Juniper Networks
Network and Security Manager

CentOS Upgrade Guide

Release
2012.2

Modified: 2015-07-20
Revision 4

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Network and Security Manager CentOS Upgrade Guide

Revision History
May 2013—Revision 1
December 2013—Revision 2
March 2015—Revision 3
July 2015—Revision 4

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Tables

About This Guide

Objectives

This *Network and Security Manager CentOS Upgrade Guide* describes how you can upgrade CentOS on the Network and Security Manager (NSM) system.

Audience

This guide is intended primarily for IT administrators who are responsible for installing, upgrading, and maintaining NSM.

Conventions

The sample screens used throughout this guide are representations of the screens that appear when you install and configure the NSM software. The actual screens may differ.

All examples show default file paths. If you do not accept the installation defaults, your paths will vary from the examples.

Table 1 on page viii defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page viii defines text conventions used in this guide.

Table 2: Text Conventions

Convention	Description	Examples
Bold typeface like this	• Represents commands and keywords in text. • Represents keywords • Represents UI elements	• Issue the **clock source** command. • Specify the keyword **exp-msg**. • Click **User Objects**
Bold typeface like this	Represents text that the user must type.	**user input**

`fixed-width font`	Represents information as displayed on the terminal screen.	`host1#`
		show ip ospf
		`Routing Process OSPF 2 with Router ID 5.5.0.250`
		`Router is an area Border Router (ABR)`

Key names linked with a plus (+) sign	Indicates that you must press two or more keys simultaneously.	Ctrl + d
Italics	• Emphasizes words • Identifies variables	• The product supports two levels of access, *user* and *privileged*. • *clusterID*, *ipAddress*.

Table 2: Text Conventions *(continued)*

Convention	Description	Examples
The angle bracket (>)	Indicates navigation paths through the UI by clicking menu options and links.	**Object Manager > User Objects > Local Objects**

Table 3 on page ix defines syntax conventions used in this guide.

Table 3: Syntax Conventions

Convention	Description	Examples
Words in plain text	Represent keywords	terminal length
Words in italics	Represent variables	*mask, accessListName*
Words separated by the pipe (|) symbol	Represent a choice to select one keyword or variable to the left or right of this symbol. The keyword or variable can be optional or required.	diagnostic | line
Words enclosed in brackets ([ ])	Represent optional keywords or variables.	[internal | external]
Words enclosed in brackets followed by an asterisk ([ ]*)	Represent optional keywords or variables that can be entered more than once.	[level1 | level2 | l1]*
Words enclosed in braces ({ })	Represent required keywords or variables.	{ permit | deny } { in | out } { clusterId | ipAddress }

Documentation

Table 4 on page ix describes documentation for NSM.

Table 4: Network and Security Manager Publications

Book	Description
Network and Security Manager Installation Guide	Describes the steps to install the NSM management system on a single server or on separate servers. It also includes information on how to install and run the NSM user interface. This guide is intended for IT administrators responsible for the installation or upgrade of NSM.

Table 4: Network and Security Manager Publications *(continued)*

Book	Description
Network and Security Manager Administration Guide	Describes how to use and configure key management features in the NSM. It provides conceptual information, suggested workflows, and examples. This guide is best used in conjunction with the NSM Online Help, which provides step-by-step instructions for performing management tasks in the NSM UI. This guide is intended for application administrators or those individuals responsible for owning the server and security infrastructure and configuring the product for multi-user systems. It is also intended for device configuration administrators, firewall and VPN administrators, and network security operation center administrators.
Network and Security Manager Configuring ScreenOS Devices Guide	Provides details about configuring device features for all supported ScreenOS platforms.
Network and Security Manager Configuring Intrusion Detection and Prevention Devices Guide	Provides details about configuring device features for all supported Intrusion Detection and Prevention (IDP) platforms.
Network and Security Manager Online Help	Provides procedures for basic tasks in the NSM user interface. It also includes a brief overview of the NSM system and a description of the GUI elements.
Network and Security Manager API Guide	Provides complete syntax and description of the SOAP messaging interface to NSM.
Network and Security Manager Release Notes	Provides the latest information about features, changes, known problems, resolved problems, and system maximum values. If the information in the Release Notes differs from the information found in the documentation set, follow the Release Notes. Release notes are included on the corresponding software CD and are available on the Juniper Networks website.
Network and Security Manager Configuring Infranet Controllers Guide	Provides details about configuring the device features for all supported Infranet Controllers.
Network and Security Manager Configuring Secure Access Devices Guide	Provides details about configuring the device features for all supported Secure Access Devices.
Network and Security Manager Configuring EX Series Switches Guide	Provides details about configuring the device features for all supported EX Series platforms.

Table 4: Network and Security Manager Publications *(continued)*

Book	Description
Network and Security Manager Configuring J Series Services Routers and SRX Series Services Gateways Guide	Provides details about configuring the device features for all supported J Series Services Routers and SRX Series Services Gateways.
Network and Security Manager M Series and MX Series Devices Guide	Provides details about configuring the device features for M Series and MX Series platforms.

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at http://www.juniper.net/support/requesting-support.html

PART 1

Network and Security Manager CentOS Upgrade Procedures

CHAPTER 1

Upgrading CentOS 4.x to CentOS 5.7 on NSM Appliances

To resolve some security vulnerabilities in CentOS 4.X releases, in NSM 2012.2 you need to upgrade NSM appliances to CentOS 5.7. NSM 2011.4 and 2010.3 can also run on CentOS 5.7. This section describes how to upgrade your existing NSMXpress appliances to run CentOS 5.7.

NOTE: **After CentOS upgrade, NSM database and logs are retained without any change. However, NSM OS IP, passwords and other OS level settings are lost and need to be configured after upgrade.**

Prerequisite

The following are the prerequisites to upgrade NSM appliance OS:

- CentOS5.7 ISO **NSMXpress-appliance-CentOS5.7-v1.iso**.
- Recovery partition update script **UpdateRecoveryPartition_5.7_v1.sh**.
- Linux build package of the current NSM version.
- NSM appliance should be accessible through the console port.

Upgrading an NSM Appliance OS

This section provides two procedures to upgrade an NSM appliance OS.

You can follow either of the procedures to upgrade the appliance.

Upgrading Using Local Hard Disk

To upgrade CentOS 4.x to CentOS to 5.7 using upgrade script:

1. Download CentOS Upgrade and Update Recovery Partition Script_v1 (by navigating to **Tools** section of the appropriate NSM release) to the NSM Appliance **/tmp** directory.
2. Download NSM Appliance ISO CentOS5.7_v1 (by navigating to **Tools** section of the appropriate NSM release) **/tmp** directory.

   

   NOTE: Compare the MD5 checksum value of the downloaded files in the NSM Appliance server with the MD5 checksum value of the corresponding file in the software download page to verify if the correct files are downloaded completely. If they are the same, then the files are successfully downloaded.

   Example of two download files :

   - **# md5sum UpdateRecoveryPartition_5.7_v1.sh**
   - **# md5sum NSMXpress-appliance-CentOS5.7-v1.zip**

3. Extract the downloaded zip file using the command **unzip NSMXpress-appliance-CentOS5.7-v1.zip**.
4. Execute the downloaded script with CentOS 5.7 ISO image using the following commands:

   # sh /tmp/UpdateRecoveryPartition_5.7_v1.sh /tmp/NSMXpress-appliance-centOS5.7-v1.iso

   Example:

```
[root@NSMXpress tmp]# sh /tmp/UpdateRecoveryPartition_5.7_v1.sh
/tmp/NSMXpress-appliance-centOS5.7-v1.iso
--- Running UpdateRecoveryPartition_5.7_v1.sh
Currently installed CentOS version is 5.7
Creating Mount directory.........................OK
Checking /var/cores disk space...................OK
Checking Mount for NSMXpress-appliance-centOS5.7-v1.isoOK
Checking Mount for sda1..........................OK
Mounting /dev/sda1...............................OK
Mounting NSMXpress-appliance-centOS5.7-v1.isoOK
Backing up existing BOOTLOADER...................OK
Replacing sda1 boot modules with NSMXpress-appliance-centOS5.7-v1.isoOK
Replacing nsm.iso in sda1........................OK
Copying ks.cfg upgrade ISO to HD.................OK
Modifying ks.cfg to boot from HD.................OK
Modifying Grub Menu..............................OK
Unmounting sda1..................................OK
Umounting NSMXpress-appliance-centOS5.7-v1.isoOK
System is ready for REBOOT
[root@NSMXpress tmp]#
```

5. After running the **UpdateRecoveryPartition_5.7_v1.sh** script, access the NSM Appliance through its console port and log in.

6. Reboot the NSM Appliance.
7. During reboot process, press any key to enter the menu when prompted.

   A menu screen with the following options are displayed:

   - NSMXpress
   - Rescue
   - Upgrade OS to Centos 5.7
   - Boot from USB to restore previous OS (Now Booting Normally)

   

   NOTE: **For NSMXpress, the last option is Boot from Secondary Drive To Restore Original OS.**

8. Select **Upgrade OS to CentOS 5.7** option and press **Enter**. The following is displayed:

   Example:

   ```
   Using this option will Upgrade the OS to CentOS 5.7 To confirm upgrade, type
   upgrade at the password prompt. To abort and boot at the Rescue mode, just hit
    <Enter> at the password prompt. Press any key.
   ```

9. Press any key for the password prompt.
10. Enter the password as **upgrade** and press **Enter**.

    The CentOS upgrade process starts. It will take approximately 15 minutes for CentOS to get upgraded to CentOS 5.7 .

Upgrading Using CDROM

To reimage an appliance using CDROM:

1. Download the ISO file from NSM Appliance ISO CentOS5.7_v1 (by navigating to **Tools** section of the appropriate NSM release), to a PC or Server having a DVD writer.

   

   NOTE: **Compare the MD5 checksum value of the downloaded files in the NSM Appliance server with the MD5 checksum value of the corresponding file in the software download page to verify if the correct files are downloaded completely. If they are the same, then the files are successfully downloaded.**

   Example of two download files :

   - **# md5sum UpdateRecoveryPartition_5.7_v1.sh**
   - **# md5sum NSMXpress-appliance-CentOS5.7-v1.zip**

2. Use a DVD burning tool to burn the image on a DVD.
3. Use an external USB DVD ROM drive for NSMXpress Series II or NSM3000 appliance.

4. Change the boot sequence in the BIOS to boot from the USB DVD ROM drive.
5. Reboot the system.

   When the system boots from the DVD, the following grub options are displayed:

   - **rescue**
   - **erase-reinstall**
   - **memtest86**
6. Select **erase-reinstall** and let the automated installation complete.
7. Refresh NSM and interface configuration after the installation.

Verifying the Upgrade

After you have upgraded the NSM Appliance OS using either an upgrade script or a CDROM, you can verify if the appliance OS has been upgraded successfully.

Use the command **# uname –r** to find the kernel name and version.

If the command output is **2.6.18-274.el5PAE**, then the appliance is upgraded to CentOS5.7.

If the command output is **2.6.9-67.0.20.ELsmp**, then the appliance is not upgraded to CentOS5.7.

Setting Up Administrative Accounts and Networking

Logging In to the System

- Log in as admin using the password **abc123**, and change the password when prompted.

Connecting an Appliance to the Network

To connect an NSM appliance to the network, follow the prompts as displayed in the console:

- Please enter new IP address for interface eth0

  Enter the value **10.205.10.161**.
- Please enter new subnet mask for interface eth0

  Enter the value **255.255.0.0**.
- Enter the default gateway as a dotted-decimal IP address:

  Enter the value **10.205.255.254**.

NOTE:

- The values used are examples.
- If you enter an incorrect value, a message appears that directs you to enter your responses in dotted-decimal format.
- To configure your system with a web browser, connect to https://10.205.10.161/administration.

Configuring and Refreshing NSM

To configure and refresh NSM:

1. Log in as the root user using the command **sudo su -**.

   When you are prompted for a password, provide the administrator password that you had set previously in .

2. Download the appropriate NSM build from Juniper Software Download Page.
3. Extract the downloaded zip files using the command **unzip NSM_Build.zip**.

   Example:

   - For NSM2012.2R1, the command is: **unzip nsm2012.2R1_servers_linux_86.zip**
   - For NSM2010.3s10, the command is **unzip nsm2010.3s10_servers_linux_x86.zip**

4. Execute the command **sh <NSM_Build.sh>** and select the Refresh option.

   Example:

   - For NSM2012.2R1, the command is: **sh nsm2012.2R1_servers_linux_x86.sh** .
   - For NSM2010.3s10, the command is : **sh nsm2010.3s10_servers_linux_x86.sh**.

Running NSM Setup

Use the **nsm_setup** command to configure DNS. The menu options available are:

NSMXpress Settings Menu

```
1> Change Password
2> Set Interfaces
3> Set Routing
4> Change Hostname
5> Set DNS Servers
6> Change Time Options
7> Forward Local Status Emails
8> System Security Update

Q> Quit
R> Redraw menu

Choice [1-8, Q,R]: 5
```

```
DNS name server options:
1> Add a nameserver

M> Return to Main Menu
R> Redraw menu

Choice [1,M,R]: 1
Please type the new nameserver in dotted decimal notation:
10.206.194.50
Added 10.206.194.50
NSMXpress Settings Menu

1> Change Password
2> Set Interfaces
3> Set Routing
4> Change Hostname
5> Set DNS Servers
6> Change Time Options
7> Forward Local Status Emails
8> System Security Update

Q> Quit
R> Redraw menu

Choice [1-8,Q,R]: Q

Select a change to cancel it:
1> DNS add: 10.206.194.50

A> Apply all changes
M> Make more changes
C> Cancel all changes and quit
R> Redraw menu

Choice [1,A,M,C,R]: A
Applying Changes...
Re-loading database
Done!
```

NOTE: The option 9 > **Configure Extended HA** is available only in NSM 3000 Series appliances.

Checking the Installation

Check if the build is installed and running. The sample output is as mentioned below:

```
[root@NSMXpress ~]# /etc/init.d/guiSvr version
   nsm owner is nsm
   Retrieving version information...
   guiSvrManager 2012.1 (Build LGB17z1bw)
   guiSvrMasterController 2012.1 (Build LGB17z1bw) 06/18/2012
   guiSvrDirectiveHandler 2012.1 (Build LGB17z1bw) 06/18/2012
   guiSvrLicenseManager 2012.1 (Build LGB17z1bw) 06/18/2012
   guiSvrStatusMonitor 2012.1 (Build LGB17z1bw)
   guiSvrWebProxy 2012.1 (Build LGB17z1bw) 06/18/2012
   [root@NSMXpress ~]# /etc/init.d/devSvr version
   nsm owner is nsm
   Retrieving version information...
```

```
devSvrDbSvr PostgreSQL 8.4.10
devSvrManager 2012.1 (Build LGB17z1bw)
devSvrLogWalker 2012.1 (Build LGB17z1bw)
devSvrDataCollector 2012.1 (Build LGB17z1bw) 06/18/2012
devSvrDirectiveHandler 2012.1 (Build LGB17z1bw) 06/18/2012
devSvrProfilerMgr 2012.1 (Build LGB17z1bw)
devSvrStatusMonitor 2012.1 (Build LGB17z1bw)
devSvrTFTP 2012.1 (Build LGB17z1bw)
```

CHAPTER 2

Update Recovery Partition to a Factory Default Version with CentOS 5.7

The recovery partition contains all files necessary to perform a clean installation of the NSMXpress OS and its applications with default settings. When the NSMXpress appliance is shipped from the factory, the recovery partition files match the version of the NSMXpress OS with factory default settings.

This chapter explains how to update the recovery partition to a factory default version of 2012.1r1 with CentOS 5.7.

Performing Recovery Partition Upgrade

To perform recovery partition upgrade:

1. Download the script **UpdateRecoveryPartition_5.7_v1.sh** from the CentOS Upgrade and Update Recovery Partition Script_v1 (by navigating to **Tools** section of the appropriate NSM release) for upgrading CentOS 5.7 to the NSM Appliance under **/tmp** directory.
2. Download the ISO image **NSMXpress-CentOS5.7-recup-RS-v1.iso** or **NSMXpress-CentOS5.7-recup-CM-v1.iso** depending on whether the appliance is RS or CM), from the Update Recovery Partition ISO for CM Server_v1 and Update Recovery Partition ISO for RS Server_v1 by navigating to **Tools** section of the appropriate NSM release.
3. Verify the downloaded files. Compare the MD5 checksum value of the downloaded files in the NSM Appliance server with the MD5 checksum value of the corresponding file in the software download page to verify if the correct files are downloaded completely. If they are the same, then the files are successfully downloaded.

   Examples of three downloaded files :

   - # md5sum UpdateRecoveryPartition_5.7_v1.sh
   - # md5sum NSMXpress-CentOS5.7-recup-RS-v1.iso (for Regional Server)
   - # md5sum NSMXpress-CentOS5.7-recup-CM-v1.iso (for Central Manager)

4. Copy the images to the NSM Appliance under **/tmp** directory for update recovery partition on CentOS 5.7 using the script.
5. Execute the downloaded script with CentOS 5.7 ISO image using the command:

   RS Appliance—# sh /tmp/UpdateRecoveryPartition_5.7_v1.sh /tmp/NSMXpress-CentOS5.7-recup-RS-v1.iso.

   CM Appliance—# sh /tmp/UpdateRecoveryPartition_5.7_v1.sh /tmp/NSMXpress-CentOS5.7-recup-CM-v1.iso.

   You have now successfully upgraded the recovery partition.

Restoring the System to Factory Setting

Some of the scenarios in which the system may need to be restored to factory setting are as follows:

- The file system of the appliance gets corrupted and cannot be repaired
- Clean up the current version of the NSM build and perform clean installation of the ISO image with 2012.1R1 NSM build

To restore the system to the factory setting, reboot the system.

1. During reboot process, press any key to enter the menu when prompted.

   A menu screen with the following options are displayed:

   - NSMXpress
   - Rescue
   - Re-install CentOS 5.7 image with 2012.1R1 NSM build
   - Boot from Secondary Drive To Restore Original OS

2. Select **Re-install CentOS 5.7 image with 2012.1R1 NSM build** option and press **Enter**. The following is displayed:

   Example:

   ```
   Using this option will completely erase your appliance and load the CentOS 5.7
    default image.  No data recovery is possible after re-installing.  To confirm
      erase and re-install, type "erase" at the password prompt.  To abort and
   boot into Rescue mode, just hit Enter at the password prompt.  Press any key.
   ```

3. Press any key for the password prompt.
4. Enter the password as **erase** and press **Enter**.

   Re-image of the appliance with CentOS 5.7 starts. The process will take approximately 30 minutes for re-installing the CentOS 5.7 image with 2012.1R1 NSM build.

NOTE: The re-imaging is always to 2012.1R1 irrespective of the build that is currently present in the appliance.

5. In NSM, log in as admin using the password **abc123**. Configure the **IP**, **subnet mask** and, **default gateway addresses**.

   After restoring the system to the factory setting, NSM is in off state, and IPs will be set to **192.168.0.2** in the NSM config files. As a workaround, change the IPs according to the management IP of the NSM Central Manager and Regional Server and then start the NSM services manually.

To change the IP address:

- Edit **/var/netscreen/DevSvr/devSvr.cfg** and change the GUI Server address **guiSvr1.addr** on line 6.
- In NSM GUI navigate to Administer > Server Manager > Server.
- Open the guiSvr, modify the IP address, and save the file.
- Open the devSvr, modify the IP, and save the file.
- Restart the NSM Server processes.

CHAPTER 3

Upgrading CentOS to Version 6.5 on NSM Appliances

To resolve some security vulnerabilities in CentOS releases, in NSM 2012.2 you need to upgrade NSM appliances to CentOS 5.7 or 6.5. This section describes how to upgrade your existing NSMXpress appliances to run CentOS 6.5.

NOTE:

- After the CentOS upgrade, the NSM database and logs are retained unchanged. However, the NSM OS IP address, passwords, and other OS-level settings are lost and need to be configured again.
- The CentOS 6.5 upgrade ISO is not compatible with the NSMXpress and NSM4000 appliances. However, it is supported on the NSMXpress-II and NSM3000 appliances.
- Update recovery partition and factory default features are not supported on CentOS 6.5 for the NSMXpress-II and NSM3000 appliances.

Prerequisites

The following are the prerequisites to upgrade the NSM appliance OS:

- CentOS6.5 ISO **NSMXpress-appliance-Upgrade-CentOS6.5-v1.iso** script.
- Update script **Upgrade-6.5.sh**.
- The NSM appliance should be accessible through the console port.

NOTE: **After the OS upgrade, you must upgrade NSM to version 2012.2R7 or later.**

Upgrading an NSM Appliance OS Using an Upgrade Script

To upgrade CentOS to version 6.5 using the upgrade script:

1. Navigate to the **Tools** section of the appropriate NSM release, and download NSM Appliance Upgrade Script CentOS6.5 v1 to the NSM Appliance **/tmp** directory.
2. Navigate to the **Tools** section of the appropriate NSM release, and download NSM Appliance Upgrade ISO CentOS6.5 v1 to the NSM appliance **/tmp** directory.

NOTE: Compare the MD5 checksum value of each of the downloaded files in the NSM Appliance server with the MD5 checksum value of the corresponding files on the software download page to verify that the correct files are downloaded completely. If the checksum values are the same, then the files are successfully downloaded.

Example of two download files :

- **# md5sum Upgrade-6.5.sh**
- **# md5sum NSMXpress-appliance-Upgrade-CentOS6.5-v1.zip**

3. Extract the downloaded ZIP file using the command **unzip NSMXpress-appliance-Upgrade-CentOS6.5-v1.zip**.
4. Execute the downloaded script with the CentOS 6.5 ISO image using the following commands:

   # sh /tmp/Upgrade-6.5.sh

   /tmp/NSMXpress-appliance-Upgrade-centOS6.5-v1.iso

   Example:

```
[root@NSMXpress tmp]# sh Upgrade-6.5.sh
NSMXpress-appliance-Upgrade-CentOS6.5-v1.iso
--- Running Upgrade-6.5.sh ---
Currently installed CentOS version is 5.7
Upgrade to CentOS 6.x will take some time.
Please wait ...
Creating Mount directory.....................OK
Checking /var/cores disk space..................OK
Checking Mount for NSMXpress-appliance-Upgrade-CentOS6.5-v1.isoOK
Checking Mount for sda1.....................OK
Mounting /dev/sda1..........................OK
Mounting NSMXpress-appliance-CentOS6.5-v1.iso.....OK
Backing up existing BOOTLOADER..................OK
Replacing sda1 boot modules with NSMXpress-appliance-CentOS6.5-v1.isoOK
Replacing nsm.iso in sda1.....................OK
Copying ks.cfg upgrade ISO to HD..............OK
Modifying ks.cfg to boot from HD..............Modifying Grub
Menu..........................OK
Unmounting sda1..............................OK
Umounting NSMXpress-appliance-CentOS6.5-v1.iso....OK
System is ready for REBOOT
[root@NSMXpress tmp]#
```

NOTE: If you are not running the recommended NSM version for CentOS 6.5, one of the following warning messages is displayed while NSM is executing the downloaded script:

- For NSM versions other than 2012.2:

```
WARNING: Currently installed NSM version is: NSM 2012.1R10

To continue CentOS 6.x Upgrade, you must upgrade NSM to Recommended
 version 2012.2R7.
```

- For NSM version 2012.2 to 2012.2R6

```
WARNING: Currently installed NSM version is: 2012.2R2

Recommended version is 2012.2R7 or later.

After upgrading OS to CentOS 6.x, you must upgrade NSM to 2012.2R7
 or later
```

5. After the **Upgrade-6.5.sh** script runs, access the NSM appliance through its console port and log in.
6. Reboot the NSM appliance.
7. During the reboot process, press any key to enter the menu when prompted.

   A menu screen with the following options is displayed:

   - NSMXpress
   - Rescue
   - Upgrade OS to Centos 6.5
   - Boot from USB to restore previous OS (Now Booting Normally)

   NOTE: For NSMXpress, the last option is Boot from Secondary Drive To Restore Original OS.

8. Select **Upgrade OS to CentOS 6.5** and press **Enter**. The following message is displayed:

   Example:

```
Using this option will Upgrade the OS to CentOS 6.5 To confirm upgrade, type
upgrade at the password prompt. To abort and boot at the Rescue mode, just hit
 <Enter> at the password prompt. Press any key.
```

9. Press any key for the password prompt.
10. Enter the password as **upgrade** and press **Enter**.

    The CentOS upgrade process starts. It will take approximately 15 minutes for CentOS to be upgraded to CentOS 6.5.

    NOTE: Ignore the Warning: Partition size of /var/netscreen are not matching message displayed in NSM3000 appliances.

Verifying the Upgrade

After you run the upgrade script to upgrade the NSM appliance OS, you can verify that the upgrade was successful.

Use the command **# uname –r** to find the kernel name and version.

If the command output is **2.6.32-504.3.3.SCLC6_5.R3.1.1.i686**, then the appliance was successfully upgraded to CentOS 6.5.

Setting Up Administrative Accounts and Networking

Logging In to the System

- Log in as admin using the password **abc123**, and change the password when prompted.

NOTE: **The following note is displayed during your first login:**

```
Note:Supported NSM version on CentOS 6.x is 2012.2R7 or later.
```

Connecting an Appliance to the Network

To connect an NSM appliance to the network, follow the prompts as displayed on the console:

- Please enter new IP address for interface eth0:

  Enter the value **10.205.10.161**.

- Please enter new subnet mask for interface eth0:

  Enter the value **255.255.0.0**.

- Enter the default gateway as a dotted-decimal IP address:

  Enter the value **10.205.255.254**.

NOTE:

- **The values used are examples.**
- **If you enter an incorrect value, a message appears that directs you to enter your responses in dotted-decimal format.**
- **To configure your system with a Web browser, connect to** https://10.205.10.161/administration.
- **For HA-enabled servers, restart HA server services using the /etc/init.d/haSvr restart command.**

Running NSM Setup

Use the **nsm_setup** command to configure DNS. The following menu options are available:

NSMXpress Settings Menu

```
1> Change Password
2> Set Interfaces
3> Set Routing
4> Change Hostname
5> Set DNS Servers
6> Change Time Options
7> Forward Local Status Emails
8> System Security Update

Q> Quit
R> Redraw menu

Choice [1-8, Q,R]: 5

DNS name server options:
1> Add a nameserver

M> Return to Main Menu
R> Redraw menu

Choice [1,M,R]: 1
Please type the new nameserver in dotted decimal notation:
10.206.194.50
Added 10.206.194.50
NSMXpress Settings Menu

1> Change Password
2> Set Interfaces
3> Set Routing
4> Change Hostname
5> Set DNS Servers
6> Change Time Options
7> Forward Local Status Emails
8> System Security Update

Q> Quit
R> Redraw menu

Choice [1-8,Q,R]: Q

Select a change to cancel it:
1> DNS add: 10.206.194.50

A> Apply all changes
M> Make more changes
C> Cancel all changes and quit
R> Redraw menu

Choice [1,A,M,C,R]: A
Applying Changes...
Re-loading database
Done!
```

NOTE: The option 9 > **Configure Extended HA** is available only on NSM3000 line appliances.

Checking the Installation

Check if the build is installed and running. Sample output is displayed below:

```
[root@NSMXpress ~]# /etc/init.d/guiSvr version
nsm owner is nsm
Retrieving version information...
guiSvrManager 2012.2R7 (Build LGB18z1e83)
guiSvrMasterController 2012.2R7 (Build LGB18z1e83) 01/30/2014
guiSvrDirectiveHandler 2012.2R7 (Build LGB18z1e83) 01/30/2014
guiSvrLicenseManager 2012.2R7 (Build LGB18z1e83) 01/30/2014
guiSvrStatusMonitor 2012.2R7 (Build LGB18z1e83)
guiSvrWebProxy 2012.2R7 (Build LGB18z1e83) 01/30/2014
[root@NSMXpress ~]# /etc/init.d/devSvr version
nsm owner is nsm
Retrieving version information...
devSvrDbSvr PostgreSQL 8.4.20
devSvrManager 2012.2R7 (Build LGB18z1e83)
devSvrLogWalker 2012.2R7 (Build LGB18z1e83)
devSvrDataCollector 2012.2R7 (Build LGB18z1e83) 01/30/2014
devSvrDirectiveHandler 2012.2R7 (Build LGB18z1e83) 01/30/2014
devSvrProfilerMgr 2012.2R7 (Build LGB18z1e83)
devSvrStatusMonitor 2012.2R7 (Build LGB18z1e83)
devSvrTFTP 2012.2R7 (Build LGB18z1e83)
[root@NSMXpress ~]# /etc/init.d/guiSvr status
nsm owner is nsm
Retrieving status...
guiSvrManager (pid 10980).....................ON
guiSvrMasterController (pid 11465).............ON
guiSvrDirectiveHandler (pid 11920).............ON
guiSvrLicenseManager (pid 14004)...............ON
guiSvrStatusMonitor (pid 14570)................ON
guiSvrWebProxy (pid 14834).....................ON
[root@NSMXpress ~]# /etc/init.d/devSvr status
nsm owner is nsm
Retrieving status...
devSvrDbSvr (pid 24300).......................ON
devSvrManager (pid 24574).....................ON
devSvrLogWalker (pid 26671)...................ON
devSvrDataCollector (pid 27080)...............ON
devSvrDirectiveHandler (pid 27650).............ON
devSvrProfilerMgr (pid 30901).................ON
devSvrStatusMonitor (pid 31395)...............ON
devSvrTFTP (pid 32329
32334)........................................ON
[root@NSMXpress ~]#
```

CHAPTER 4

CentOS Upgrade Path Examples

This chapter provides some examples for CentOS upgrade path.

Upgrade Paths for CentOS 5.7

The upgrade scenarios require the following components:

- ISO image
- CentOS Upgrade and Update Recovery Partition Script
- NSM builds of main and patch releases as mentioned in the scenarios

The scenarios available for CentOS upgrade on NSM 3000 and NSM Series II appliances are:

Scenario 1

2009.1r1a (CentOS 4.x) to **2010.3s7 (CentOS 4.x)** through **CentOS 5.7 ISO** to **2010.3s7, 2010.3s12, 2012.1R6 & 2012.2R2** on NSMxpress II Appliance.

The purpose of this scenario is to check if CentOS upgrade works for 2010.3s7. This scenario covers the following:

- Migration from 2009.1.r1a build having 4.x CentOS version to 2010.3s7 build having CentOS 4.x.

- Upgradation of CentOS to 5.7 using ISO.
- Migration to 2010.3s12, user interface testing and continue migration to 2012.1R6 and 2012.2R2

Scenario 2

2009.1r1a (CentOS 4.x) to **2011.4s4 (CentOS 4.x)** through **CentOS 5.7 ISO** to **2011.4s4, 2011.4s9, 2012.1R6 & 2012.2R2** on NSMXpress RS appliance.

The purpose of this scenario is to check if CentOS upgrade works for 2011.4s4. This scenario covers the following:

- Migration from 2009.1.r1a build having 4.x CentOS version to 2011.4s4 build having CentOS 4.x.
- Upgradation of CentOS to 5.7 using ISO.
- Migration to 2011.4s9, user interface testing and continue migration to 2012.1R6 and 2012.2R2.
- Update recovery partition using ISO Script.

Scenario 3

2009.1r1a (CentOS 4.x) to **2012.1R1(CentOS 4.x)** through **CentOS 5.7 ISO** to **2012.1R1, 2012.1R6 & 2012.2R2 on NSM3000 appliance**

The purpose of this scenario is to check if CentOS upgrade works for 2012.1R1. This scenario covers the following:

- Migration from 2009.1.r1a build having 4.x CentOS version to 2012.1R1 build having CentOS 4.x.
- Upgradation of CentOS to 5.7 using ISO.
- Migration to 2012.1R6, user interface testing and continue migration to 2012.2R2.

Scenario 4

2009.1r1a (CentOS 4.x) to **2012.2(CentOS 4.X)** through **CentOS 5.7 ISO** to **2012.2 and 2012.2R2** on NSMXpress Central Manager Appliance.

The purpose of this scenario is to check if CentOS upgrade works for 2012.2. This scenario covers the following:

- Migration from 2009.1.r1a build having 4.x CentOS version to 2012.2 build having CentOS 4.x.
- Upgradation of CentOS to 5.7 using ISO.
- Migration to 2012.2, user interface testing and continue migration to 2012.2R2
- Update recovery Partition using ISO Script.

Scenario 5

2009.1r1a (CentOS 4.x) to **2010.3s7(CentOS 4.x)** through **CentOS 5.7 ISO** to **2010.3s7 and 2012.2R2 on NSM3000 appliance** .

The purpose of this scenario is to check if CentOS upgrade works for 2010.3s7. This scenario covers the following:

- Migration from 2009.1.r1a build having 4.x CentOS version to 2010.3s7 build having CentOS 4.x.
- Upgradation of CentOS to 5.7 using ISO.
- Migration to 2012.2R2
- Update recovery Partition using ISO Script.

Scenario 6

2009.1r1a (CentOS 4.x) to **2011.4s4(CentOS 4.x)** through **CentOS 5.7 ISO** to **2011.4s4 & 2012.2R2 on NSM-Xpress-CM Appliance**.

The purpose of this scenario is to check if CentOS upgrade works for 2011.4s4. This scenario covers the following:

- Migration from 2009.1.r1a build having 4.x CentOS version to 2011.4s4 build having CentOS 4.x.
- Upgradation of CentOS to 5.7 using ISO.
- Migration to 2012.2R2.

Scenario 7

2009.1r1a (CentOS 4.x) to **2012.2(CentOS 4.x)** through **CentOS 5.7 ISO** to **2012.2 & 2012.2R2 on NSMXpress Regional Server Appliance** .

The purpose of this scenario is to check if CentOS upgrade works for 2012.2. This scenario covers the following:

- Migration from 2009.1.r1a build having 4.x CentOS version to 2012.2 build having CentOS 4.x.
- Upgradation of CentOS to 5.7 using ISO.
- Migration to 2012.2R2
- Update recovery Partition using ISO Script.

Scenario 8

2009.1r1a (CentOS 4.x) to **2012.1R1(CentOS 4.x)** through **CentOS 5.7 ISO** to **2012.1R1 & 2012.2R2 on NSMXpress II appliance**.

The purpose of this scenario is to check if CentOS upgrade works for 2012.1R1. This scenario covers the following:

- Migration from 2009.1.r1a build having 4.x CentOS version to 2012.1R1 build having CentOS 4.x.
- Upgradation of CentOS to 5.7 using ISO.
- Migration to 2012.2R2
- Update recovery Partition using ISOscript .

Upgrade Paths for CentOS 6.5

The upgrade scenarios require the following components:

- ISO image
- CentOS Upgrade
- NSM builds of main and patch releases as mentioned in the scenarios

The scenarios available for CentOS upgrade on NSM appliances are:

- Scenario 1 on page 24
- Scenario 2 on page 24

Scenario 1

2009.1r1a (CentOS 4.x) through **2010.3s7 (CentOS 4.x)** to **2012.2R2 (CentOS 4.x)**; through **CentOS 6.5 ISO** to **2012.2R2, 2012.2R7, and later versions** on NSM appliances.

The purpose of this scenario is to check if the CentOS upgrade works for 2012.2R2. This scenario covers the following:

- Migration from NSM versions 2009.1.r1a to 2012.2R2 through 2010.3s7, on appliances with CentOS 4.x.
- Upgrade of CentOS to 6.5 using ISO.
- Migration to NSM 2012.2R7 and later versions.

Scenario 2

2009.1r1a (CentOS 4.x) to **2010.3s7 (CentOS 4.x)** through **CentOS 5.7 ISO** to **2012.2R7 and later versions** with **CentOS 6.5 ISO** on NSM appliances.

The purpose of this scenario is to check if the CentOS upgrade works for 2012.2R7. This scenario covers the following:

- Migration from NSM versions 2009.1.r1a to 2010.3s7, on appliances with CentOS 4.x.
- Upgrade of CentOS to 5.7 using ISO.

- Migration to NSM 2012.2R7 and later versions.
- Upgrade of CentOS to 6.5 using ISO.

PART 2

Index

Index