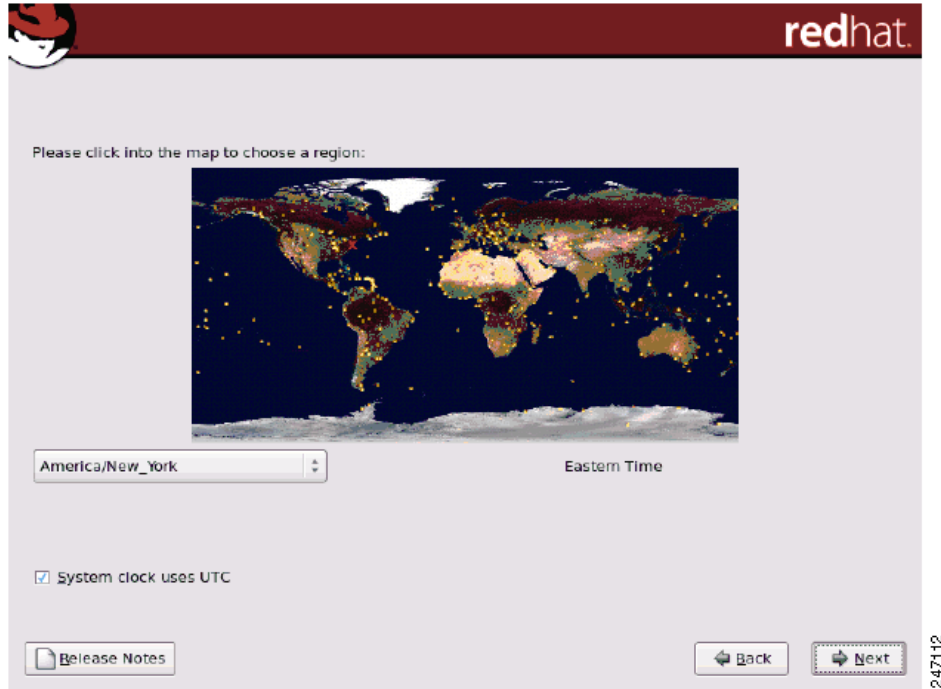
Step 21 In the Network Devices/Hostname/Miscellaneous Settings window, enter the following information in the Miscellaneous Settings fields:

- Server hostname.
- Gateway IP address.
- Primary domain name server.
- Secondary domain name server.

Step 22 Click **Next**.

A world map window appears with a UTC check box that is checked by default as shown in [Figure A-6](#).

Figure A-6 Time Zone Map with UTC Settings Checkbox

**Step 23** In the world map window, do one or both of the following:

- Click the region of the world on the map where your server is located (or the one for which you would like the time zone set).
- (Optional) Uncheck the **UTC** checkbox if you do not want timestamps to appear in Universal Coordinated Time (atomic time).

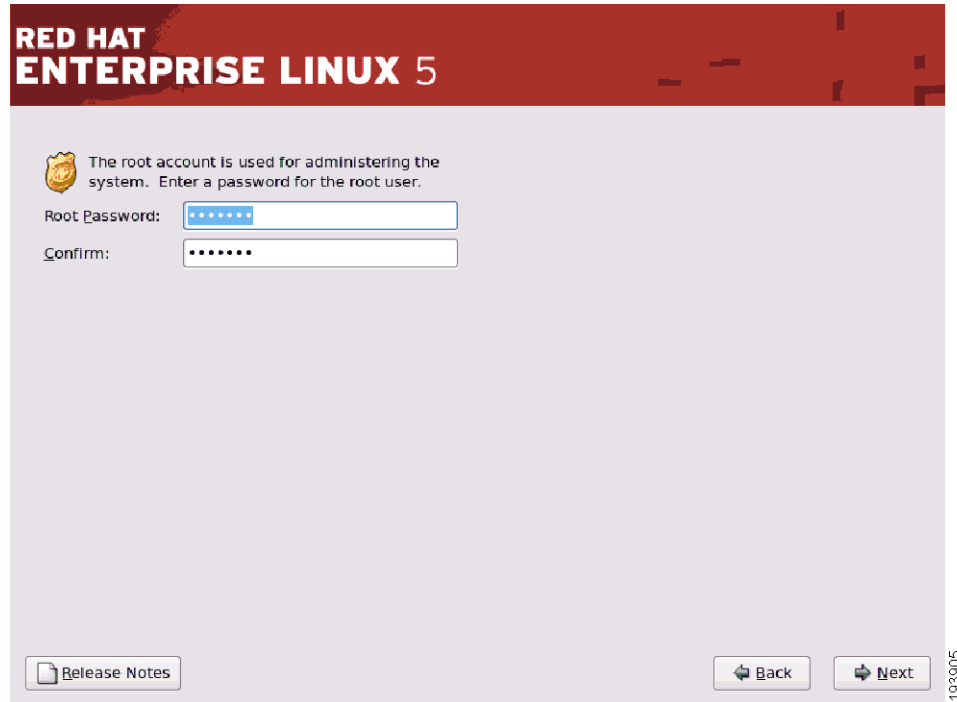


Note These choices affect the clock that ANM uses when it generates events.

Step 24 Click **Next**.

A Root Password Configuration Settings dialog box appears as shown in [Figure A-7](#).

Figure A-7 Root Password Configuration Settings Dialog Box



Step 25 In the Root Password and Confirm fields, enter and confirm your root password.

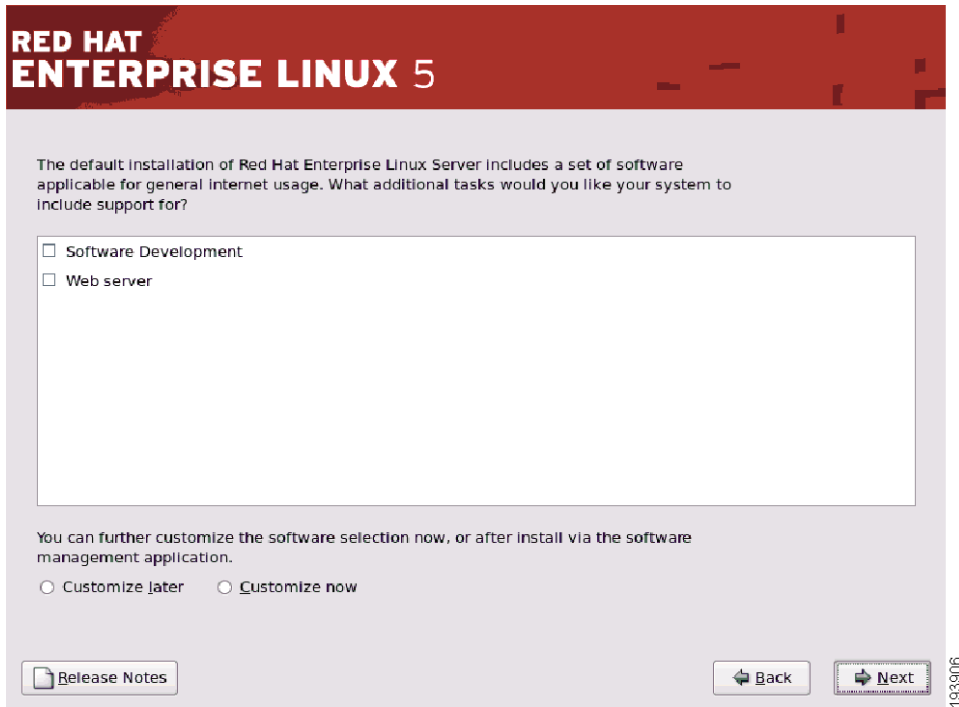
Step 26 Click **Next**.

Steps [27](#) through [30](#) guide you through the operating system installation itself.

Operating System Installation

In the Software Development Web Server Selection window, a progress bar appears indicating that the installation is being retrieved. The progress bar fills in approximately in one minute, and then a Software Development/Web server selection window appears as shown in [Figure A-8](#).

Figure A-8 Software Development Web Server Selection Window



In the Software Development Web Server Selection window, you will see two checkboxes; Software Development, and Web server. Do not check either checkbox.



Note It is essential for the proper functioning of ANM that you do not install *any* Software Development (optional packages or SDK) or Web server.

Step 27 Click **Next**.

A window with a progress bar appears indicating that dependencies and packages selected for installation will be installed (even though you did not select any optional packages).

Step 28 Click **Next** to begin the installation.

The following message displays: “Click next to begin installation of Red Hat Enterprise Linux Server. A complete log of the installation can be found in the file ‘/root/install.log’ after rebooting your system. A kickstart file containing the installation options selected can be found in the file ‘/root/anaconda-ks.cfg’ after rebooting the system.”

Step 29 In the Software Development Web Server Selection window, click **Next**.
A window that lists the number of CD-ROMs needed for installation appears.



Note This step is your last chance to return to earlier screens and change your selections, return to the beginning of the installation program, or perform a media check by choosing **Back**. If you want to continue with the installation, proceed to Step 30. If you want to discontinue the installation, click **Back**.

Step 30 In the CD-ROMs Needed for Installation window, click **Continue**.

The installation proceeds with a separate progress bar window for each CD-ROM or DVD. You are prompted to change media when a new CD-ROM is required to complete the installation. A splash screen displays “Congratulations! Your Red Hat Enterprise Linux installation is now complete!” when the installation is finished.



Note This part of the installation takes approximately 10 minutes. When it is finished, you will see a message that asks you to remove the final CD-ROM or installation DVD and reboot the server. You will now be taken through the RHEL Setup Agent process. Your server automatically reboots.

Setup Agent Guided Startup

After the server reboots a Red Hat welcome window appears followed by a Setup Agent window that tells you that there are a few more steps before your system is ready to use.

Step 31 In the Setup Agent window, click **Forward**.

The RHEL License Agreement appears in a separate window. You need to scroll down through the text and click **Forward** to indicate your agreement.

Step 32 In the RHEL License Agreement window, click **Forward**.

The Red Hat Firewall window appears.

Step 33 In the Red Hat Firewall window, click **Enable Firewall**.



Caution Disabling the firewall is a security risk. We do *not* recommend that you do so.

Step 34 Check the following checkboxes:

- Firewall Enable
- SSH
- Secure WWW (HTTPS)
- Telnet
- WWW (HTTP)

A confirmation window appears asking you to confirm your choices.

Step 35 In the confirmation window, do one of the following:

- Click **Yes** to continue with Setup
- Click **No** to return to the Firewall window and redo your selections.



INDEX

A

- active host (see HA) [2-3](#)
- admin password
 - resetting [5-2](#)
- ANM (anm) process [5-4](#)
- ANM interface
 - logging in [4-3](#)
- ANM Mobile
 - overview [1-3](#)
- ANM plug-in [2-6, 2-7](#)
- ANM server [1-2](#)
- ANM Virtual Appliance [1-2](#)

B

- backing up data [5-9, 5-12](#)
- backup
 - create
 - HA configuration [5-12](#)
 - standalone configuration [5-9](#)
- browser requirements, client [1-5](#)

C

- caution
 - logging in as root user [5-7](#)
- checking ANM status [5-5](#)
- config property errors, fixing [5-8](#)
- cookies, client browser requirement [1-5, 4-4](#)
- copying data [5-9, 5-12](#)

D

- data
 - backing up [5-9, 5-12](#)
 - restoring [5-10, 5-12](#)
- data center manager process. See ANM process
- device access layer (dal) process [5-4](#)
- device licenses
 - managing in ANM [4-6](#)
- disk space, server requirement [1-4](#)
- Dynamic Workload Scaling (DWS) [1-3](#)

E

- errors
 - using Lifeline to collect data [5-7](#)

F

- firewall monitoring
 - process status of in ANM [5-4](#)
- firewall monitor process, firewall monitoring [5-4](#)

H

- HA mode
 - ANM server requirement [1-4](#)
 - configuring ANM [2-2](#)
 - installation [2-3](#)
 - installation parameter descriptions [2-4](#)
 - uninstalling ANM with [2-6, 2-7](#)
- HA properties
 - fixing errors for configuration [5-8](#)

hard disk, server requirement [1-4](#)

High Availability

See HA mode [1-4](#)

HTTP

disabled [2-1](#)

I

installation

HA mode [2-3](#)

in non-HA mode [2-2](#)

installation session log, obtaining [5-5](#)

J

JavaScript, client browser requirement [1-5, 4-4](#)

L

licenses

installing on ANM server [4-2](#)

managing ANM [4-6](#)

process status in ANM [5-4](#)

server requirement [1-4](#)

using PAK for key file [4-1](#)

licman process, licensing [5-4](#)

Lifeline

install troubleshooting [5-7](#)

running manually [5-7](#)

Linux system users for ANM [2-1, 2-7](#)

log, obtaining install session [5-5](#)

logging in

to ANM [4-3](#)

login problems

various [5-2](#)

M

Media Check and Server Partitioning [A-2](#)

migrating

list of post upgrade features [3-2](#)

monitoring

ANM licenses [4-6](#)

MySQL process

installation of [1-3, 2-1](#)

restarting ANM [5-4](#)

N

node ID [2-5](#)

non-HA mode

installation [2-2](#)

O

operating system

client requirement [1-5](#)

P

password, resetting admin [5-2](#)

plug-in for vCenter Server

overview [1-3](#)

popup

windows, enabled requirement [4-4](#)

ports

ANM, used for ANM client (browser) to ANM server communication [4-9](#)

ANM, used for managed device communication [4-10](#)

reference [4-9](#)

processes

active node in ANM HA example [5-5, 5-6](#)

standalone ANM example [5-5](#)

standby node in ANM HA example [5-6](#)

starting ANM [5-5](#)

status of ANM [5-4](#)
 stopping ANM [5-7](#)
 processor, server requirement [1-4](#)

R

RAM

client requirements [1-5](#)
 server requirement [1-4](#)

Red Hat

guidelines for OS installation [A-1](#)

Red Hat Installation [A-1](#)

resetting, admin password [5-2](#)

restarting ANM [5-4](#)

restore

HA configuration [5-12](#)

restoring data [5-10, 5-12](#)

reverting to old data [5-10, 5-12](#)

RHEL

see Red Hat [A-1](#)

root user, becoming [1-5](#)

S

saving data [5-9, 5-12](#)

staged objects, upgrade requirement [3-2](#)

standalone mode installation [2-2](#)

standby host (see non-HA) [2-3](#)

starting ANM [5-5](#)

status

ANM process [5-4](#)

checking ANM [5-5](#)

stopping ANM [5-7](#)

system requirements [1-1](#)

server [1-3](#)

T

technical support, required information for [5-4](#)

timeout, setting web [5-8](#)

troubleshooting [5-2](#)

forwarding installation log [5-5](#)

post-install login problems [5-2](#)

reconfiguring node ID [5-8](#)

restoring data [5-10](#)

web idle session time out, setting [5-8](#)

U

uninstallation

in HA mode [2-6, 2-7](#)

in non-HA mode [2-6](#)

upgrade

overview [3-1](#)

upgrade, ANM

HA mode [3-6](#)

standalone mode [3-4](#)

V

vCenter Server

plug-in, overview [1-3](#)

VMware [2-6, 2-7](#)

VMware integration [1-3](#)

W

web timeout, setting [5-8](#)

