Legal notice

Nokia is a registered trademark of Nokia Corporation. Other products and company names mentioned herein may be trademarks or tradenames of their respective owners.

The information presented is subject to change without notice. No responsibility is assumed for inaccuracies contained herein.

© 2018 Nokia.
# Contents

**About this document** ................................................................................................................................. 9

**Part I: Getting started** ................................................................................................................................. 11

1 **Safety information** ..................................................................................................................................... 13
   1.1 Structure of safety statements ................................................................................................................ 13

2 **Before you begin** ....................................................................................................................................... 15
   2.1 Overview .................................................................................................................................................. 15

General deployment information .......................................................................................................................... 16
   2.2 Introduction ............................................................................................................................................... 16
   2.3 To obtain the UUID of a station ............................................................................................................ 18
   2.4 Using hostnames in the management network .................................................................................... 19
   2.5 Deployment in a VM .................................................................................................................................. 22
   2.6 Client deployment .................................................................................................................................... 23

NFM-P deployment requirements and restrictions .............................................................................................. 25
   2.7 NFM-P deployment requirements ........................................................................................................ 25
   2.8 NFM-P deployment restrictions ........................................................................................................... 29

3 **Using samconfig** ......................................................................................................................................... 33
   3.1 Overview ............................................................................................................................................... 33
   3.2 Introduction ............................................................................................................................................ 33
   3.3 Usage instructions .................................................................................................................................. 36

4 **RHEL OS configuration** ............................................................................................................................ 41
   4.1 Overview ............................................................................................................................................... 41

RHEL OS deployment restrictions and requirements .......................................................................................... 42
   4.2 Introduction ............................................................................................................................................ 42
   4.3 RHEL deployment restrictions ............................................................................................................ 42
   4.4 RHEL deployment requirements .......................................................................................................... 43
   4.5 To prepare disk partitions for NFM-P installation ............................................................................. 44
   4.6 To reset the disk partition reserved block counts ............................................................................. 45

RHEL OS deployment in a VM .......................................................................................................................... 47
   4.7 Introduction ........................................................................................................................................... 47
   4.8 To deploy the RHEL OS for NFM-P using a qcow2 image ................................................................. 47
Manual RHEL OS installation........................................................................................................................................53
4.9 RHEL OS installation requirements..................................................................................................................................................53
4.10 Required RHEL environment and OS packages..........................................................................................................................54
4.11 Required additional OS packages, auxiliary database.................................................................................................................60
4.12 Required additional OS packages, NSP Flow Collector..................................................................................................................61

5 RHEL disk configuration........................................................................................................................................................................63
5.1 Overview......................................................................................................................................................................................................63
5.2 Introduction.....................................................................................................................................................................................................63
5.3 Sizing the NE configuration backup partition......................................................................................................................................64
5.4 To configure an NFM-P disk partition created after the RHEL OS installation...............................................................................65
5.5 Disk partitioning for trial deployments................................................................................................................................................67
5.6 Disk partitioning for live deployments................................................................................................................................................73

6 TLS configuration and management......................................................................................................................................................81
6.1 Overview......................................................................................................................................................................................................81
6.2 Introduction......................................................................................................................................................................................................83
6.3 About TLS.....................................................................................................................................................................................................83
6.4 NFM-P TLS implementation.................................................................................................................................................................83
6.5 TLS deployment methods........................................................................................................................................................................85
6.6 Managing TLS versions and ciphers..................................................................................................................................................89

Automated TLS deployment procedures...............................................................................................................................................90
6.6 Workflow for automated TLS deployment..........................................................................................................................................90
6.7 To configure and enable an NSP PKI server.......................................................................................................................................91
6.8 To configure an NFM-P main server to request a PKI-server TLS certificate..................................................................................94
6.9 To configure an NFM-P auxiliary server to request a PKI-server TLS certificate.........................................................................97
6.10 To configure an NSP Flow Collector to request a PKI-server TLS certificate..............................................................................101

Manual TLS deployment procedures................................................................................................................................................105
6.11 Workflow for manual TLS deployment.............................................................................................................................................105
6.12 To perform the TLS preconfiguration.............................................................................................................................................107
6.13 To manually configure TLS on a main server.....................................................................................................................................111
6.14 To manually configure TLS on an auxiliary server......................................................................................................................114
6.15 To manually configure TLS on an NSP Flow Collector..................................................................................................................117
6.16 To manually configure TLS on an NSP analytics server................................................................................................................119

General TLS configuration procedures.................................................................................................................................................123
6.17 To disable TLS for XML API clients.............................................................................................................................................123
6.18 To enable TLS for XML API clients..............................................................................................................................................125
6.19 To suppress security warnings in NFM-P browser sessions......................................................................................................128
Part II: NFM-P system deployment

7 NFM-P installation

7.1 Overview

Introduction

7.2 General information

Standalone NFM-P system installation

7.3 Standalone system installation workflow

7.4 To install a standalone NFM-P system

Redundant NFM-P system installation

7.5 Redundant system installation workflow

7.6 To install a redundant NFM-P system

Auxiliary server installation

7.7 Auxiliary server installation workflow

7.8 To install an NFM-P auxiliary server

7.9 To add auxiliary servers to an NFM-P system

NSP Flow Collector installation

7.10 NSP Flow Collector installation workflow

7.11 To install an NSP Flow Collector

7.12 To configure NSP Flow Collector communication

Auxiliary database installation

7.13 Auxiliary database installation workflow

7.14 To prepare a station for auxiliary database installation

7.15 To install the NFM-P auxiliary database software

7.16 To add an auxiliary database to an NFM-P system

7.17 To add a station to an NFM-P auxiliary database

8 NFM-P qcow2 deployment

8.1 Introduction

8.2 To deploy a collocated standalone NFM-P system using a qcow2 image

9 5620 SAM upgrade to NFM-P

9.1 Overview

Introduction

9.2 General information

9.3 To perform the pre-upgrade tasks

Standalone 5620 SAM system upgrade to NFM-P

9.4 Standalone 5620 SAM system upgrade workflow

9.5 To upgrade a standalone 5620 SAM system to the NFM-P
Redundant 5620 SAM system upgrade to NFM-P ................................................................. 285
9.6 Component references ........................................................................................................ 285
9.7 Redundant 5620 SAM system upgrade workflow ............................................................ 286
9.8 To upgrade a redundant 5620 SAM system to the NFM-P ............................................... 291

5620 SAM auxiliary server upgrade .................................................................................... 329
9.9 To upgrade a 5620 SAM auxiliary server ........................................................................ 329

5620 SAM Cflowd auxiliary server upgrade ......................................................................... 335
9.10 To upgrade a 5620 SAM Cflowd auxiliary server ........................................................... 335

5620 SAM auxiliary database upgrade .................................................................................. 340
9.11 To upgrade a 5620 SAM auxiliary database .................................................................. 340

5620 SAM analytics server upgrade .................................................................................... 351
9.12 To upgrade the 5620 SAM analytics servers .................................................................. 351

10 NFM-P upgrade ................................................................................................................. 367
10.1 Overview ........................................................................................................................ 367

Introduction .......................................................................................................................... 368
10.2 General information ......................................................................................................... 368
10.3 To perform the pre-upgrade tasks ................................................................................... 369
10.4 To apply an NSP RHEL qcow2 OS update ...................................................................... 380

Standalone NFM-P system upgrade ...................................................................................... 383
10.5 Standalone system upgrade workflow .......................................................................... 383
10.6 To upgrade a standalone NFM-P system ...................................................................... 385

Redundant NFM-P system upgrade ....................................................................................... 400
10.7 Component references .................................................................................................... 400
10.8 Redundant system upgrade workflow .......................................................................... 401
10.9 To upgrade a redundant NFM-P system ...................................................................... 406

Auxiliary server upgrade ..................................................................................................... 435
10.10 To upgrade an NFM-P auxiliary server ....................................................................... 435

NSP Flow Collector upgrade ............................................................................................... 438
10.11 To upgrade an NSP Flow Collector .............................................................................. 438

Auxiliary database upgrade ................................................................................................. 441
10.12 To upgrade an NFM-P auxiliary database ................................................................... 441

NFM-P analytics server upgrade .......................................................................................... 449
10.13 To upgrade the NFM-P analytics servers ................................................................... 449

11 NFM-P conversion to redundancy ..................................................................................... 465
11.1 Overview ........................................................................................................................ 465
## Introduction

- 11.2 General information .......................................................... 466
- 11.3 System conversion to redundancy workflow .......................... 467

**NFM-P system conversion to redundancy** ........................................ 469

- 11.4 To convert a standalone NFM-P system to a redundant system ........................................ 469

## 12 NFM-P conversion to IPv6

- 12.1 Overview ........................................................................... 501

**Introduction** .............................................................................. 502

- 12.2 General information................................................................. 502
- 12.3 System conversion to IPv6 workflow ........................................ 503
- 12.4 To perform the pre-conversion tasks ....................................... 503

**NFM-P system conversion to IPv6** .................................................. 508

- 12.5 To convert a standalone NFM-P system to IPv6 ........................ 508
- 12.6 To convert a redundant NFM-P system to IPv6 ......................... 518

## 13 NFM-P uninstallation

- 13.1 Overview ........................................................................... 545

**Introduction** .............................................................................. 545

- 13.2 NFM-P system uninstallation workflow ................................. 546
- 13.4 To uninstall an NSP Flow Collector ........................................ 547
- 13.5 To uninstall an auxiliary server .............................................. 548
- 13.6 To uninstall an auxiliary database .......................................... 550
- 13.7 To uninstall a main server .................................................... 552
- 13.8 To uninstall a main database ................................................ 554

**Part III: NFM-P client deployment** ................................................ 557

## 14 Single-user client deployment

- 14.1 Overview ........................................................................... 559

**Introduction** .............................................................................. 560

- 14.2 Single-user GUI client deployment ........................................ 560
- 14.3 To install the Oracle JRE on a RHEL station ............................. 561

**Single-user GUI client installation** .................................................. 564

- 14.4 To install a single-user GUI client ........................................... 564

**Single-user GUI client upgrade** .................................................... 569

- 14.5 To upgrade an NFM-P Release 17 or 5620 SAM single-user GUI client ........................................ 569
- 14.6 To upgrade an NFM-P Release 18 single-user GUI client ............................. 572
Contents

**Single-user GUI client uninstallation** .............................................................. 578
14.7 To uninstall a single-user GUI client ............................................................... 578

15 **Client delegate server deployment** ................................................................. 581
15.1 Overview .............................................................................................................. 581

**Introduction** ........................................................................................................ 582
15.2 Client delegate server deployment ................................................................. 582

**Client delegate server installation** ................................................................. 584
15.3 To install a client delegate server ................................................................. 584
15.4 To add a client delegate server to an existing system ........................................... 592

**Client delegate server upgrade** ................................................................. 596
15.5 To upgrade an NFM-P Release 17 or 5620 SAM client delegate server ................ 596
15.6 To upgrade an NFM-P Release 18 client delegate server ................................... 600

**Client delegate server uninstallation** ............................................................... 606
15.7 To uninstall a client delegate server ............................................................... 606
About this document

Purpose

The NSP NFM-P Installation and Upgrade Guide describes NFM-P installation, upgrade, and platform modification operations such as system conversion to redundancy and system conversion to IPv6.

Safety information

For your safety, this document contains safety statements. Safety statements are given at points where risks of damage to personnel, equipment, and operation may exist. Failure to follow the directions in a safety statement may result in serious consequences.

Document support

Customer documentation and product support URLs:

• Customer Documentation Welcome Page
• Technical support

How to comment

Documentation feedback
Part I: Getting started

Overview

Purpose
This part describes how to prepare for NFM-P system or system component deployment, and includes important requirements, restrictions, and platform configuration procedures.

Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, Safety information</td>
<td>13</td>
</tr>
<tr>
<td>Chapter 2, Before you begin</td>
<td>15</td>
</tr>
<tr>
<td>Chapter 3, Using samconfig</td>
<td>33</td>
</tr>
<tr>
<td>Chapter 4, RHEL OS configuration</td>
<td>41</td>
</tr>
<tr>
<td>Chapter 5, RHEL disk configuration</td>
<td>63</td>
</tr>
<tr>
<td>Chapter 6, TLS configuration and management</td>
<td>81</td>
</tr>
</tbody>
</table>
# 1 Safety information

## 1.1 Structure of safety statements

### 1.1.1 Overview

This topic describes the components of safety statements that appear in this document.

### 1.1.2 General structure

Safety statements include the following structural elements:

![Diagram of safety statement structure]

<table>
<thead>
<tr>
<th>Item</th>
<th>Structure element</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Safety alert symbol</td>
<td>Indicates the potential for personal injury (optional)</td>
</tr>
<tr>
<td>2</td>
<td>Safety symbol</td>
<td>Indicates hazard type (optional)</td>
</tr>
<tr>
<td>3</td>
<td>Signal word</td>
<td>Indicates the severity of the hazard</td>
</tr>
<tr>
<td>4</td>
<td>Hazard type</td>
<td>Describes the source of the risk of damage or injury</td>
</tr>
<tr>
<td>5</td>
<td>Safety message</td>
<td>Consequences if protective measures fail</td>
</tr>
<tr>
<td>6</td>
<td>Avoidance message</td>
<td>Protective measures to take to avoid the hazard</td>
</tr>
<tr>
<td>7</td>
<td>Identifier</td>
<td>The reference ID of the safety statement (optional)</td>
</tr>
</tbody>
</table>
### Signal words

The signal words identify the hazard severity levels as follows:

<table>
<thead>
<tr>
<th>Signal word</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>DANGER</td>
<td>Indicates the described activity or situation may, or will, represent a potential for a serious injury.</td>
</tr>
<tr>
<td>WARNING</td>
<td>Indicates the described activity or situation may, or will, cause equipment damage or serious performance problems.</td>
</tr>
<tr>
<td>CAUTION</td>
<td>Indicates the described activity or situation may, or will, cause service disruption.</td>
</tr>
<tr>
<td>NOTICE</td>
<td>Indicates the described activity or situation may, or will, cause minor performance problems.</td>
</tr>
</tbody>
</table>
2 Before you begin

2.1 Overview

2.1.1 Purpose

This chapter describes the requirements and restrictions that apply to NFM-P system deployment, and contains other important information that you must read and understand before you attempt to deploy an NFM-P component.

2.1.2 Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 Overview</td>
<td>15</td>
</tr>
<tr>
<td>General deployment information</td>
<td>16</td>
</tr>
<tr>
<td>2.2 Introduction</td>
<td>16</td>
</tr>
<tr>
<td>2.3 To obtain the UUID of a station</td>
<td>18</td>
</tr>
<tr>
<td>2.4 Using hostnames in the management network</td>
<td>19</td>
</tr>
<tr>
<td>2.5 Deployment in a VM</td>
<td>22</td>
</tr>
<tr>
<td>2.6 Client deployment</td>
<td>23</td>
</tr>
<tr>
<td>NFM-P deployment requirements and restrictions</td>
<td>25</td>
</tr>
<tr>
<td>2.7 NFM-P deployment requirements</td>
<td>25</td>
</tr>
<tr>
<td>2.8 NFM-P deployment restrictions</td>
<td>29</td>
</tr>
</tbody>
</table>
General deployment information

2.2 Introduction

2.2.1 Description

CAUTION

Service Disruption

An NFM-P system upgrade, conversion to redundancy, or conversion to IPv6 requires a thorough understanding of NFM-P system administration and platform requirements, and is supported only under the conditions described in this guide, the NSP NFM-P Planning Guide, and the NFM-P Release Notice.

Such an operation must be planned, documented, and tested in advance on a trial system that is representative of the target live network. Contact technical support to assess the requirements of your NFM-P deployment, and for information about the upgrade service, which you are strongly recommended to engage for any type of deployment.

This chapter describes the general conditions that apply to NFM-P deployment. Before you attempt to deploy or configure an NFM-P component, you must comply with the conditions in this chapter and ensure that the NFM-P platform is configured as described in the other chapters of Part I: “Getting started”.

Part III: “NFM-P client deployment” contains OS-specific information about single-user GUI client and client delegate server deployment.

Guide conventions

This guide uses the following terminology:

- station—a discrete processing entity, such as a physical or virtual computer
- peer—an equivalent component in the same system. For example, the peer main server of the primary main server in a redundant system is the standby main server. The term peer is irrespective of the primary or standby role.

The procedures in this guide include default parameter values, when appropriate. A default value is acceptable in most deployment environments, but must be validated against specific requirements, for example, firewall constraints. For more information, see the NSP NFM-P Planning Guide and the current NFM-P Release Notice, or contact technical support.

Platform support

You can deploy NFM-P components in a virtual machine, or VM. See the NSP NFM-P Planning Guide for VM host system requirements, and 2.5 “Deployment in a VM” (p. 22) for general deployment requirements and restrictions.

An NFM-P system has the following required components:

- one standalone main server, or two in a redundant deployment
• one standalone main database, or two in a redundant deployment
• one or more single-user GUI clients or client delegate servers

An NFM-P deployment may include the following optional components and NSP modules:
• auxiliary servers
• an auxiliary database
• NSP Flow Collectors
• NSP analytics servers

**Note:** This guide describes the following analytics server deployment operations:
• upgrade from 5620 SAM to NSP
• upgrade from NFM-P to NSP
The *NSP Deployment and Installation Guide* describes the following:
• NSP analytics server installation
• NSP analytics server upgrade

**Note:** CPAM functions in an NFM-P system are enabled only when the system includes one or more operational 7701 CPAA devices. See the *7701 CPAA and vCPAA Setup and Installation Guide* for 7701 CPAA deployment information.

The following table lists the supported platforms for each NFM-P component type.

**Table 2-1** NFM-P platform support by component

<table>
<thead>
<tr>
<th>NFM-P component</th>
<th>Mac OS X</th>
<th>Microsoft Windows</th>
<th>RHEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main server</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Main database</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Auxiliary server</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Auxiliary database</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>NSP Flow Collector</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Client delegate server</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Single-user client</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**nsp user account**

NFM-P system operation and management require a RHEL user account called nsp in the nsp user group.

• The initial installation of any of the following components on a station creates the group and account:
  - main server
  - auxiliary server
  - NSP Flow Collector
• The *nsp* user owns all NFM-P server processes; only the *nsp* user can start or stop a server, or run a server script.
• The *nsp* home directory is */opt/nsp*.
• The initial *nsp* password is randomly generated, and must be changed by the root user.
• The root user owns some files in the */opt/nsp/nfmp/server* directory for low-level installation and support functions.
• Server uninstallation does not remove the *nsp* user account, user group, or home directory.
• Root user privileges are required only for component installation or upgrade, and for low-level support functions.

### 2.3 To obtain the UUID of a station

#### 2.3.1 Description
An NFM-P license is specific to the UUID of a main server station, and must be provided in a license request. The following steps describe how to obtain the UUID of a station that is to host an NFM-P main server.

**Note:** If you are using an Integrated Lights Out Management system, ensure that you obtain the UUID of the intended blade and not the UUID of the ILO module.

**Note:** You must perform this procedure on each station that is to host a main server.

**Note:** A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

#### 2.3.2 Steps

1. Log in to the main server station as the root user.

2. Open a console window.

3. Enter the following:

   ```
   # cat /sys/devices/virtual/dmi/id/product_uuid
   ```

   The UUID is displayed; for example:
   
   ```
   35F59783-2258-11E1-BBDA-38B41F432C41
   ```

4. Record the value for use when you request the NFM-P license for the main server.

**END OF STEPS**
2.4 Using hostnames in the management network

2.4.1 Overview

The topology of an NFM-P management network may be sufficiently complex to benefit from or require the use of hostnames, rather than fixed IP addresses, for communication between NFM-P components. Hostname resolution is of even greater benefit when NAT is used between NFM-P clients and a main server that communicates over multiple networks.

Also, some CA signing authorities include only hostnames, and not IP addresses, in the SAN field of a signed TLS certificate.

**Note:** If the SAN field of a signed certificate includes only hostnames, when you use the `samconfig` utility to configure client access on a main server, you must specify a hostname, rather than an IP address.

**Description**

This section provides a configuration example for hostname resolution in a moderately complex NFM-P management network that does not include a NAT configuration.

**Note:** When the NFM-P clients and the auxiliary or peer main servers use different main server interfaces to communicate with a main server, the clients must use a hostname to reach the main server. See the *NSP NFM-P Planning Guide* for more information.

**Note:** If a TLS certificate to be signed by a public CA includes a hostname, the hostname must be an FQDN and not a short hostname. A self-signed certificate can use an FQDN or a short hostname.

**Note:** Only local hostname resolution is supported. The use of a DNS server for NFM-P hostname resolution is not supported.

To enable hostname resolution in an NFM-P management network, you must do the following:

- Configure the local `/etc/hosts` file on each component to ensure that each hostname translates to the correct IP address.
- During component deployment, specify hostnames instead of IP addresses.

**Note:** Hostnames are case-sensitive, and must not begin with a number; an NFM-P hostname must comply with the hostname syntax defined in IETF RFC 1034.

**Hostname usage requirements and restrictions**

When two server components use hostnames to communicate, the `/etc/hosts` file must contain the following:

- **on a main server:**
  - an entry for each auxiliary server that maps the auxiliary server hostname to the IP address of the auxiliary server interface that is used for main server communication
  - an entry for each database that maps the database hostname to the IP address of the database interface that is used for main server to database communication
• on an auxiliary server:
  - an entry for each main server that maps the main server hostname to the IP address of the main server interface that is used for auxiliary server communication
  - an entry for each auxiliary server that maps the auxiliary server hostname to the IP address of the auxiliary server interface that is used for main server communication
  - an entry for each database that maps the database hostname to the IP address of the database interface that is used for database communication

Note: Each main server must map an auxiliary server hostname to the same IP address.

Note: A component hostname that you specify in an /etc/hosts file must be the exact hostname returned by the following command:

```
hostname
```
If the command returns localhost.localdomain, the hostname is not set; you must set the hostname using the following command as the root user:

```
hostnamectl set-hostname hostname
```
where `hostname` is the short hostname or FQDN, depending on your requirement

Note: Depending on the management network topology, the hosts files of various components may map the same main server hostname to different IP addresses in order to reach the correct main server interface.

Note: Each main and auxiliary server must have a network route to each address provided in a TLS certificate.

Management network configuration example

The following example provides guidance about configuring local hostname resolution for NFM-P components in a relatively complex management network. In the example, each main server communicates with multiple networks using separate interfaces, as shown in Figure 2-1, "Management network topology" (p. 21).
The client IP addresses are in the 192.168.1 subnet, and the internal management IP addresses are in the 192.168.2 subnet.

The component hostnames in the example are the following:
- main servers—main_a and main_b
- main databases—db_a and db_b
- auxiliary servers—aux_a and aux_b

The same configuration methodology must be applied to all components in the internal management network. The following are the configuration requirements for each component in the 192.168.2 subnet.

The /etc/hosts file on station main_a requires the following entries:
Before you begin
General deployment information
Deployment in a VM

2.5 Deployment in a VM

2.5.1 Description

The requirements and restrictions below apply to NFM-P component deployment in a virtual machine, or VM. VM deployment is supported in the following environments:

- KVM
- Openstack
- VMware

Note: The requirements and restrictions in “NFM-P deployment requirements and restrictions” (p. 25) also apply to VM deployments.

Note: Before you deploy an NFM-P component in a VMware VM, you must install the latest VMware Tools software.

See the NSP NFM-P Planning Guide for the hardware virtualization requirements, and for the specific configuration requirements of a supported environment.
2.5.2 VM deployment using qcow2 images

You can use qcow2 disk images to deploy the following:

• RHEL OS, for subsequent component installation; see “RHEL OS deployment in a VM” (p. 47)
• NFM-P system; see Chapter 8, “NFM-P qcow2 deployment”

2.5.3 NFM-P server and database virtualization

The following conditions apply to main server, auxiliary server, client delegate server, or database deployments in VMs.

• The guest OS must be an NFM-P-supported version of RHEL 7 Server x86-64.
• A RHEL deployment on VMware requires VMXNET 3 NIC adapters; see the VMware documentation for information.

2.5.4 Client virtualization

The following conditions apply to NFM-P single-user GUI client deployment in a VM.

• You can deploy a VM client in a live network environment only if the client resources are dedicated to the guest OS, and not shared or oversubscribed.
• The guest OS must be a supported OS version; see the NSP NFM-P Planning Guide.
• The supported connection application for a VMware ESXi Windows platform is Windows Remote Desktop.

Additional EMS requirements and restrictions

The following conditions apply to an NFM-P single-user GUI client or client delegate server in a VM that requires the installation of an additional element manager on the same platform, or is to use an additional NE management interface.

• You can use two or more NICs to isolate network traffic between the client VM and the managed NEs. Such a configuration may be required when an additional element manager, for example, NEIO, must share the client resources, or when web-based NE management is to be performed from the client station.
• Additional RAM, disk space, and CPU resources are required to accommodate an element manager that shares a client platform; see the NSP NFM-P Planning Guide.

2.6 Client deployment

2.6.1 Description

The installation or upgrade of an NFM-P single-user GUI client or client delegate server is a software push from a main server that you initiate using a browser on the client station. The main server must be installed and fully initialized before you can install or upgrade the client software.
The software push mechanism enables centralized client software management. During startup, an existing single-user client or client delegate server checks for available software updates on the main server. Any available client configuration updates are automatically applied.

See the following for client installation and upgrade information:

- Chapter 14, “Single-user client deployment” — single-user client deployment
- Chapter 15, “Client delegate server deployment” — client delegate server deployment

### 2.6.2 Client software upgrades

After an NFM-P main server is upgraded, a GUI client that connects to the main server automatically detects the release mismatch and attempts an upgrade to the main server release level.

During a software upgrade, an NFM-P client downloads and installs only the files required for the upgrade. The upgrade process removes previously downloaded local files that are not required by the updated client software.

### 2.6.3 Client configuration changes

When the single-user GUI clients or client delegate servers that connect to a main server require a configuration update, an administrator updates the global client configuration stored on a main server. Each client software instance detects and applies the update at the start of the next client session. See “System component configuration procedures” in the *NSP NFM-P System Administrator Guide* for information about globally updating client configurations.

**Note:** A client backs up the existing configuration files as part of a configuration update.
NFM-P deployment requirements and restrictions

2.7 NFM-P deployment requirements

2.7.1 Network requirements

CAUTION

Service Disruption

The use of hostname resolution for GUI and XML API client communication with an NFM-P main server in a NAT environment is strongly recommended.

When IP addresses are used in a NAT environment, the following conditions apply:

• All client communication with the main server must use the public IP address of the main server.
• The NAT firewall must be configured to allow the main server to communicate with itself using the public IP address.

CAUTION

Service Disruption

In a redundant system, a GUI client that opens a browser connection to the primary NFM-P main server may need to use the IP address or hostname of the peer main server after a main server communication failure.

To resolve the two IP addresses or hostnames, a GUI client can use a common DNS name which maps each main server IP address provided by the DNS server to the primary main server.

• Configure a DNS server for GUI clients to map each main server IP address to a common DNS name.
• Configure each GUI client to use the common DNS name for browser connections to the NFM-P.
• Use a client browser that caches multiple IP addresses associated with one hostname.

The NFM-P network requirements apply to the following:

• management network—the network in which the NFM-P components communicate with each other
• managed network and external systems—the managed NEs, and external management systems that are integrated with the NFM-P

Management network

The following requirements apply to the NFM-P management network.

• During a main server installation or upgrade, you must use hostnames to identify the main server interfaces under the following conditions:
  - when the XML API and GUI clients communicate with a main server using multiple IP addresses for the main server
- when the XML API and GUI clients use different addresses to communicate with a main server through one interface on the main server

• An auxiliary server must be accessible to each main server and database in a redundant NFM-P system. Optimally, all components in a deployment are in the same LAN and have high-quality network interconnection.

• Each station in an auxiliary database must be on the same side of the management LAN, and not geographically dispersed.

• When two components use hostnames to communicate, the /etc/hosts file on each component station must contain the following:
  - an entry that maps the hostname assigned to the interface on the other component to the IP address used to reach the other component
  - an entry that maps the hostname of the other component station to each IP address used to reach the other component

• Using NAT adds an extra level of complexity to an NFM-P network. The /etc/hosts file on each component station must contain the correct public and private address entries for reaching other components at the following times:
  - during normal operation
  - after an NFM-P component or network component failure

• Specifying a TCP or UDP port other than the default during an installation or upgrade can affect component communication through a firewall. Ensure that you record any changes to default port numbers and make the ports available through the firewall.

• The hostname of an NFM-P component must meet the following criteria.
  - It contains only ASCII alphanumeric and hyphen characters.
  - It does not begin or end with a hyphen.
  - If the hostname is an FQDN, period characters delimit the FQDN components.
  - The FQDN of the hostname does not exceed 63 characters.

• When you use a hostname to identify an NFM-P component, you must use local hostname resolution; the use of DNS is not supported.

**Note:** A component hostname that you specify in an /etc/hosts file must be the exact hostname returned by the following command:

```
hostname
```

**Note:** Hostnames are case-sensitive.
Managed network and external systems

CAUTION

Management Disruption

If an NFM-P system that is to be upgraded manages a device as a GNE, and the new NFM-P release supports native management of the device, you must unmanage the device and delete it from the main database before the upgrade.

After the upgrade, you can use the NFM-P to discover and manage the device natively, rather than as a GNE.

CAUTION

Management Disruption

NFM-P eNodeB PM statistics collection fails when the eNodeB and NFM-P real-time clocks are not synchronized.

The NFM-P and all eNodeB devices require a common time-synchronization server that uses a protocol such as NTP.

CAUTION

Management Disruption

A Release 14.0 R6 or earlier 5620 SAM system that manages 9500 MPR devices requires special configuration for an upgrade to the NFM-P; otherwise, the NFM-P cannot manage the devices after the upgrade.

The 5620 SAM system upgrade procedures include links to the required configuration procedures in the NSP NFM-P Wavence User Guide.

See “Wavence migration to revised service model” in the NSP NFM-P Wavence User Guide for more information.

Note: An upgrade from a 5620 SAM release creates, for each existing IPSec IKE policy, a new IKE transform policy using the IKE transform settings in the IPSec IKE policy. The IKE Transform policy ID created during the upgrade is equal to the ID of the IPSec IKE policy plus 2048. The IKE transform policy is associated with the IPSec IKE policy and saved in Draft mode. After the upgrade, the IKE transform policy must be set to Released to be distributed to the NEs.

The following requirements apply to the network of NFM-P-managed devices, and to the external systems with which the NFM-P is integrated.

- Before you upgrade an NFM-P system, you must confirm that the new NFM-P software release supports the release of each managed device. If this is not true, you must perform one of the following before you attempt the upgrade, or service disruption may occur.
  - Upgrade the device to a release that the new NFM-P release supports.
Use an NFM-P client to unmanage the device, remove the device from the managed network, and remove the discovery rule element for the device.

• Before you upgrade an NFM-P system, you must ensure that the new NFM-P software is compatible with the software release of each integrated external system. Contact technical support for information about external system compatibility.

• An NFM-P system that manages eNodeB devices has special disk partitioning requirements. See Chapter 5, "RHEL disk configuration" for information.

• An NFM-P system upgrade does not preserve 9500 MPR device software images. If you want to retain the images, you must export the images to a remote file system before the upgrade, and import the images to the NFM-P after the upgrade.

• Before the NFM-P can manage an eNodeB, functions such as PM statistics transfers and network snapshots require configuration; see the NSP NFM-P LTE RAN User Guide for specific eNodeB management information.

2.7.2 Platform requirements

Note: For optimal storage performance on a supported Nokia AirFrame server, set the default write cache policy for each created storage volume to Write Through. See the Nokia AirFrame server documentation for information about verifying, configuring, and setting the write cache policy for a volume.

The following are the NFM-P platform requirements.

• The platform must meet the minimum requirements described in the NSP NFM-P Planning Guide.

• The OS release and patch level of all main server, main database, and optional component stations in an NFM-P system must be identical.

• The platform must be dedicated to the NFM-P only; sharing the platform is not supported. System operation may be adversely affected by the activity of other software on the same station.

• Before you install or upgrade a redundant NFM-P system, you must enable SSH on each main server, auxiliary server, and main database station in the system.

• If the NFM-P is to collect statistics on a large scale, as defined in the NSP NFM-P Planning Guide, you must use a disk array with the main database to increase performance. See Chapter 5, "RHEL disk configuration" for information.

• The NFM-P XML API and GUI client real-time clocks must always be synchronized with the main server real-time clock. The use of NTP or an equivalent time protocol is strongly recommended.

• The Bash shell is the supported command shell for RHEL CLI operations.
2.7.3 Security requirements

**Note:** The use of sudo to gain root user privileges is supported for NFM-P installation, and for any other operation in this guide that requires root user privileges.

The following are the NFM-P security requirements.

- The Oracle management user requires full read and write permissions on the main database installation directory, /opt/nsp/nfmp/db, and any specifically created partitions, for example, /opt/nsp/nfmp/dbbackup.

- The user that installs an NFM-P single-user GUI nt requires local user privileges only, but must have full access permissions on the client installation directory. The user that opens the client installer must have sufficient file permissions to create the installation directory, or the installation fails.

2.7.4 Software requirements

The following are the NFM-P software requirements.

- An NFM-P system deployment requires a license file in compressed format with a .zip extension. A license file has the following characteristics.
  - The UUID of the host station is required to generate the license. 2.3 “To obtain the UUID of a station” (p. 18) describes how to obtain a station UUID.
  - The file can accommodate two system IDs, which enables the use of the same file on redundant main servers, and is recommended.
  - Renaming the compressed file has no effect on the validity of the contained license file, but renaming the contained XML license file renders it invalid.
  - The main server configuration utility copies the license file content to a backup location; a change to the license file content or location after an installation or upgrade does not affect the main server operation.

- You must ensure that you have sufficient time to complete a main database upgrade. The time required for an upgrade depends on the platform resources, database complexity, and tablespace configuration. See the *NSP NFM-P Planning Guide* for database upgrade time estimates.

2.8 NFM-P deployment restrictions

2.8.1 Network restrictions

**Note:** The use of NAT between NFM-P server and database components is not supported. The NFM-P supports NAT only between the following:

- main server and single-user client or client delegate server
- main or auxiliary server and XML API client
- main or auxiliary server and managed network

**Note:** Before you attempt to deploy an NFM-P system, or add a component to a system, you must ensure that any firewalls between the components allow the required traffic to pass...
between the components, or are disabled. The *NSP NFM-P Planning Guide* lists the open ports required by each component, and provides information about using NFM-P templates to create RHEL Firewalld rules.

**Note:** If you use SSH X forwarding to perform a procedure in this guide, the “su - oracle” command fails. In such a scenario, you must log in directly as the Oracle management user to perform the required actions.

The following restrictions apply to the network environment in which an NFM-P system or component is deployed.

- **DNS or NIS name resolution is not supported between NFM-P components, and a pre-existing name service must not conflict with NFM-P address resolution. The restriction also applies to XML API client communication with the NFM-P.**

- **You cannot use “localhost” or an alias IP address to identify a component.**

- **An NFM-P main server listens for GUI and XML API client communication on only one interface unless you specify a hostname for the main server during an installation or upgrade.**

- **You cannot use a hostname to identify a main database station; NFM-P components can use only an IP address to reach a database.**

- **All IP communication from an NFM-P auxiliary server to an NFM-P main server must originate from one IP address, which is the auxiliary server address specified during the main server configuration. A main server rejects communication from an auxiliary server if the auxiliary server uses a source address other than the configured address.**

- **During a single-user client installation, you can specify a hostname instead of an IP address to identify a main server. A client upgrade occurs automatically through a connection to a main server named in the client configuration.**

**IPv4 and IPv6**

- **NFM-P components communicate with other NFM-P components and external entities using IPv4 or IPv6 exclusively, with the following exceptions:**
  - The NFM-P can communicate with and manage a network using IPv4 and IPv6 concurrently.
  - An NFM-P GUI or browser-based application client can connect to the NFM-P using IPv4 or IPv6, regardless of the protocol version in use between the NFM-P server and database components.

  **Note:** If the GUI or application clients are to connect to the NFM-P using IPv4 and IPv6, when you use the samconfig utility to configure client access on a main server, you must specify a hostname rather than an IP address.

- **Before you can specify an IPv6 address for an NFM-P component, the IPv6 interface must be plumbed and operational. See the OS documentation for information about enabling and configuring an IPv6 interface.**

- **Before you use a procedure in Chapter 12, “NFM-P conversion to IPv6” to convert an NFM-P system from IPv4 to IPv6, the system must be at the software release described in this guide.”**
2.8.2 Platform restrictions

The following are the NFM-P platform restrictions.

- An NFM-P single-user client or client delegate server cannot be installed on the same station as an NFM-P server or database.
- An NFM-P single-user client and client delegate server cannot be installed on the same station.
- An optional system component requires a dedicated station. The sharing of a station by optional components is not supported; attempts to deploy multiple components on one station fail.
- If you plan to convert a standalone NFM-P system to a redundant system, and also plan to upgrade the system, you must perform the upgrade before the conversion.
- An NFM-P system conversion from IPv4 to IPv6 is not supported during an upgrade or conversion to redundancy.

2.8.3 Security restrictions

The following are the NFM-P security restrictions.

- The user that starts an NFM-P client must be the user that installs the client software, or another user that has read, write, and execute privileges on the client files and directories.
- An NFM-P domain name defines the network-management domain to which an NFM-P component belongs, and must be unique to a network. An NFM-P component can interact only with other NFM-P components in the same NFM-P domain. During system installation, you must specify the same domain name for each component in the system.

2.8.4 Software restrictions

**CAUTION**

Service Disruption

An NFM-P upgrade does not preserve all non-default settings in configuration files such as nms-server.xml.

If an NFM-P configuration file contains non-default settings that you want to retain after an upgrade, contact technical support for assistance before the upgrade.

**CAUTION**

Data Loss

At the beginning of an NFM-P server upgrade, the NFM-P installation utility backs up specific configuration and log files to a time-stamped directory under the installation directory, and then deletes specific directories below the installation directory.

If you create or modify a file under the main server installation directory, you risk losing the file during an NFM-P upgrade unless you first back up the file to a location that is unaffected by the upgrade activity.
**Note:** An NFM-P server upgrade applies a default set of file permissions to each directory below the main server installation directory. If you change the file permissions of a directory below the main server installation directory and want the permissions to be in effect after an upgrade, you must re-apply the permissions after the upgrade.

**Note:** After an NSP analytics server upgrade:
- Scheduled report creation continues, but uses the new report versions, which may differ from the former versions.
- Saved reports remain available, but lack any new features of the upgraded report versions; it is recommended that you recreate and save the reports.
- If a report changes significantly between releases, the report may no longer function. See the *NFM-P Release Notice* for limitations regarding specific reports.

The following are the NFM-P software restrictions.

- The *NFM-P Release Notice* contains important release-specific information. Ensure that you read the Release Notice for the current release before you attempt an NFM-P installation or upgrade.
- You can upgrade an NFM-P component that is no more than two major releases older than the current release. For example, you can upgrade a Release 14.0 or later 5620 SAM system to NFM-P Release 18, but you cannot upgrade a Release 13.0 5620 SAM system directly to NFM-P Release 18; you must first perform an intermediate upgrade to 5620 SAM Release 14.0 or NFM-P Release 17.
- After an upgrade to an intermediate release, for example, an upgrade from 5620 SAM Release 13.0 to Release 14.0 before a final upgrade to an NFM-P release, you must allow each main server to initialize fully before the final upgrade, or the final upgrade fails.
- A redundant system upgrade requires a network-management outage and must be performed only during a scheduled maintenance period of sufficient duration.
- You cannot share an existing Oracle installation with the NFM-P, and no other application can use the NFM-P Oracle software.
- You can specify the installation directory for a single-user client or client delegate server, but not for any other type of component.
- You can deploy a main server without specifying a license file. However, if you do not specify a license file, you cannot start the main server until you import a license. See “Software and license configuration procedures” in the *NSP NFM-P System Administrator Guide* for information about importing licenses.
3 Using samconfig

3.1 Overview

3.1.1 Purpose
This chapter describes the NFM-P configuration utility called samconfig.

3.1.2 Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1 Overview</td>
<td>33</td>
</tr>
<tr>
<td>3.2 Introduction</td>
<td>33</td>
</tr>
<tr>
<td>3.3 Usage instructions</td>
<td>36</td>
</tr>
</tbody>
</table>

3.2 Introduction

3.2.1 General information
To deploy or configure most NFM-P system components, an operator uses the CLI-based samconfig utility. After you install the samconfig RPM package on a station, you can use the samconfig utility to:
• Immediately configure and deploy a component on the station.
• Create component configuration files for subsequent use in other deployments.

You can configure and deploy the following components using samconfig:
• main server
• main database
• auxiliary server
• NSP Flow Collector
• client delegate server

3.2.2 Functional description
The samconfig utility has a hierarchical menu structure similar to the menu structure of some NEs. The top level is called the root level. The configuration level, which is directly below the root level, contains the objects that you can configure. An object is a parameter, or a functional area that contains parameters.

The following commands are available at any menu level:
• show—show the non-default configuration values
• show-detail—show all configuration values
• ?, h, or help—display a help menu
• help-detail—display a detailed help menu
• back—move to the parent level
• exit—move to the root level, or, from the root level, exit samconfig

Root level
The root level is the level at which samconfig opens. The root-level prompt includes the component type, as shown below for a main server:

<main>

The following commands are exclusive to the root level:
• configure—enter the configuration level
• save filename—save the configuration in a file; the default is /opt/nsp/nfmp/config/nms/config/component_config.xml
  If a previous configuration file exists, it is renamed to include a time stamp.
• apply—apply the configuration

Configuration level
To configure an NFM-P component, you must enter the configuration level and specify objects, parameters, and values, as required. To move to the configuration level from the root level, you enter the following:

<component> configure

The configuration-level prompt is the following:

<component configure>

The configuration-level help menu lists the configurable objects, which are specific to the component type. The following is a help-menu sample that lists the configurable objects for a main server:

ip - Private IP address for local server communications

domain - NFM-P server complex domain name

[no] license - Absolute path to the NFM-P license file

client + Client Configuration

database + Database Configuration

mediation + Mediation Configuration

[no] aux + Auxiliary Server Configuration
[no] redundancy + Redundancy Configuration
[no] tls + Security Configuration
[no] oss + OSS Configuration
  auxdb + Auxiliary Database Configuration
[no] aa-stats + AA Stats Configuration
[no] registry + Registry Configuration

Note: The [no] option beside an object means that you can delete or disable the object configuration using the following syntax:
  no object

The following table defines the special characters that may be displayed beside an object or command.

Table 3-1  Special characters in samconfig menus

<table>
<thead>
<tr>
<th>Character</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>The object has child objects or parameters.</td>
</tr>
<tr>
<td>-</td>
<td>The object does not have child objects or parameters.</td>
</tr>
<tr>
<td>*</td>
<td>The object has one or more mandatory parameters that are not configured.</td>
</tr>
</tbody>
</table>

Note: You can save, but not apply a configuration that includes an unconfigured mandatory parameter.

Contextual help

At the configuration level, or in an object context below the configuration level, you can enter the following to obtain the help information for a specific parameter:

  parameter ?

The following example shows the help command and output for the ip parameter of a main database:

  <db configure> ip ?

  NAME: ip
  DESCRIPTION: Database IP address accessible to servers
               Default Value [nnn.nnn.nnn.nnn]
               Current Value [nnn.nnn.nnn.nnn]
  USAGE: ip <IP>
3.2.3 Advance creation of configuration files

You can use `samconfig` to create multiple configuration files for subsequent component deployments on other stations.

For example, if you plan to deploy a standalone NFM-P system that includes two auxiliary servers, you create the following files using the parameter values required for each component:

- one main server configuration file
- one main database configuration file
- two auxiliary server configuration files

You can then copy the files to stations in a staging environment for trial purposes, and then subsequently use the files on the stations in a live system when testing is complete.

**Note:** You can create a configuration file for a component only when the RPM packages that the component requires are installed on the component.

**Note:** After you specify a license, keystore, or truststore file using `samconfig`, the associated parameter may display the following:

```
Use Current object File
```

In such a case, before you can apply the file on a different station, you must use `samconfig` on the new station to specify the license, keystore, or truststore file.

3.3 Usage instructions

3.3.1 Opening `samconfig`

**Note:** Using `samconfig` requires root user privileges.

To invoke `samconfig`, you enter one of the following:

- To create and optionally deploy a new component configuration:
  ```bash
  samconfig -m component
  ```
- To open a saved configuration file:
  ```bash
  samconfig -f file
  ```
- To deploy a saved configuration:
  ```bash
  samconfig -f file -apply
  ```
- To display the `samconfig` version information:
  ```bash
  samconfig -version
  ```

where
file is a configuration file created using samconfig

component is one of the following:
• main—main server
• db—main database
• aux—auxiliary server
• flow—NSP Flow Collector

3.3.2 General usage

The following steps describe general samconfig usage; see the samconfig man page for comprehensive usage information.

Note: samconfig has an auto-complete function; pressing the TAB key in the samconfig CLI has the following effects:
• at the prompt—lists the available options
• after one or more characters—completes a matching option name, or lists the possible matches for further refinement

Note: samconfig has a history function; you can cycle through previous commands using the up and down cursor keys, and can search for characters in a previous command by pressing the Page Up key or by entering characters and pressing the Up cursor key.

General usage steps:
1. Enter the following in a console window to open samconfig.
   ```
   # samconfig -m component
   
   The root prompt is displayed:
   <component>
   ```
2. To move to the configuration level, enter the following:
   ```
   <component> configure
   
   The configuration prompt is displayed:
   <component configure>
   ```
3. Perform one of the following.
   a. To configure multiple parameters of an object, enter the following:
      ```
      <component configure> object
      
      The object configuration prompt is displayed:
      <component configure object>
      
      You can then configure one or more parameters by entering the following:
      <component configure object> parameter value
      ```
   b. To configure only one parameter of an object, enter the following:
      ```
      <component configure> object parameter value
      
      samconfig moves to the object configuration level after the parameter is set, as shown below:
c. To enable a Boolean object, for example, the aa-stats object on a main server, enter the following:

```
<component configure> object
```

d. To disable a Boolean object, for example, the aa-stats object on a main server, enter the following:

```
<component configure> no object
```

4. To return to the parent level, enter the following:

```
back
```

5. Repeat steps 3 and 4 to configure additional objects and parameters, as required.

6. Enter the following to exit the configuration level and return to the root level:

```
exit
```

7. Perform one or more of the following, as required.

a. To review only the non-default configuration values, enter the following:

```
<component> show
```

The non-default values are listed.

b. To review the entire configuration, enter the following:

```
<component> show-detail
```

The entire configuration is displayed.

c. To save the configuration using the default filename, such as when you are configuring a component on the local station, enter the following:

```
<component> save
```

The utility backs up the previous configuration file, if any, and displays the following:

```
Backup of existing file saved as: backup_file
Configuration saved as: /opt/nsp/nfmp/samconfig/nms/config/component_config.xml
```

d. To save the configuration to a different file, for example, if you are creating a configuration for component deployment on a separate station, enter the following:

```
<component> save filename
```

**Note:**

If *filename* does not include a relative or absolute path, the file is saved in the /opt/nsp/nfmp/samconfig/nms/config directory:

The following is displayed:

```
Configuration saved as: filename
```

e. To immediately apply the component configuration, enter the following; you can apply a configuration only when the associated component is not running:

```
<component> apply
```

f. To exit samconfig, enter the following:

```
<component> exit
```

Samconfig prompts you to save any unsaved configuration changes, as shown below:

```
Finished processing command line inputs...
Save changes before exiting? (y/n)
```
If you enter y, the following is displayed:

Backup of existing file saved as: backup_file
Configuration saved as:
/opt/nsp/nfmp/samconfig/nms/config/component_config.xml

3.3.3 Usage in procedure steps

Some configuration steps in procedures that require samconfig include a table that lists and
describes the available parameters in an object context. The table provides additional information
and default values, if available.

The table layout facilitates the copying and pasting of parameter names into a CLI, and the last
term in a table title is the name of the object that contains the parameters; for example, the title of
the table in the example below shows that the operator is in the mediation object context.

![Note: If the parameters are at the top configuration level, the table title describes the
parameters as general parameters.

Configuration step example

The following example uses a procedure step from the standalone main server installation
procedure. An operator needs to enable NAT and specify an IPv4 address other than the default for
network management; the remaining parameter defaults are deemed acceptable.

In an earlier step, the operator enters configure at the samconfig prompt to enter the configuration
level. To set the mediation parameters, the operator enters mediation to move to the mediation
object, and then the following configuration commands:

1. nat —enables NAT; to disable NAT, the no nat form is required
2. snmp-ipv4 192.168.3.141 —sets the snmp-ipv4 parameter to a non-default value
3. back —returns the operator to the parent menu, from which the operator can configure other
objects

![Note: To configure only one parameter of an object, you can combine the object, parameter,
and value in one command; for example, configure mediation snmp-ipv4 192.168.3.141.

The following is the step from the installation procedure

27. Configure the mediation parameters in the following table, and then enter back.

Table 3-2  Standalone main server parameters — mediation

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nat</td>
<td>Whether NAT is used between the main server and the managed NEs</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td>snmp-ipv4</td>
<td>The IPv4 address that the managed NEs must use to reach the main server</td>
</tr>
<tr>
<td></td>
<td>Default: IPv4 address of primary network interface</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>snmp-ipv6</td>
<td>The IPv6 address that the managed NEs must use to reach the main server</td>
</tr>
<tr>
<td></td>
<td>Default: IPv6 address of primary network interface</td>
</tr>
<tr>
<td>snmp-port</td>
<td>The TCP port on the main server station that the managed NEs must use to</td>
</tr>
<tr>
<td></td>
<td>reach the main server</td>
</tr>
<tr>
<td></td>
<td>Default: 162</td>
</tr>
<tr>
<td>traplog-id</td>
<td>The SNMP trap log ID associated with the main server</td>
</tr>
<tr>
<td></td>
<td>Default: 98</td>
</tr>
</tbody>
</table>
4 RHEL OS configuration

4.1 Overview

4.1.1 Purpose

This chapter describes the following:

• RHEL OS specifications for NFM-P deployment
• RHEL OS deployment in a VM using a qcow2 image
• manual RHEL OS installation and package requirements

4.1.2 Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 Overview</td>
<td>41</td>
</tr>
<tr>
<td>RHEL OS deployment restrictions and requirements</td>
<td>42</td>
</tr>
<tr>
<td>4.2 Introduction</td>
<td>42</td>
</tr>
<tr>
<td>4.3 RHEL deployment restrictions</td>
<td>42</td>
</tr>
<tr>
<td>4.4 RHEL deployment requirements</td>
<td>43</td>
</tr>
<tr>
<td>4.5 To prepare disk partitions for NFM-P installation</td>
<td>44</td>
</tr>
<tr>
<td>4.6 To reset the disk partition reserved block counts</td>
<td>45</td>
</tr>
<tr>
<td>RHEL OS deployment in a VM</td>
<td>47</td>
</tr>
<tr>
<td>4.7 Introduction</td>
<td>47</td>
</tr>
<tr>
<td>4.8 To deploy the RHEL OS for NFM-P using a qcow2 image</td>
<td>47</td>
</tr>
<tr>
<td>Manual RHEL OS installation</td>
<td>53</td>
</tr>
<tr>
<td>4.9 RHEL OS installation requirements</td>
<td>53</td>
</tr>
<tr>
<td>4.10 Required RHEL environment and OS packages</td>
<td>54</td>
</tr>
<tr>
<td>4.11 Required additional OS packages, auxiliary database</td>
<td>60</td>
</tr>
<tr>
<td>4.12 Required additional OS packages, NSP Flow Collector</td>
<td>61</td>
</tr>
</tbody>
</table>
4.2 Introduction

4.2.1 Description

You must comply with the conditions in Chapter 2, "Before you begin" and the specific requirements in this chapter before you attempt to perform a procedure in this guide on a RHEL station.

Note: See the current NFM-P Release Notice for the required RHEL version and patch information.

Note: It is strongly recommended to install any OS, driver, or firmware update that your hardware vendor advises for RHEL.

Note: It is strongly recommended that you verify the checksum of each software package or file that you download from OLCS. You can compare the checksum value on the download page with, for example, the output of the RHEL md5sum or sha256sum command. See the appropriate RHEL man page for information.

Note: The Bash shell is the supported command shell for RHEL CLI operations.

4.3 RHEL deployment restrictions

4.3.1 Description

The following are the RHEL OS configuration restrictions for NFM-P components.

- The NFM-P supports the use of RHEL IP bonding only when IP bonding is deployed in an active/backup configuration; see the RHEL documentation for IP bonding information.
  
  Note: IP bonding is not supported on an NSP Flow Collector.

- The RHEL SELinux function is not supported; you must disable the function on a station after the OS installation and before you attempt to install an NFM-P component.

- The RHEL TFTP server conflicts with the NFM-P TFTP server, and must be disabled on a main or auxiliary server station.

Note: It is recommended that you create the NFM-P disk partitions during the RHEL OS installation. Each partition created after the OS installation requires additional configuration, as described in 5.4 "To configure an NFM-P disk partition created after the RHEL OS installation" (p. 65).
4.4 RHEL deployment requirements

4.4.1 Description

The following are the RHEL OS configuration requirements for NFM-P components.

<i>Note:</i> Before you deploy an NFM-P component on RHEL in a VM, you must also install the latest VMware Tools software; see the VMware documentation for information.

- The system locale must be POSIX.
- The file system type must be ext4.
- You must choose English (English) as the RHEL OS installation language.
- You must select the “Create custom layout” disk configuration option, and must then create the file system partitions as specified in Chapter 5, “RHEL disk configuration”.
- You must specify the required RHEL packages and package groups listed in “Manual RHEL OS installation” (p. 53) during the RHEL OS installation.
- After the OS installation, you must do the following.
  - Configure each ext4 disk partition with the required options for NFM-P software deployment; see 4.5 “To prepare disk partitions for NFM-P installation” (p. 44).
  - Reset the reserved block count on each NFM-P disk partition; see 4.6 “To reset the disk partition reserved block counts” (p. 45).
- The /etc/hosts entry that maps a main or auxiliary server hostname to an external IP address must be listed above the loopback address entry, and optimally is the first line of the file.
- If XML API clients are to use the registerLogToFile method, you must enable the RHEL FTP, SCP, or SFTP services, as required, and ensure that firewalls allow the file-transfer traffic between the clients and servers.

Using a firewall between components

The following firewall types are supported in an NFM-P system:

- native RHEL firewall implemented using Firewalld
- external firewall

Before you attempt to deploy an NFM-P system, or add a component to a system, you must ensure that any firewalls between the components allow the required traffic to pass between the components, or are disabled. The <i>NSP NFM-P Planning Guide</i> lists the open ports required by each component.

<i>Note:</i> If you intend to use Firewalld, you must configure Firewalld according to the rules in the <i>NSP NFM-P Planning Guide</i>, which describes using NFM-P templates to create Firewalld rules.
4.5 To prepare disk partitions for NFM-P installation

4.5.1 Description

The following steps describe how to configure the disk partitions on a station after a manual RHEL OS installation and before you attempt to install an NFM-P component on the station.

4.5.2 Steps

1. Log in to the station as the root user.

2. Open a console window.

3. Open the /etc/fstab file using a plain-text editor such as vi. The following is an example partition entry:

   ```
   UUID=UUID mount_point type options
   ```

   where

   mount_point is the partition mount point, for example, /opt/nsp/nfmp

4. Perform the following steps for the / and /tmp partition entries.

   1. If the "defaults" option is shown, remove the option.
   2. Insert "barrier=0" to make the entry read as follows:

      ```
      UUID=UUID mount_point ext4 barrier=0 1 1
      ```

5. Perform the following steps for each remaining ext4 partition entry.

   1. If the "defaults" option is shown, remove the option.
   2. For a partition in a physical hardware deployment, insert "barrier=0,noatime" to make the entry read as follows:

      ```
      UUID=UUID mount_point ext4 barrier=0,noatime 1 2
      ```
   3. For a partition in a VM deployment, insert "noatime" to make the entry read as follows:

      ```
      UUID=UUID mount_point ext4 noatime 1 2
      ```

6. Perform one of the following.

   a. If the station is to host an NFM-P main database, perform the following steps.

      1. Locate the tmpfs file system entry.
2. Remove the noexec option so that the entry reads as follows:
   
   `tmpfs /dev/shm tmpfs nodev,nosuid 0 0`

3. Save and close the /etc/fstab file.

4. Enter the following to remount the /dev/shm partition:
   
   `# mount -o remount /dev/shm`

   b. Save and close the /etc/fstab file.

---

**4.6 To reset the disk partition reserved block counts**

**4.6.1 Description**

The following steps describe how to ensure that the number of reserved blocks for the root user on each NFM-P disk partition is zero.

**Note:** You must perform this procedure on each station that hosts one of the following NFM-P system components:

- main server
- auxiliary server
- main database

**4.6.2 Steps**

1.

Log in to the station as the root user.

2.

Open a console window.

3.

Enter the following:

   `# mount | grep nfmp`

   The NFM-P disk partitions are listed; for example:

   `/dev/sda2 on /opt/nsp/nfmp type ext4 (options)`
   `/dev/sda3 on /opt/nsp/nfmp/dbbackup type ext4 (options)`
   `/dev/sdb1 on /opt/nsp/nfmp/db/archivelog type ext4 (options)`
Note: The example lists physical disk partitions, which are named sd xn; a logical partition is named vdx n.

4

Enter the following once for each NFM-P partition:

```
# tune2fs -m 0 /dev/partition
```

where partition is the partition name

5

Close the console window.

END OF STEPS
RHEL OS deployment in a VM

4.7 Introduction

4.7.1 Description

You can install the required RHEL 7 OS for an NFM-P component or NSP module using a qcow2 disk image. The image contains only the RHEL 7 OS, and does not include any product-specific packages or application files.

After you deploy the image as described in 4.8 “To deploy the RHEL OS for NFM-P using a qcow2 image” (p. 47), you can install one of the following in the VM:

- main server
- main database
- collocated main server and database
- auxiliary server
- client delegate server
- single-user client
- NSP modules such as analytics servers, Flow Collectors

Note: Auxiliary database installation is not supported.

Note: The OS installation includes all required and optional packages for a component. See 4.10 “Required RHEL environment and OS packages” (p. 54) for a list of the required and optional packages.

4.8 To deploy the RHEL OS for NFM-P using a qcow2 image

4.8.1 Purpose

This procedure describes how to create one or more RHEL OS instances for the installation of NFM-P components or NSP modules.

4.8.2 Steps

Prepare required images

1. Log in to the VM host station as the root user.

2. Download the following file from OLCS to a local directory on the station:
   - NSP_RHEL7_{yy_mm}.qcow2
   where {yy_mm} represents the year and month of the file issue
Open a console window.

For each VM that you require, enter the following to create a raw VM disk image file:

```
# qemu-img convert -f qcow2 qcow2_file -O raw -S 0 raw_image.img
```

where

- `qcow2_file` is the name of the downloaded qcow2 file
- `raw_image` is the name that you want to assign to the image; for example, NFM-P_Main_Server_A

Perform one of the following:

a. If you want only one disk to contain all OS, product software, and data files on a VM, you must resize the VM disk image in accordance with your Platform Sizing Response for the specific module or component.

   For each one-disk VM that you require, enter the following:

   ```
   # qemu-img resize "raw_image.img" sizeG
   ```

   where

   - `raw_image` is the raw disk image name specified in Step 4
   - `size` is the required disk size, in Gbytes

b. If you want more than one disk in a VM, for example, one for the OS, and one for all main server software and data, or separate disks for specific partitions, you must create a separate raw image for each required disk. The disk size must be in accordance with your Platform Sizing Response for the specific module, component, or partition.

   For each separate disk image that you require, enter the following:

   ```
   # qemu-img create -f raw "raw_image.img" sizeG
   ```

   where

   - `raw_image` is the name that you want to assign to the disk image; for example, NFM-P_Main_Database_A_Complete, for an image that is to contain all main database software and data, or NFM-P_Main_Database_A_Tablespace, for an image that is to contain only the database tablespace partition
   - `size` is the required disk size, in Gbytes

The raw image files that you create in Step 5 are in sparse format; conversion of an image file to non-sparse format provides optimal disk performance.

**Note:** Non-sparse format is strongly recommended for a live system deployment.

For each disk image created in Step 5 that you want to convert to non-sparse format, enter the following:
```
# cp --sparse=never raw_image.img non-sparse_raw_image.img
```

*raw_image* is a raw disk image name specified in Step 5

*non-sparse_raw_image* is the name to assign to the non-sparse image

### Deploy VMs

7

For each VM, enter the following to deploy the VM:

```
# virt-install --connect qemu:///system --ram RAM --vcpu=cores -n instance --os-type=linux --os-variant=rhel7 --disk path="image_1", device=disk, bus=virtio, format=raw, io=native, cache=none --disk path="image_2", device=disk, bus=virtio, format=raw, io=native, cache=none --disk path="image_n", device=disk, bus=virtio, format=raw, io=native, cache=none --network bridge=bridge_name --import
```

*RAM* is the required amount of RAM specified in your Customer Sizing Response

*cores* is the required number of vCPU cores specified in your Customer Sizing Response

*instance* is the name to assign to the VM

*image_1, image_2, and image_n* are the raw disk images created for the VM

*bridge_name* is the name of the network bridge for a VM interface

**Note:** One "--network bridge=bridge_name" entry is required for each VM interface that you intend to configure.

8

Log in to the new VM as the root user; the default password is available from technical support.

9

Configure the RHEL OS as required for the module or component to be installed; for example:

- Plumb the required IPv4 and IPv6 addresses.
- Set the hostname.
- Update the `/etc/hosts` file.

See Chapter 2, "Before you begin", and the appropriate NSP documentation for information.

10

Perform one of the following; see Chapter 5, "RHEL disk configuration" for specific NFM-P disk partitioning information.

**Note:** If you are using multiple disks in a VM, you must mount a parent partition before you mount any child partition. For example, you cannot mount the `/var/log/audit` partition before you mount the `/var/log` partition.

a. If you are using only one disk per VM, perform the following steps for each such VM.
1. Enter the following commands:

   # mkdir -p /extra
   # mkdir -p /opt/nsp

2. Use the RHEL fdisk utility to create the required sub-disks for the following directories:
   - /extra
   - /opt/nsp
   - /var/log
   - /var/log/audit

   For each directory, enter the following and respond to the prompts; specify the directory size from your Platform Sizing Response:

   # fdisk /dev/virtual_device

   where `virtual_device` is the virtual device name, for example, vda in a KVM VM.

3. Enter the following to reboot the VM:

   # systemctl reboot

4. After the reboot, perform one of the following.

   a. If you are using LVM, perform the following steps.
      1. Enter the following sequence of commands for each sub-disk:
         
            # pvcreate /dev/virtual_devicen
            # vgcreate vg2 /dev/virtual_devicen

         where

         virtual_device is the virtual device name, for example, vda in a KVM VM
         n is the number associated with the sub-disk

         2. Go to Step 11.

   b. If you are not using LVM, perform the following steps.
      1. Enter the following for each sub-disk:
         
            # mkfs.ext4 -L path /dev/devicen

         where

         path is the directory path associated with the sub-disk, for example, /opt/nsp
         device is the device name, for example, vda in a KVM VM
         n is the device number associated with the sub-disk

         2. Open the /etc/fstab file using a plain-text editor such as vi.

         3. Add one line in the following format for each sub-disk:

            /dev/virtual_devicen path fs_type defaults 0 0

         where

         device is the device name, for example, vda in a KVM VM
         n is the number associated with the sub-disk
         path is the directory path associated with the sub-disk, for example, /opt/nsp
         fs_type is the file system type, which is ext4 for all sub-disks except /var/log and /var/log/audit, for which it is xfs

         4. Save and close the file.

         5. Enter the following:
# mount -a

6. Go to **Step 12**.

b. If you specify multiple disks per VM and are using LVM, enter the following sequence of commands for each disk in each VM:

```bash
# pvcreate /dev/device
# vgcreate group /dev/device
```

where

- `device` is the device name for the disk
- `group` is the name to assign to the volume group, and must be unique in the VM

### Configure LVM

11

Create the LVM volumes and partitions.

Perform the following steps for each disk in a VM, beginning with the parent disk partitions.

**Note**: If you are using multiple disks in a VM, you must mount a parent partition before you mount any child partition. For example, you cannot mount the `/opt/nspp/nfmp/nebackup` partition before you mount the `/opt/nspp` partition.

1. Enter the following to create a logical volume:

```bash
# lvcreate -n volume -L sizeG group /dev/device
```

where

- `volume` is the name to assign to the logical volume
- `size` is the volume size from your Platform Sizing Response
- `group` is the name to assign to the volume group, and must be unique in the VM
- `device` is the device name

2. Enter the following:

```bash
# mkdir directory
```

where `directory` is the name of the directory to associate with the volume, for example, `/opt/nspp`

3. Enter the following:

```bash
# mkfs.ext4 -L directory /dev/group/volume
```

where

- `directory` is the directory associated with the volume
- `group` is the volume group
- `volume` is the logical volume name

4. Open the `/etc/fstab` file using a plain-text editor such as `vi`.

5. Add an entry in the following format:

```
/dev/group/partition directory fs_type noatime 0 0
```
where

group is the volume group

partition is the partition name

directory is the associated directory path

fs_type is the file system type, which is one of the following:

• ext4, for all partitions except /var/log and /var/log/audit
• xfs, for the /var/log and /var/log/audit partitions

6. Save and close the file.
7. Enter the following:

   # mount -a

**Install and configure product software**

12

As described in Chapter 7, “NFM-P installation” or the NSP documentation, install and configure the product software on the VMs.

**Note:** The /extra partition is allocated for use as a temporary storage location for downloaded product software.

**END OF STEPS**
Manual RHEL OS installation

4.9 RHEL OS installation requirements

4.9.1 Introduction

Each NFM-P component requires the following, as described in 4.10 "Required RHEL environment and OS packages" (p. 54):

- a specific RHEL Software Selection as the base environment
- the installation of specific OS packages

If the required base environment and packages are not installed, a component installation fails.

Depending on the component type, additional packages may be required, as described in 4.11 “Required additional OS packages, auxiliary database” (p. 60) and 4.12 “Required additional OS packages, NSP Flow Collector” (p. 61).

Note: Management of LTE-N devices requires the installation of one or more additional packages. See “NFM-P server configuration tasks” in the NSP NFM-P MultiRadio BTS User Guide for information.

Note: The RHEL rpm utility requires hardware driver files in binary format. If the RHEL driver files provided by your server hardware vendor are in source rpm format, you may need to install additional packages in order to compile the files into binary format. See the station hardware documentation for information.

4.9.2 Using the yum utility

To simplify package management, it is recommended that you use the RHEL yum utility to install and remove OS packages.

The package installation syntax is the following:

```
yum -y install package_1 package_2 ... package_n
```

The package removal syntax is the following:

```
yum -y remove package_1 package_2 ... package_n
```

Note: Package installation using yum requires a yum repository. The following repository types are available:

- local repository, which you can create during the RHEL OS installation
- Internet-based repository, which you can access after you register with the Red Hat Network

See the RHEL documentation for information about setting up a yum repository.

Note: If a package has dependencies on one or more additional packages that are not listed in a table, the yum utility installs the additional packages.
4.10 **Required RHEL environment and OS packages**

4.10.1 **Description**

During the RHEL OS installation for any NFM-P component, you must do the following.

1. Specify "Minimal Install" as the Software Selection in the RHEL installer.
2. Install specific OS packages, as described in 4.10.2 "RHEL OS packages to install" (p. 53).
3. Remove specific OS packages, as described in 4.10.3 "RHEL OS packages to remove" (p. 57).
4. Upgrade or install specific OS packages, as required, depending on the RHEL version; see 4.10.4 "Special RHEL OS package requirements" (p. 59).
5. Depending on the component type, install the required additional OS packages; see 4.11 “Required additional OS packages, auxiliary database” (p. 60) and 4.12 “Required additional OS packages, NSP Flow Collector” (p. 61).
6. Optionally, install one or more packages listed in 4.10.5 "Optional RHEL OS packages" (p. 60).

4.10.2 **RHEL OS packages to install**

You must install a set of RHEL OS packages that are common to each NFM-P component. Most of the packages are available from the RHEL ISO disk image and the default RHEL package repository. The packages are listed in “Required packages, RHEL ISO image or default RHEL repository” (p. 53).

You must also install additional packages that are available only from the RHEL optional package repository. The packages are listed in “Required packages, RHEL optional package repository” (p. 57).

**Required packages, RHEL ISO image or default RHEL repository**

The RHEL ISO image and default package repository each contain the following OS packages that you must install. To facilitate the installation, copy the following command block and paste it in a CLI:

```bash
yum -y install @base @gnome-desktop @legacy-x @x11
yum -y install autofs bc.x86_64 binutils.x86_64 compat-libcap1.x86_64
yum -y install dialog elfutils-libelf-devel.x86_64 elfutils.x86_64
yum -y install firefox.x86_64 ftp gcc.x86_64 gcc-c++.x86_64 glibc.i686
yum -y install glibc.x86_64 glibc-devel.i686 glibc-devel.x86_64
yum -y install gtk2.i686 haproxy.x86_64 hdparm.x86_64 irqbalance.x86_64
yum -y install keepalived.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64
yum -y install libaio-devel.i686 libaio-devel.x86_64 libgcc.i686
yum -y install libgcc.x86_64 libibverbs.x86_64
yum -y install libstdc++.i686 libstdc++.x86_64 libstdc++-devel.i686
yum -y install libstdc++-devel.x86_64 libX11.i686 libX11.x86_64
yum -y install libXrender.i686 libXtst.i686 libXtst.x86_64 lshw.x86_64
yum -y install lsof.x86_64 make.x86_64 man mcelog net-snmp
yum -y install net-snmp-utils ntp numactl-devel.i686
yum -y install numactl-devel.x86_64 openssh.x86_64
yum -y install openssh-askpass.x86_64 openssh-clients.x86_64
```
### yum -y install openssh-server.x86_64 procps rsync.x86_64 tcpdump.x86_64
### yum -y install unzip.x86_64 which xinetd.x86_64 zip.x86_64

#### Table 4-1  Required OS packages from default RHEL repository or ISO image

<table>
<thead>
<tr>
<th>Package</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>@base</td>
<td>Base package group</td>
</tr>
<tr>
<td>@gnome-desktop</td>
<td>Gnome package group</td>
</tr>
<tr>
<td>@legacy-x</td>
<td>Legacy X package group</td>
</tr>
<tr>
<td>@x11</td>
<td>X11 package group</td>
</tr>
<tr>
<td>autos</td>
<td>A tool for automatically mounting and unmounting filesystems</td>
</tr>
<tr>
<td>bc.x86_64</td>
<td>GNU's bc (a numeric processing language) and dc (a calculator)</td>
</tr>
<tr>
<td>binutils.x86_64</td>
<td>A GNU collection of binary utilities</td>
</tr>
<tr>
<td>compat-libcap1.x86_64</td>
<td>Library for getting and setting POSIX.1e capabilities</td>
</tr>
<tr>
<td>dialog</td>
<td>A utility for creating TTY dialog boxes</td>
</tr>
<tr>
<td>elfutils.x86_64</td>
<td>A collection of utilities and DSOs to handle compiled objects</td>
</tr>
<tr>
<td>elfutils-libelf-devel.x86_64</td>
<td>Development support for libelf</td>
</tr>
<tr>
<td>firefox.x86_64</td>
<td>Mozilla Firefox web browser</td>
</tr>
<tr>
<td>ftp</td>
<td>The standard UNIX FTP client</td>
</tr>
<tr>
<td>gcc.x86_64</td>
<td>Various compilers, for example, C, C++, Objective-C, and Java</td>
</tr>
<tr>
<td>gcc-c++.x86_64</td>
<td>C++ support for GCC</td>
</tr>
<tr>
<td>glibc.i686</td>
<td>The GNU libc libraries</td>
</tr>
<tr>
<td>glibc.x86_64</td>
<td>The GNU libc libraries</td>
</tr>
<tr>
<td>glibc-devel.i686</td>
<td>Object files for development using standard C libraries</td>
</tr>
<tr>
<td>glibc-devel.x86_64</td>
<td>Object files for development using standard C libraries</td>
</tr>
<tr>
<td>gtk2.i686</td>
<td>The GIMP ToolKit (GTK+), a library for creating GUIs for X</td>
</tr>
<tr>
<td>haproxy.x86_64</td>
<td>TCP/HTTP proxy and load balancer for high availability environments</td>
</tr>
<tr>
<td>hdparm.x86_64</td>
<td>Utility for displaying and/or setting hard disk parameters</td>
</tr>
<tr>
<td>irqbalance.x86_64</td>
<td>Daemon that evenly distributes IRQ load across multiple CPUs</td>
</tr>
<tr>
<td>keepalived.x86_64</td>
<td>Load balancer and high availability service</td>
</tr>
<tr>
<td>ksh.x86_64</td>
<td>The Original ATT Korn Shell</td>
</tr>
<tr>
<td>libaio.i686</td>
<td>Linux-native asynchronous I/O access library</td>
</tr>
<tr>
<td>libaio.x86_64</td>
<td>Linux-native asynchronous I/O access library</td>
</tr>
<tr>
<td>libaio-devel.i686</td>
<td>Development files for Linux-native asynchronous I/O access</td>
</tr>
<tr>
<td>libaio-devel.x86_64</td>
<td>Development files for Linux-native asynchronous I/O access</td>
</tr>
<tr>
<td>Package</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>libgcc.i686</td>
<td>GCC version 4.8 shared support library</td>
</tr>
<tr>
<td>libgcc.x86_64</td>
<td>GCC version 4.4 shared support library</td>
</tr>
<tr>
<td>libibverbs.x86_64</td>
<td>Core user space library that implements hardware abstracted verbs protocol</td>
</tr>
<tr>
<td>libstdc++.i686</td>
<td>GNU Standard C++ Library</td>
</tr>
<tr>
<td>libstdc++.x86_64</td>
<td>GNU Standard C++ Library</td>
</tr>
<tr>
<td>libstdc++-devel.i686</td>
<td>Header files and libraries for C++ development</td>
</tr>
<tr>
<td>libstdc++-devel.x86_64</td>
<td>Header files and libraries for C++ development</td>
</tr>
<tr>
<td>libXi.i686</td>
<td>X.Org X11 libXi runtime library</td>
</tr>
<tr>
<td>libXi.x86_64</td>
<td>X.Org X11 libXi runtime library</td>
</tr>
<tr>
<td>libXrender.i686</td>
<td>X.Org X11 libXrender runtime library</td>
</tr>
<tr>
<td>libXtst.i686</td>
<td>X.Org X11 libXtst runtime library</td>
</tr>
<tr>
<td>libXtst.x86_64</td>
<td>X.Org X11 libXtst runtime library</td>
</tr>
<tr>
<td>lshw.x86_64</td>
<td>Hardware lister</td>
</tr>
<tr>
<td>lsof.x86_64</td>
<td>Provides a utility to list information about open files</td>
</tr>
<tr>
<td>make.x86_64</td>
<td>GNU tool which simplifies the build process for users</td>
</tr>
<tr>
<td>man</td>
<td>A set of documentation tools: man, apropos and whatis</td>
</tr>
<tr>
<td>mcelog</td>
<td>Tool to translate x86-64 CPU Machine Check Exception data</td>
</tr>
<tr>
<td>net-snmp</td>
<td>SNMP Agent Daemon and documentation</td>
</tr>
<tr>
<td>net-snmp-utils</td>
<td>SNMP clients such as snmppget and snmpwalk</td>
</tr>
<tr>
<td>ntp</td>
<td>The NTP daemon and utilities</td>
</tr>
<tr>
<td>numaclt-devel.i686</td>
<td>Development package for building Applications that use numa</td>
</tr>
<tr>
<td>numaclt-devel.x86_64</td>
<td>Development package for building Applications that use numa</td>
</tr>
<tr>
<td>openssh.x86_64</td>
<td>Open source implementation of SSH protocol versions 1 and 2</td>
</tr>
<tr>
<td>openssh-askpass.x86_64</td>
<td>Passphrase dialog for OpenSSH and X</td>
</tr>
<tr>
<td>openssh-clients.x86_64</td>
<td>Open-source SSH client application</td>
</tr>
<tr>
<td>openssh-server.x86_64</td>
<td>Open source SSH server daemon</td>
</tr>
<tr>
<td>procps</td>
<td>OS utilities for /proc</td>
</tr>
<tr>
<td>rsync.x86_64</td>
<td>A program for synchronizing files over a network</td>
</tr>
<tr>
<td>tcpdump.x86_64</td>
<td>Command-line packet analyzer and network traffic capture; used by technical support for debugging</td>
</tr>
<tr>
<td>unzip.x86_64</td>
<td>A utility for unpacking zip files</td>
</tr>
<tr>
<td>which</td>
<td>Displays where a particular program in your path is located</td>
</tr>
</tbody>
</table>
Table 4-1  Required OS packages from default RHEL repository or ISO image (continued)

<table>
<thead>
<tr>
<th>Package</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>xinetd.x86_64</td>
<td>A secure replacement for inetd</td>
</tr>
<tr>
<td>zip.x86_64</td>
<td>A file compression utility</td>
</tr>
</tbody>
</table>

**Required packages, RHEL optional package repository**

The RHEL optional package repository contains the following OS packages that you must install. To facilitate the installation, copy the following command and paste it in a CLI:

```sh
yum -y install compat-libstdc++-33.i686 compat-libstdc++-33.x86_64
```

Table 4-2  Required OS packages from RHEL optional package repository

<table>
<thead>
<tr>
<th>Package</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>compat-libstdc++-33.i686</td>
<td>Compatibility standard C++ libraries</td>
</tr>
<tr>
<td>compat-libstdc++-33.x86_64</td>
<td>Compatibility standard C++ libraries</td>
</tr>
</tbody>
</table>

**4.10.3  RHEL OS packages to remove**

After you install the required OS packages on a component station, you must remove packages that are installed by default but not required by the NFM-P.

The packages that you remove depend on the RHEL version, as described below.

**RHEL 7.3 or 7.4**

For RHEL 7.3 or 7.4, you must remove the following.

- the packages described in “All RHEL 7 versions” (p. 57)
- the additional packages listed in Table 4-3, “Additional OS packages to remove, RHEL 7.3 or 7.4” (p. 57); to facilitate the package removal, copy the following command and paste it in a CLI:

```sh
yum -y remove NetworkManager.x86_64 NetworkManager-wifi.x86_64
```

Table 4-3  Additional OS packages to remove, RHEL 7.3 or 7.4

<table>
<thead>
<tr>
<th>Package</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetworkManager.x86_64</td>
<td>Network connection manager and user applications</td>
</tr>
<tr>
<td>NetworkManager-wifi.x86_64</td>
<td>Wifi plugin for NetworkManager</td>
</tr>
</tbody>
</table>

**All RHEL 7 versions**

For all RHEL 7 versions, you must remove the packages listed in Table 4-4, “RHEL OS packages to remove, all RHEL versions” (p. 58). To facilitate the package removal, copy the following command block and paste it in a CLI:

```sh
yum -y remove anaconda-core.x86_64 anaconda-gui.x86_64
```
yum -y remove anaconda-tui.x86_64 avahi.x86_64 biosdevname
yum -y remove dnsmasq.x86_64 gnome-boxes.x86_64
yum -y remove initial-setup.x86_64 initial-setup-gui.x86_64
yum -y remove libstoragemgmt.x86_64 libstoragemgmt-python.noarch
yum -y remove libvirt-daemon-config-network.x86_64
yum -y remove libvirt-daemon-driver-network.x86_64
yum -y remove libvirt-daemon-driver-qemu.x86_64
yum -y remove libvirt-daemon-kvm.x86_64 libvirt-gconfig.x86_64
yum -y remove libvirt-gobject.x86_64
yum -y remove NetworkManager-libreswan.x86_64
yum -y remove NetworkManager-libreswan-gnome.x86_64
yum -y remove NetworkManager-team.x86_64 NetworkManager-tui.x86_64
yum -y remove qemu-kvm.x86_64 qemu-kvm-common.x86_64
yum -y remove setroubleshoot.x86_64 setroubleshoot-plugins.noarch
yum -y remove setroubleshoot-server.x86_64
yum -y remove subscription-manager-initial-setup-addon.x86_64

Table 4-4  RHEL OS packages to remove, all RHEL versions

<table>
<thead>
<tr>
<th>Package</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>anaconda-core.x86_64</td>
<td>Core of the Anaconda installer</td>
</tr>
<tr>
<td>anaconda-gui.x86_64</td>
<td>Graphical user interface for the Anaconda installer</td>
</tr>
<tr>
<td>anaconda-tui.x86_64</td>
<td>Textual user interface for the Anaconda installer</td>
</tr>
<tr>
<td>avahi.x86_64</td>
<td>Local network service discovery</td>
</tr>
<tr>
<td>biosdevname</td>
<td>Utility that provides an optional convention for naming network interfaces</td>
</tr>
<tr>
<td>dnsmasq.x86_64</td>
<td>A lightweight DHCP/caching DNS server</td>
</tr>
<tr>
<td>gnome-boxes.x86_64</td>
<td>A simple GNOME 3 application to access remote or virtual systems</td>
</tr>
<tr>
<td>initial-setup.x86_64</td>
<td>Initial system configuration utility</td>
</tr>
<tr>
<td>initial-setup-gui.x86_64</td>
<td>Graphical user interface for the initial-setup utility</td>
</tr>
<tr>
<td>libstoragemgmt.x86_64</td>
<td>Storage array management library</td>
</tr>
<tr>
<td>libstoragemgmt-python.noarch</td>
<td>Python2 client libraries and plug-in support for libstoragemgmt</td>
</tr>
<tr>
<td>libvirt-daemon-config-network.x86_64</td>
<td>Default configuration files for the libvirtd daemon</td>
</tr>
<tr>
<td>libvirt-daemon-driver-network.x86_64</td>
<td>Network driver plugin for the libvirtd daemon</td>
</tr>
<tr>
<td>libvirt-daemon-driver-qemu.x86_64</td>
<td>Qemu driver plugin for the libvirtd daemon</td>
</tr>
<tr>
<td>libvirt-daemon-kvm.x86_64</td>
<td>Server side daemon &amp; driver required to run KVM guests</td>
</tr>
<tr>
<td>libvirt-gconfig.x86_64</td>
<td>libvirt object APIs for processing object configuration</td>
</tr>
<tr>
<td>libvirt-gobject.x86_64</td>
<td>libvirt object APIs for managing virtualization hosts</td>
</tr>
<tr>
<td>NetworkManager-libreswan.x86_64</td>
<td>NetworkManager VPN plugin for libreswan</td>
</tr>
<tr>
<td>NetworkManager-libreswan-gnome.x86_64</td>
<td>NetworkManager VPN plugin for libreswan - GNOME files</td>
</tr>
</tbody>
</table>
Table 4-4  RHEL OS packages to remove, all RHEL versions  (continued)

<table>
<thead>
<tr>
<th>Package</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetworkManager-team.x86_64</td>
<td>Team device plugin for NetworkManager</td>
</tr>
<tr>
<td>NetworkManager-tui.x86_64</td>
<td>NetworkManager curses-based UI</td>
</tr>
<tr>
<td>qemu-kvm.x86_64</td>
<td>QEMU metapackage for KVM support</td>
</tr>
<tr>
<td>qemu-kvm-common.x86_64</td>
<td>QEMU common files needed by all QEMU targets</td>
</tr>
<tr>
<td>setroubleshoot.x86_64</td>
<td>Helps troubleshoot SELinux problem</td>
</tr>
<tr>
<td>setroubleshoot-plugins.noarch</td>
<td>Analysis plugins for use with setroubleshoot</td>
</tr>
<tr>
<td>setroubleshoot-server.x86_64</td>
<td>SELinux troubleshoot server</td>
</tr>
<tr>
<td>subscription-manager-initial-setup-addon.x86_64</td>
<td>Initial setup screens for subscription manager</td>
</tr>
</tbody>
</table>

4.10.4 Special RHEL OS package requirements

The NFM-P requires specific versions of some packages, as described in “Specific package version requirements” (p. 59), and requires the installation of specific packages after an upgrade to RHEL 7.5, as described in “Upgrading to RHEL 7.5” (p. 59).

Specific package version requirements

The NFM-P requires the version of each RHEL 7 package quoted in Table 4-5, “Required RHEL OS package versions” (p. 59), or a later version. After the initial OS installation, if a listed package version is lower than the minimum required, you must upgrade the package.

Table 4-5  Required RHEL OS package versions

<table>
<thead>
<tr>
<th>Package</th>
<th>Minimum version required</th>
</tr>
</thead>
<tbody>
<tr>
<td>nspr.x86_64</td>
<td>4.19.0-1.el7</td>
</tr>
<tr>
<td>nss-softokn-freebl.i686</td>
<td>3.36.0-5.el7</td>
</tr>
<tr>
<td>nss-softokn-freebl.x86_64</td>
<td>3.36.0-5.el7</td>
</tr>
<tr>
<td>nss-softokn.x86_64</td>
<td>3.36.0-5.el7</td>
</tr>
<tr>
<td>nss-softokn.x86_64</td>
<td>3.36.0-1.el7</td>
</tr>
</tbody>
</table>

Upgrading to RHEL 7.5

If you upgrade from RHEL 7.3 or 7.4 to RHEL 7.5, you must install the packages listed in Table 4-6, “Additional OS packages required after upgrade to RHEL 7.5” (p. 59).

Table 4-6  Additional OS packages required after upgrade to RHEL 7.5

<table>
<thead>
<tr>
<th>Package</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetworkManager.x86_64</td>
<td>Network connection manager and user applications</td>
</tr>
</tbody>
</table>
### Additional OS packages required after upgrade to RHEL 7.5 (continued)

<table>
<thead>
<tr>
<th>Package</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetworkManager-wifi.x86_64</td>
<td>Wifi plugin for NetworkManager</td>
</tr>
</tbody>
</table>

### Optional RHEL OS packages

Table 4-7, "Optional RHEL OS packages" (p. 60) lists the optional packages that you can install for any component. To facilitate the package installation, copy the following command and paste it in a CLI:

```bash
yum -y install nfs-utils telnet.x86_64 vsftpd.x86_64
```

### Required additional OS packages, auxiliary database

#### Description

Table 4-8, "Required additional OS packages, auxiliary database" (p. 60) lists the OS packages that are required, in addition to the base package set, for an NFM-P auxiliary database. To facilitate the package installation, copy the following command line and paste it in a CLI:

```bash
yum -y install bash chrony gdb grubby.x86_64 sysstat.x86_64 tzdata
```

### Required additional OS packages, auxiliary database

<table>
<thead>
<tr>
<th>Package</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bash</td>
<td>The GNU Bourne Again shell</td>
</tr>
<tr>
<td>chrony</td>
<td>An NTP client/server</td>
</tr>
<tr>
<td>gdb</td>
<td>A stub package for GNU source-level debugger</td>
</tr>
<tr>
<td>grubby.x86_64</td>
<td>Command-line tool for updating bootloader configs</td>
</tr>
<tr>
<td>sysstat.x86_64</td>
<td>Collection of performance monitoring tools for Linux</td>
</tr>
<tr>
<td>tzdata</td>
<td>Timezone data</td>
</tr>
</tbody>
</table>
4.12 Required additional OS packages, NSP Flow Collector

4.12.1 Description

Table 4-9, “Required additional OS packages, NSP Flow Collector” (p. 60) lists the OS packages that are required, in addition to the base package set, for an NSP Flow Collector. To facilitate the package installation, copy the following command block and paste it in a CLI:

```bash
yum -y install bash sysstat.x86_64 unzip
```

Table 4-9 Required additional OS packages, NSP Flow Collector

<table>
<thead>
<tr>
<th>Package</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bash</td>
<td>The GNU Bourne Again shell</td>
</tr>
<tr>
<td>sysstat.x86_64</td>
<td>Collection of performance monitoring tools for Linux</td>
</tr>
<tr>
<td>unzip</td>
<td>A utility for unpacking zip files</td>
</tr>
</tbody>
</table>
RHEL OS configuration
Manual RHEL OS installation
Required additional OS packages, NSP Flow Collector
5 RHEL disk configuration

5.1 Overview

5.1.1 Purpose
This chapter describes the disk configuration and partitioning requirements for NFM-P components in trial and live deployments.

5.1.2 Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 Overview</td>
<td>63</td>
</tr>
<tr>
<td>5.2 Introduction</td>
<td>63</td>
</tr>
<tr>
<td>5.3 Sizing the NE configuration backup partition</td>
<td>64</td>
</tr>
<tr>
<td>5.4 To configure an NFM-P disk partition created after the RHEL OS installation</td>
<td>65</td>
</tr>
<tr>
<td>5.5 Disk partitioning for trial deployments</td>
<td>67</td>
</tr>
<tr>
<td>5.6 Disk partitioning for live deployments</td>
<td>73</td>
</tr>
</tbody>
</table>

5.2 Introduction

5.2.1 General information
If the NFM-P is to perform large-scale statistics collection, you must implement high-performance disk throughput using one of the following:

- internal disks in a hardware RAID 0 configuration
- external disks in a hardware RAID 0 or RAID 1+0 configuration
- SAN storage

**Note:** An NFM-P disk subsystem requires read and write caching with fault protection.

**Note:** It is recommended that you create disk partitions during the RHEL OS installation. A partition created after the OS installation requires additional configuration, as described in 5.4 “To configure an NFM-P disk partition created after the RHEL OS installation” (p. 65).

You can determine the number of disks required for high-performance throughput by submitting an NFM-P Platform Sizing Request. See the *NSP NFM-P Planning Guide* for scaling guidelines related to statistics collection. Contact technical support for information about using a disk array.
5.2.2 RAID and the NFM-P

**CAUTION**

**Service Disruption**

An improper RAID configuration may result in throughput degradation or failure.

RAID in an NFM-P deployment is supported only when implemented as described in this guide and in the NSP NFM-P Planning Guide. You must strictly follow the RAID specifications in the NSP NFM-P Planning Guide before you attempt to install, upgrade, or convert an NFM-P system. Contact technical support for more information.

A RAID implementation for the NFM-P requires a hardware RAID controller that can create and manage the required number of volumes.

For optimal performance, an NFM-P station requires the recommended number of disks configured in a striping, or RAID 0, volume. A single RAID 0 disk failure can cause a complete file system failure, so for live deployments, disk mirroring using a RAID 1+0 configuration is recommended for greater resiliency and to reduce the recovery time after a disk failure.

**Note:** The use of software RAID is not supported.

**Note:** The installation, administration, and recovery of RAID in an NFM-P system are the responsibility of the owner of the system.

5.2.3 Logical disk management

Logical disk implementation is supported using the LVM function according to the NSP NFM-P Planning Guide specifications.

**Note:** LVM is supported only for resizing disk partitions, and not for creating software RAID volumes. See the NSP NFM-P Planning Guide for information about the LVM features that are supported in an NFM-P deployment.

**Note:** Before you use LVM to resize a partition, you must ensure that the throughput and latency of the new configuration are within the allowed NFM-P tolerances. See “To test NFM-P disk performance” in the NSP NFM-P System Administrator Guide for information about performing the required check.

5.3 Sizing the NE configuration backup partition

5.3.1 Description

Each NFM-P main server stores NE configuration backups on the local file system in the following partition:

```
/opt/nsp/nfmp/nebackup
```

The partition size is specific to an NFM-P system, and is based on the following:

- number of managed NEs
To configure an NFM-P disk partition created after the RHEL OS installation

5.4 To configure an NFM-P disk partition created after the RHEL OS installation

5.4.1 Description
Perform this procedure on each NFM-P disk partition that you create after the RHEL OS installation.
CAUTION

Service Disruption

This procedure requires a restart of the station that hosts the partition.
If an NFM-P component is installed on the station, you must perform the procedure only during a scheduled maintenance period.

Note: The Bash shell is the supported command shell for RHEL CLI operations.

5.4.2 Steps

1. Log into the NFM-P station as the root user.

2. Open a console window.

3. Mount the partition; see the RHEL OS documentation for information.

4. Enter the following:
   
   `# tune2fs -m 0 -o +acl /dev/device`

   where `device` is the name of the device associated with the partition

5. Open the `/etc/fstab` file using a plain-text editor such as `vi`.

6. Perform one of the following.
   a. For a partition in a physical hardware deployment, add the following entry:
      
      `/dev/device mount_point ext4 barrier=0, noatime 1 2`
   b. For a partition in a VM deployment, add the following entry:
      
      `/dev/device mount_point ext4 noatime 1 2`

   where
   `device` is the name of the device associated with the partition
   `mount_point` is the partition mount point, for example, `/opt/nsp/nfmp`

7. Save and close the `/etc/fstab` file.
Enter the following to reboot the station:

```bash
# systemctl reboot
```

The station reboots.

---

5.5 Disk partitioning for trial deployments

5.5.1 Description

**CAUTION**

Service Disruption

*Each disk partition described in this section must be a mounted partition and not a symbolic link. The NFM-P does not support the use of symbolic links to represent partitions.*

The following disk layouts are supported only for trial deployments in a lab environment, or for demonstration purposes.

**Note:** See the *NSP NFM-P Planning Guide* or the response to your NFM-P Platform Sizing Request for information about the supported disk types.

**Note:** For each database partitioning scheme, the Oracle management user home directory specified by the ORACLE_HOME environment variable is `/opt/nsp/nfmp/oracle12r1`.

The following table lists the partitions required for the trial deployment of a collocated main database and main server.

**Table 5-2**  Trial partitioning scheme, collocated main server and database

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>Size (Gbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>swap</td>
<td>Swap space</td>
<td>16</td>
</tr>
<tr>
<td>/</td>
<td>Root</td>
<td>26</td>
</tr>
<tr>
<td>/home</td>
<td>User home directories</td>
<td>0.5</td>
</tr>
<tr>
<td>/tmp</td>
<td>Temporary files</td>
<td>4</td>
</tr>
<tr>
<td>/var</td>
<td>System data</td>
<td>14</td>
</tr>
<tr>
<td>/var/log</td>
<td>System data</td>
<td>6</td>
</tr>
<tr>
<td>/var/log/audit</td>
<td>System data</td>
<td>6</td>
</tr>
</tbody>
</table>

---

Release 18.9
September 2018
Issue 1
Table 5-2  Trial partitioning scheme, collocated main server and database (continued)

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>Size (Gbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>/opt/nspp</td>
<td>NSP and NFM-P software, operating data</td>
<td>50 ¹</td>
</tr>
<tr>
<td>/opt/nspp/dbbackup</td>
<td>Database backups</td>
<td>35</td>
</tr>
<tr>
<td>/opt/nspp/nfmp/nebackup</td>
<td>NE configuration backups</td>
<td>Network-specific ²</td>
</tr>
<tr>
<td>/opt/nspp/db</td>
<td>Database tablespaces</td>
<td>90</td>
</tr>
<tr>
<td>/opt/nspp/nfmp/db/archivelog</td>
<td>Database archive logs</td>
<td>35</td>
</tr>
<tr>
<td>/opt/nspp/nfmp/server/nms/log</td>
<td>NFM-P server log files</td>
<td>15</td>
</tr>
<tr>
<td>/opt/nspp/nfmp/server/xml_output</td>
<td>Output of XML API file export operations</td>
<td>10</td>
</tr>
<tr>
<td>/opt/nspp/os</td>
<td>NSP system files</td>
<td>30</td>
</tr>
<tr>
<td>/extra</td>
<td>NSP and NFM-P software storage</td>
<td>50</td>
</tr>
</tbody>
</table>

Notes:
1. CMM PM statistics may require additional storage space, depending on the collection volume and retention period; contact CMM technical support to define your PM storage requirement, which must be added to the listed partition size
2. Derived using the formula in 5.3 “Sizing the NE configuration backup partition” (p. 64)

The following table lists the partitions required for the trial deployment of a main server in a distributed NFM-P system.

Table 5-3  Trial partitioning scheme, main server, distributed system

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>Size (Gbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>swap</td>
<td>Swap space</td>
<td>16</td>
</tr>
<tr>
<td>/</td>
<td>Root</td>
<td>26</td>
</tr>
<tr>
<td>/home</td>
<td>User home directories</td>
<td>0.5</td>
</tr>
<tr>
<td>/tmp</td>
<td>Temporary files</td>
<td>4</td>
</tr>
<tr>
<td>/var</td>
<td>System data</td>
<td>14</td>
</tr>
<tr>
<td>/var/log</td>
<td>System logs</td>
<td>6</td>
</tr>
<tr>
<td>/var/log/audit</td>
<td>System audit logs</td>
<td>6</td>
</tr>
<tr>
<td>/opt/nspp</td>
<td>Main server software, operating data</td>
<td>70 ¹</td>
</tr>
<tr>
<td>/opt/nspp/nfmp/nebackup</td>
<td>NE configuration backups</td>
<td>Network-specific ²</td>
</tr>
<tr>
<td>/opt/nspp/nfmp/server/nms/log</td>
<td>NFM-P server log files</td>
<td>15</td>
</tr>
</tbody>
</table>
Table 5-3  Trial partitioning scheme, main server, distributed system  (continued)

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>Size (Gbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>/opt/nsp/nfmp/server/xml_output</td>
<td>Output of XML API file export operations</td>
<td>10</td>
</tr>
<tr>
<td>/opt/nsp/os</td>
<td>NSP system files</td>
<td>40</td>
</tr>
<tr>
<td>/extra</td>
<td>NSP and NFM-P software storage</td>
<td>50</td>
</tr>
</tbody>
</table>

Notes:

1. CMM PM statistics may require additional storage space, depending on the collection volume and retention period; contact CMM technical support to define your PM storage requirement, which must be added to the listed partition size.

2. Derived using the formula in 5.3 “Sizing the NE configuration backup partition” (p. 64)

The following table lists the partitions required for the trial deployment of a main database in a distributed NFM-P system.

Table 5-4  Trial partitioning scheme, main database, distributed system

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>Size (Gbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>swap</td>
<td>Swap space</td>
<td>16</td>
</tr>
<tr>
<td>/</td>
<td>Root</td>
<td>26</td>
</tr>
<tr>
<td>/home</td>
<td>User home directories</td>
<td>0.5</td>
</tr>
<tr>
<td>/tmp</td>
<td>Temporary files</td>
<td>4</td>
</tr>
<tr>
<td>/var</td>
<td>System data</td>
<td>14</td>
</tr>
<tr>
<td>/var/log</td>
<td>System logs</td>
<td>6</td>
</tr>
<tr>
<td>/var/log/audit</td>
<td>System audit logs</td>
<td>6</td>
</tr>
<tr>
<td>/opt/nsp/nfmp</td>
<td>Main database software</td>
<td>40</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/dbbackup</td>
<td>Database backups</td>
<td>40</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/db</td>
<td>Database tablespaces</td>
<td>100</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/db/archivelog</td>
<td>Database archive logs</td>
<td>40</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/db/redolog</td>
<td>Database redo logs</td>
<td>8</td>
</tr>
<tr>
<td>/extra</td>
<td>NSP and NFM-P software storage</td>
<td>50</td>
</tr>
</tbody>
</table>

The following table lists the partitions required for the trial deployment of an auxiliary server that is to collect statistics.
### Table 5-5  Trial partitioning scheme, statistics-collection auxiliary server

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>One disk</th>
<th>Two disks</th>
</tr>
</thead>
<tbody>
<tr>
<td>swap</td>
<td>Swap space</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>/</td>
<td>Root</td>
<td>26</td>
<td></td>
</tr>
<tr>
<td>/home</td>
<td>User home directories</td>
<td>0.5</td>
<td></td>
</tr>
<tr>
<td>/tmp</td>
<td>Temporary files</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>/var</td>
<td>System data</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>/var/log</td>
<td>System logs</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>/var/log/audit</td>
<td>System audit logs</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>/opt/nsp</td>
<td>NFM-P server software, operating data</td>
<td>40</td>
<td>90</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/auxserver/nms/log</td>
<td>NFM-P server log files</td>
<td>20</td>
<td>30</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/auxserver/xml_output</td>
<td>Output of XML API file export operations</td>
<td>10</td>
<td>20</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/lte</td>
<td>Collected wireless core statistics files</td>
<td>20</td>
<td>60</td>
</tr>
<tr>
<td>/extra</td>
<td>NSP and NFM-P software storage</td>
<td>50</td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**
1. Required only if wireless core NE statistics are to be collected
2. CMM PM statistics may require additional storage space, depending on the collection volume and retention period; contact CMM technical support to define your PM storage requirement, which must be added to the listed partition size

The following table lists the partitions required for the trial deployment of an auxiliary server that is to collect call-trace data.

### Table 5-6  Trial partitioning scheme, call-trace auxiliary server

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>Size (Gbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>swap</td>
<td>Swap space</td>
<td>16</td>
</tr>
<tr>
<td>/</td>
<td>Root</td>
<td>26</td>
</tr>
<tr>
<td>/home</td>
<td>User home directories</td>
<td>0.5</td>
</tr>
<tr>
<td>/tmp</td>
<td>Temporary files</td>
<td>4</td>
</tr>
<tr>
<td>/var</td>
<td>System data</td>
<td>14</td>
</tr>
<tr>
<td>/var/log</td>
<td>System logs</td>
<td>6</td>
</tr>
<tr>
<td>/var/log/audit</td>
<td>System audit logs</td>
<td>6</td>
</tr>
<tr>
<td>/opt/nsp</td>
<td>NFM-P server software, operating data</td>
<td>40</td>
</tr>
</tbody>
</table>
The following table lists the partitions required for the trial deployment of an auxiliary server that is to collect PCMD records.

**Table 5-7**  Trial partitioning scheme, PCMD auxiliary server

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>Size (Gbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>swap</td>
<td>Swap space</td>
<td>16</td>
</tr>
<tr>
<td>/</td>
<td>Root</td>
<td>26</td>
</tr>
<tr>
<td>/home</td>
<td>User home directories</td>
<td>0.5</td>
</tr>
<tr>
<td>/tmp</td>
<td>Temporary files</td>
<td>4</td>
</tr>
<tr>
<td>/var</td>
<td>System data</td>
<td>14</td>
</tr>
<tr>
<td>/var/log</td>
<td>System logs</td>
<td>6</td>
</tr>
<tr>
<td>/var/log/audit</td>
<td>System audit logs</td>
<td>6</td>
</tr>
<tr>
<td>/opt/nsp</td>
<td>NFM-P server software, operating data</td>
<td>40</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/auxserver/nms/log</td>
<td>NFM-P server log files</td>
<td>20</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/pcmd_output</td>
<td>PCMD output</td>
<td>100</td>
</tr>
<tr>
<td>/extra</td>
<td>NSP and NFM-P software storage</td>
<td>50</td>
</tr>
</tbody>
</table>

The following table lists the partitions required for the trial deployment of an NSP Flow Collector.

**Table 5-8**  Trial partitioning scheme, NSP Flow Collector

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>Size (Gbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>swap</td>
<td>Swap space</td>
<td>16</td>
</tr>
<tr>
<td>/</td>
<td>Root</td>
<td>26</td>
</tr>
<tr>
<td>/home</td>
<td>User home directories</td>
<td>0.5</td>
</tr>
<tr>
<td>/tmp</td>
<td>Temporary files</td>
<td>4</td>
</tr>
<tr>
<td>/var</td>
<td>System data</td>
<td>14</td>
</tr>
<tr>
<td>/var/log</td>
<td>System logs</td>
<td>6</td>
</tr>
</tbody>
</table>
Table 5-8  Trial partitioning scheme, NSP Flow Collector  (continued)

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>Size (Gbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>/var/log/audit</td>
<td>System audit logs</td>
<td>6</td>
</tr>
<tr>
<td>/opt/nsp</td>
<td>Auxiliary server software, operating data</td>
<td>20</td>
</tr>
<tr>
<td>/opt/nsp/flow/dcp_data</td>
<td>Collected statistics data files</td>
<td>57</td>
</tr>
<tr>
<td>/extra</td>
<td>NSP and NFM-P software storage</td>
<td>50</td>
</tr>
</tbody>
</table>

Disks required: one 300-Gbyte or larger

The following table lists the partitions required for the trial deployment of an auxiliary database.

Table 5-9  Trial partitioning scheme, auxiliary database

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>Size (Gbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>swap</td>
<td>Swap space</td>
<td>16</td>
</tr>
<tr>
<td>/</td>
<td>Root</td>
<td>26</td>
</tr>
<tr>
<td>/home</td>
<td>User home directories</td>
<td>0.5</td>
</tr>
<tr>
<td>/opt</td>
<td>NFM-P auxiliary database software</td>
<td>49</td>
</tr>
<tr>
<td>/tmp</td>
<td>Temporary files</td>
<td>4</td>
</tr>
<tr>
<td>/var</td>
<td>System data</td>
<td>14</td>
</tr>
<tr>
<td>/var/log</td>
<td>System logs</td>
<td>6</td>
</tr>
<tr>
<td>/var/log/audit</td>
<td>System audit logs</td>
<td>6</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/auxdb/data</td>
<td>Auxiliary database data</td>
<td>400</td>
</tr>
<tr>
<td>/extra</td>
<td>NSP and NFM-P software storage</td>
<td>50</td>
</tr>
</tbody>
</table>

Optional storage

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>Size (Gbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>/opt/nsp/nfmp/auxdb/backup</td>
<td>Auxiliary database backup</td>
<td>Equal to /opt/nsp/nfmp/auxdb/data</td>
</tr>
</tbody>
</table>

Notes:

1. For multi-station auxiliary database, or single-station deployment with high data rate, remote mount point and 10 Gb/s link recommended

   The following table lists the partitions required for the trial deployment of a single-user client or client delegate server on RHEL.
Table 5-10  Trial partitioning scheme, single-user client or client delegate server

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>Size (Gbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>Swap space</td>
<td>16</td>
</tr>
<tr>
<td>/</td>
<td>Root, including /usr and /var</td>
<td>26</td>
</tr>
<tr>
<td>/opt/nsp</td>
<td>NFM-P client software</td>
<td>16</td>
</tr>
<tr>
<td>At operator discretion</td>
<td>Customer data; can be partitioned according to customer requirements</td>
<td>Remainder</td>
</tr>
</tbody>
</table>

5.6  Disk partitioning for live deployments

5.6.1  Description

CAUTION

![Service Disruption](image)

Each disk partition described in this section must be a mounted partition and not a symbolic link. The NFM-P does not support the use of symbolic links to represent partitions.

The following disk layouts are for a deployment in a live network environment.

Note: See the NSP NFM-P Planning Guide or the response to your NFM-P Platform Sizing Request for information about the supported disk types.

Note: For each database partitioning scheme, the Oracle management user home directory specified by the ORACLE_HOME environment variable is /opt/nsp/nfmp/oracle12r1.

The following table lists the partitions required for the live deployment of a collocated main database and main server.

Table 5-11  Live partitioning scheme, collocated main server and database

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>Physical</th>
<th>qcow2</th>
</tr>
</thead>
<tbody>
<tr>
<td>swap</td>
<td>Swap space</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>/</td>
<td>Root</td>
<td>26</td>
<td></td>
</tr>
<tr>
<td>/home</td>
<td>User home directories</td>
<td>0.5</td>
<td></td>
</tr>
<tr>
<td>/tmp</td>
<td>Temporary files</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>/var</td>
<td>System data</td>
<td>14</td>
<td></td>
</tr>
</tbody>
</table>

RHEL disk configuration
Disk partitioning for live deployments

NFM-P
Table 5-11  Live partitioning scheme, collocated main server and database  (continued)

Disks required:
• Physical deployment—four 300-Gbyte (RAID 0) or eight 300-Gbyte (RAID 1+0)
• qcow2 deployment—minimum of 558 Gbytes, plus calculated /opt/nsp/nfmp/nfmp/nebackup partition size

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>Size (Gbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Physical</td>
</tr>
<tr>
<td>/var/log</td>
<td>System data</td>
<td>6</td>
</tr>
<tr>
<td>/var/log/audit</td>
<td>System data</td>
<td>6</td>
</tr>
<tr>
<td>/opt/nsp</td>
<td>NSP and NFM-P software, operating data</td>
<td>150 ¹</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/db</td>
<td>Main database software, tablespaces</td>
<td>360</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/db/archivelog</td>
<td>Database archive logs</td>
<td>120</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/db.backup</td>
<td>Main database backup sets</td>
<td>120</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/nebackup</td>
<td>NE configuration backup files</td>
<td>Network-specific ²</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/server/nms/log</td>
<td>NFM-P server log files</td>
<td>50</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/server/xml_output</td>
<td>Output of XML API file export operations</td>
<td>20</td>
</tr>
<tr>
<td>/opt/nsp/os</td>
<td>NSP system files</td>
<td>90</td>
</tr>
<tr>
<td>/extra</td>
<td>NSP and NFM-P software storage</td>
<td>50</td>
</tr>
</tbody>
</table>

Notes:
1. CMM PM statistics may require additional storage space, depending on the collection volume and retention period; contact CMM technical support to define your PM storage requirement, which must be added to the listed partition size

2. Derived using the formula in 5.3 “Sizing the NE configuration backup partition” (p. 64)

The following table lists the partitions required for the live deployment of a main server in a distributed NFM-P system.

Table 5-12  Live partitioning scheme, main server, distributed system

Disks required: two 300-Gbyte (RAID 0)

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>Size (Gbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>swap</td>
<td>Swap space</td>
<td>16</td>
</tr>
<tr>
<td>/</td>
<td>Root</td>
<td>26</td>
</tr>
<tr>
<td>/home</td>
<td>User home directories</td>
<td>0.5</td>
</tr>
<tr>
<td>/tmp</td>
<td>Temporary files</td>
<td>4</td>
</tr>
<tr>
<td>/var</td>
<td>System data</td>
<td>14</td>
</tr>
<tr>
<td>/var/log</td>
<td>System logs</td>
<td>6</td>
</tr>
<tr>
<td>/var/log/audit</td>
<td>System audit logs</td>
<td>6</td>
</tr>
<tr>
<td>/opt/nsp</td>
<td>Main server software, operating data</td>
<td>150 ¹</td>
</tr>
</tbody>
</table>
Table 5-12  Live partitioning scheme, main server, distributed system  (continued)

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>Size (Gbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>/opt/nsp/nfmp/nebackup</td>
<td>NE configuration backups</td>
<td>Network-specific ²</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/server/nms/log</td>
<td>NFM-P server log files</td>
<td>50</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/server/xml_output</td>
<td>Output of XML API file export operations</td>
<td>20</td>
</tr>
<tr>
<td>/opt/nsp/os</td>
<td>NSP system files</td>
<td>90</td>
</tr>
<tr>
<td>/extra</td>
<td>NSP and NFM-P software storage</td>
<td>50</td>
</tr>
</tbody>
</table>

Notes:
1. CMM PM statistics may require additional storage space, depending on the collection volume and retention period; contact CMM technical support to define your PM storage requirement, which must be added to the listed partition size.
2. Derived using the formula in 5.3 “Sizing the NE configuration backup partition” (p. 64)

The following table lists the partitions required for the live deployment of a main database in a distributed NFM-P system.

Table 5-13  Live partitioning scheme, main database, distributed system

<table>
<thead>
<tr>
<th>Partition</th>
<th>Size (Gbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>swap</td>
<td>Swap space</td>
</tr>
<tr>
<td>/</td>
<td>Root</td>
</tr>
<tr>
<td>/home</td>
<td>User home directories</td>
</tr>
<tr>
<td>/tmp</td>
<td>Temporary files</td>
</tr>
<tr>
<td>/var</td>
<td>System data</td>
</tr>
<tr>
<td>/var/log</td>
<td>System logs</td>
</tr>
<tr>
<td>/var/log/audit</td>
<td>System audit logs</td>
</tr>
<tr>
<td>/opt/nsp/nfmp</td>
<td>Main database software</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/dbbackup</td>
<td>Database backups</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/db</td>
<td>Database tablespaces</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/db/archivelog</td>
<td>Database archive logs</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/db/redolog</td>
<td>Database redo logs</td>
</tr>
<tr>
<td>/extra</td>
<td>NSP and NFM-P software storage</td>
</tr>
</tbody>
</table>

The following table lists the partitions required for the live deployment of an auxiliary server that is to collect statistics.
Table 5-14  Live partitioning scheme, statistics-collection auxiliary server

<table>
<thead>
<tr>
<th>Disks required: four 300-Byte (RAID 0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partition</td>
</tr>
<tr>
<td>swap</td>
</tr>
<tr>
<td>/</td>
</tr>
<tr>
<td>/home</td>
</tr>
<tr>
<td>/tmp</td>
</tr>
<tr>
<td>/var</td>
</tr>
<tr>
<td>/var/log</td>
</tr>
<tr>
<td>/var/log/audit</td>
</tr>
<tr>
<td>/opt/nsp</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/auxserver/nms/log</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/auxserver/xml_output</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/lte</td>
</tr>
<tr>
<td>/extra</td>
</tr>
</tbody>
</table>

Notes:
1. Required only if wireless core NE statistics are to be collected
2. CMM PM statistics may require additional storage space, depending on the collection volume and retention period; contact CMM technical support to define your PM storage requirement, which must be added to the listed partition size

The following table lists the partitions required for the live deployment of an auxiliary server that is to collect call-trace data.

Table 5-15  Live partitioning scheme, call-trace auxiliary server

<table>
<thead>
<tr>
<th>Disks required: four 300-Byte (RAID 0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partition</td>
</tr>
<tr>
<td>swap</td>
</tr>
<tr>
<td>/</td>
</tr>
<tr>
<td>/home</td>
</tr>
<tr>
<td>/tmp</td>
</tr>
<tr>
<td>/var</td>
</tr>
<tr>
<td>/var/log</td>
</tr>
<tr>
<td>/var/log/audit</td>
</tr>
<tr>
<td>/opt/nsp</td>
</tr>
</tbody>
</table>
### Table 5-15  Live partitioning scheme, call-trace auxiliary server (continued)

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>Size (Gbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>/opt/nsp/nfmp/auxserver/nms/log</td>
<td>Auxiliary server log files</td>
<td>30</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/calltrace</td>
<td>Call-trace output</td>
<td>600</td>
</tr>
<tr>
<td>/extra</td>
<td>NSP and NFM-P software storage</td>
<td>50</td>
</tr>
</tbody>
</table>

The following table lists the partitions required for the live deployment of an auxiliary server that is to collect PCMD records.

### Table 5-16  Live partitioning scheme, PCMD auxiliary server

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>Size (Gbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>swap</td>
<td>Swap space</td>
<td>16</td>
</tr>
<tr>
<td>/</td>
<td>Root</td>
<td>26</td>
</tr>
<tr>
<td>/home</td>
<td>User home directories</td>
<td>0.5</td>
</tr>
<tr>
<td>/tmp</td>
<td>Temporary files</td>
<td>4</td>
</tr>
<tr>
<td>/var</td>
<td>System data</td>
<td>14</td>
</tr>
<tr>
<td>/var/log</td>
<td>System logs</td>
<td>6</td>
</tr>
<tr>
<td>/var/log/audit</td>
<td>System audit logs</td>
<td>6</td>
</tr>
<tr>
<td>/opt/nsp</td>
<td>Auxiliary server software, operating data</td>
<td>40</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/auxserver/nms/log</td>
<td>Auxiliary server log files</td>
<td>20</td>
</tr>
<tr>
<td>/extra</td>
<td>NSP and NFM-P software storage</td>
<td>50</td>
</tr>
<tr>
<td>/opt/nsp/nfmp/pcmd_output</td>
<td>PCMD files</td>
<td>1800</td>
</tr>
</tbody>
</table>

The following table lists the partitions required for the live deployment of an NSP Flow Collector.

### Table 5-17  Live partitioning scheme, NSP Flow Collector

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>Size (Gbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>swap</td>
<td>Swap space</td>
<td>16</td>
</tr>
<tr>
<td>/</td>
<td>Root</td>
<td>26</td>
</tr>
<tr>
<td>/home</td>
<td>User home directories</td>
<td>0.5</td>
</tr>
<tr>
<td>/tmp</td>
<td>Temporary files</td>
<td>4</td>
</tr>
</tbody>
</table>
### Table 5-17  Live partitioning scheme, NSP Flow Collector (continued)

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>Size (Gbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>/var</td>
<td>System data</td>
<td>14</td>
</tr>
<tr>
<td>/var/log</td>
<td>System logs</td>
<td>6</td>
</tr>
<tr>
<td>/var/log/audit</td>
<td>System audit logs</td>
<td>6</td>
</tr>
<tr>
<td>/opt/nsp</td>
<td>Auxiliary server software, operating data</td>
<td>50</td>
</tr>
<tr>
<td>/opt/nsp/flow/dcp_data</td>
<td>Collected statistics data files</td>
<td>200</td>
</tr>
<tr>
<td>/extra</td>
<td>NSP and NFM-P software storage</td>
<td>50</td>
</tr>
</tbody>
</table>

The following table lists the partitions required for the live deployment of an auxiliary database.

### Table 5-18  Live partitioning scheme, auxiliary database

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>Size (Gbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>swap</td>
<td>Swap space</td>
<td>16</td>
</tr>
<tr>
<td>/</td>
<td>Root</td>
<td>26</td>
</tr>
<tr>
<td>/var</td>
<td>System data</td>
<td>14</td>
</tr>
<tr>
<td>/var/log</td>
<td>System logs</td>
<td>6</td>
</tr>
<tr>
<td>/var/log/audit</td>
<td>System audit logs</td>
<td>6</td>
</tr>
<tr>
<td>/opt</td>
<td>Auxiliary database software</td>
<td>120</td>
</tr>
<tr>
<td>/extra</td>
<td>NSP and NFM-P software storage</td>
<td>50</td>
</tr>
<tr>
<td>Disks 3 and above, RAID 1+0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/opt/nsp/nfmp/auxdb/data</td>
<td>Auxiliary database data</td>
<td>3300</td>
</tr>
</tbody>
</table>

**Optional storage**

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>Size (Gbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>/opt/nsp/nfmp/auxdb/backup ¹</td>
<td>Auxiliary database backup data</td>
<td>Equal to /opt/nsp/nfmp/auxdb/data</td>
</tr>
</tbody>
</table>

**Notes:**

1. For multi-station auxiliary database, or single-station deployment with high data rate, remote mount point and 10 Gb/s link recommended

The following table lists the partitions required for the live deployment of a single-user client or client delegate server on RHEL.
Table 5-19  Live partitioning scheme, single-user client or client delegate server

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
<th>Size (Gbytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>swap</td>
<td>Swap space</td>
<td>16</td>
</tr>
<tr>
<td>/</td>
<td>Root, including /usr and /var</td>
<td>26</td>
</tr>
<tr>
<td>/opt/nsp</td>
<td>NFM-P client software</td>
<td>16</td>
</tr>
<tr>
<td>At operator discretion</td>
<td>Customer data; can be partitioned according to customer requirements</td>
<td>Remainder</td>
</tr>
</tbody>
</table>
6 TLS configuration and management

6.1 Overview

6.1.1 Purpose

This chapter describes how to configure and manage TLS for communication security in an NFM-P system.

6.1.2 Contents

<table>
<thead>
<tr>
<th>6.1 Overview</th>
<th>81</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>83</td>
</tr>
<tr>
<td>6.2 About TLS</td>
<td>83</td>
</tr>
<tr>
<td>6.3 NFM-P TLS implementation</td>
<td>83</td>
</tr>
<tr>
<td>6.4 TLS deployment methods</td>
<td>85</td>
</tr>
<tr>
<td>6.5 Managing TLS versions and ciphers</td>
<td>89</td>
</tr>
<tr>
<td><strong>Automated TLS deployment procedures</strong></td>
<td>90</td>
</tr>
<tr>
<td>6.6 Workflow for automated TLS deployment</td>
<td>90</td>
</tr>
<tr>
<td>6.7 To configure and enable an NSP PKI server</td>
<td>91</td>
</tr>
<tr>
<td>6.8 To configure an NFM-P main server to request a PKI-server TLS certificate</td>
<td>94</td>
</tr>
<tr>
<td>6.9 To configure an NFM-P auxiliary server to request a PKI-server TLS certificate</td>
<td>97</td>
</tr>
<tr>
<td>6.10 To configure an NSP Flow Collector to request a PKI-server TLS certificate</td>
<td>101</td>
</tr>
<tr>
<td><strong>Manual TLS deployment procedures</strong></td>
<td>105</td>
</tr>
<tr>
<td>6.11 Workflow for manual TLS deployment</td>
<td>105</td>
</tr>
<tr>
<td>6.12 To perform the TLS preconfiguration</td>
<td>107</td>
</tr>
<tr>
<td>6.13 To manually configure TLS on a main server</td>
<td>111</td>
</tr>
<tr>
<td>6.14 To manually configure TLS on an auxiliary server</td>
<td>114</td>
</tr>
<tr>
<td>6.15 To manually configure TLS on an NSP Flow Collector</td>
<td>117</td>
</tr>
<tr>
<td>6.16 To manually configure TLS on an NSP analytics server</td>
<td>119</td>
</tr>
<tr>
<td><strong>General TLS configuration procedures</strong></td>
<td>123</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>6.17</td>
<td>To disable TLS for XML API clients</td>
</tr>
<tr>
<td>6.18</td>
<td>To enable TLS for XML API clients</td>
</tr>
<tr>
<td>6.19</td>
<td>To suppress security warnings in NFM-P browser sessions</td>
</tr>
</tbody>
</table>
6.2 About TLS

6.2.1 Overview

The NFM-P uses Transport Layer Security, or TLS, to secure communication between system components. TLS supersedes the obsolescent SSL, and uses stronger ciphers.

Network entities that communicate using TLS each require a copy of a security certificate that is digitally signed by a common certification authority, or CA. The signed certificate is distributed among the entities for use during TLS authentication. Only entities that have the same certificate signed by the same CA can communicate using TLS.

A signed TLS certificate is one of the following, depending on the signing method used:

• self-signed—certificate creator acts as CA; requires manual keystore distribution to each communicating entity, and is untrusted by entity unless imported to local truststore
• CA-signed
  – public-CA-signed—signed by a publicly recognized CA; provides security between entities that communicate across a public network; typically not required in an NFM-P management domain
  – private-CA-signed—signed by a CA that is not publicly recognized, such as a root CA service that is internal to an organization; provides security between entities in an isolated or internal network

Depending on the TLS role of an entity—client or server—a certificate is stored by the entity in a local keystore file, truststore file, or both. One entity can act as a TLS client to some entities and a TLS server to others, if required.

6.3 NFM-P TLS implementation

6.3.1 Overview

TLS is mandatory and enabled by default on all interfaces between the following:

• main server
• auxiliary server
• NSP Flow Collector
• NSP analytics server

Figure 6-1, “NFM-P TLS communication channels” (p. 84) shows the TLS communication channels in an NFM-P system.
6.3.2 Client and server communication

The NFM-P client GUI status bar displays the padlock icon in Figure 6-2, “NFM-P client GUI security icon” (p. 84) to show that communication with the main server is secured by TLS. The icon is also displayed on the following:
• client GUI login form
• information form opened using Help→About NFM-P

You can secure the following client interfaces using TLS:
• single-user GUI client or client delegate server—EJB, JMS, and HTTP
• XML API client—JMS and HTTP

To support non-TLS OSS clients, you can disable TLS on the XML API.
**Note:** Disabling TLS on the XML API disables TLS for all clients that use the XML API, and for all NFM-P GUI clients. Browser-based clients are unaffected, and must use HTTPS for application access.

When the NFM-P is configured for secure client access and a non-secure single-user GUI client or client delegate server connects to a main server for the first time, TLS communication is automatically enabled for client communication; no additional user action is required.

### 6.3.3 Managing TLS certificate expiry

When TLS is configured on a main or auxiliary server, the server checks the expiry date of the TLS certificate in the local keystore during server initialization and once every 24 hours thereafter. If the certificate is to expire within a predefined period, the NFM-P raises a warning alarm. If the certificate is expired, the NFM-P clears the warning alarm and raises a critical alarm.

The default warning period is 30 days from the current date. To change the warning period, contact technical support.

The NFM-P updates the Last Time Detected value of an expiry warning alarm daily, and raises a new critical alarm daily when a certificate is expired. The alarm information includes the certificate ID, and the expiry date and time. When you replace an expiring or expired certificate with a new and valid certificate, the associated expiry alarms clear. Each type of alarm persists through events such as server switchovers.

**Note:** The Days Remaining value in an expiry alarm is based on the number of complete 24-hour periods until the certificate expiry time. If fewer than 24 hours remain until the expiry, the Days Remaining value is zero, but the NFM-P does not raise an alarm about the expired certificate until the actual expiry time.

**Note:** If a keystore contains hierarchical certificates, the NFM-P checks the expiry date of each certificate in the hierarchy, starting with the lowest, and uses the earliest expiry date found as the reference point for raising an alarm.

### TLS certificate renewal

The TLS certificate renewal process is the same as the initial configuration process. After you obtain the new certificate file, you must follow 6.11 “Workflow for manual TLS deployment” (p. 105) to update the NFM-P TLS configuration.

### 6.4 TLS deployment methods

#### 6.4.1 Overview

The NFM-P supports system-wide TLS deployment using the following methods:

- automated, using an NSP PKI server that:
  - creates a local private root CA service
  - generates a TLS certificate and uses the CA service to sign it, or imports a certificate
  - distributes the certificate to each entity, called a requestor, that submits a certificate request

This is the recommended method; see 6.4.2 “Automated TLS deployment” (p. 86) for more information.
• manual, which requires that you:
  − provide a self-signed, private-CA-signed, or public-CA-signed TLS certificate
  − generate the keystore and truststore files
  − manually distribute the keystore and truststore files to modules and components, as required
See 6.4.3 “Manual TLS deployment” (p. 88) for more information.

Note: You can use a keystore or truststore file from a 5620 SAM system in an NSP deployment that includes only the NFM-P, but only if the SAN field of the certificate contains the public IP address or hostname of each NFM-P main server.

Note: It is strongly recommended to save your TLS keystore and certificate files in a secure and remote location, such as a separate physical facility, for future use.

The following describe the available TLS deployment methods for common scenarios.

Installation
For a system installation, you can use either method described in 6.4.1 “Overview” (p. 85).

Upgrade
For a system upgrade, you can continue to use the current TLS keystore and truststore files; no further action is required.

Note: The NFM-P TLS configuration persists through system upgrades.

System expansion
If you are adding a system element, for example, an NSP module or NFM-P component, or converting a standalone system to a redundant system, the following options are available for implementing TLS on the new system elements:
• automated
  − Recommended—If you are using a TLS certificate generated by the PKI server, no action is required other than specifying the PKI server in the configuration of each new system element. Alternatively, if you provide a certificate, you must also import the certificate to the PKI server for distribution to each requestor. System operation is unaffected in either case.
  − You can use a PKI server to implement a new TLS certificate throughout the system; however, each requestor requires configuration and a restart, which can affect system operation.
• manual
  − You must copy the required keystore and truststore files to the new system element, and then configure the system element to use the new files. See the appropriate configuration procedure in “Manual TLS deployment procedures” (p. 105) for information.

6.4.2 Automated TLS deployment
To reduce the complexity of configuring TLS in a new NFM-P system, or adding components to an existing system, you can use an NSP utility called a Public Key Infrastructure, or PKI, server. Based
on user input, a PKI server creates, signs, and distributes certificates to each entity that is configured to use the PKI server.

**Note:** An NFM-P system upgrade preserves the TLS keystore and truststore files, which are used if no PKI server is specified during the upgrade.

**Benefits of automated TLS deployment**

In addition to simplifying the implementation of TLS, using a PKI server has the following benefits:

• No component or module downtime when adding NFM-P components or NSP modules, or during operations such as system conversion to redundancy
• No complex CLI operations or manual file transfers
• No operator requirement for knowledge of interface IP address or hostname assignments
• Compatible with current and future product releases
• Can generate certificate, use existing certificate, or use new certificate that you provide

See "Automated TLS deployment procedures" (p. 90) for information about using an NSP PKI server to deploy TLS.

**Functional description**

The NSP PKI server is a standalone utility that services TLS certificate signing requests, or CSRs, from requesting entities in an NFM-P or NSP system. A PKI server is available on an NFM-P main server after an installation or upgrade. A PKI server is also available on a station to which you extract an NSD and NRC software bundle.

**Note:** Only one PKI server instance is required for automated TLS deployment; the instance serves an entire NSP system.

**Note:** It is recommended that you run the utility from the installation location on an NFM-P main server or NSP server; optionally, however, you can run a copy of the utility on any RHEL station that is reachable by each requestor.

Initially, a PKI server looks for an existing TLS certificate to import; if no certificate is available, the server prompts the operator for certificate parameters and creates a local private root CA service. Subsequently, the PKI server listens for CSRs.

Upon receiving a CSR, for example, from an NFM-P auxiliary server or NSP Flow Collector, the PKI server directs the private root CA to sign the requestor certificate, and then returns the signed certificate to the requestor. The requestor uses the signed certificate to create the required keystore and truststore files, and then enables TLS on the required local interfaces.

In order for a PKI server to implement TLS on an NSP module or NFM-P component, the module or component configuration must include the PKI server information.

If a PKI server is specified, but

• no keystore and truststore files are specified, the PKI server generates a TLS certificate using the specified alias, which is mandatory.
• no keystore and truststore passwords are specified, the default password, which is available from technical support, is used.
Securing XML API clients in an automated TLS deployment

Securing an XML API client in an automated TLS deployment is the same as in a manual TLS deployment; you must import the required TLS certificate to a truststore on the client station. In an automated deployment, you must import the certificate in the ca.pem file on the PKI server.

See the NSP NFM-P XML API Developer Guide for information about establishing a secure XML API client connection to the NFM-P.

6.4.3 Manual TLS deployment

Each of the following requires the import of a TLS certificate to a local truststore:

- main server
- auxiliary server
- OSS client
- NSP Flow Collector
- NSP analytics server

After you import the certificate to a main server truststore, you must configure TLS on each main server using the NFM-P samconfig utility. Subsequently, the standalone or primary main server automatically distributes the truststore file to each single-user GUI client or client delegate server that connects to the main server.

**Note:** You must use the Java Key Store, or JKS, keystore format in an NFM-P system. If you have a keystore in a different format, for example, PKCS12, you must use the Java keytool utility to convert the keystore to JKS format.

**Note:** The NFM-P does not support the use of multiple private encryption keys. Only the first encryption key in a keystore is used; any others are ignored.

**Note:** You must manually copy the keystore file associated with a truststore file to each auxiliary server, NSP Flow Collector, and NSP analytics server station, after which you can enable TLS on each component.

See “Manual TLS deployment procedures” (p. 105) for information about manually generating and deploying TLS certificates in an NFM-P system.

NSP-specific requirements

In an NSP deployment that includes the NSD and NRC, the Subject Alternative Name, or SAN, field of the certificate for the NFM-P main servers must include the following:

- public IP address of each NSD and NRC server
- public IP address or hostname of each NFM-P main server

In an NSP deployment that includes only the NFM-P, the SAN field of the certificate for the main servers must include the public IP address or hostname of each main server.
6.5 Managing TLS versions and ciphers

6.5.1 Configuring TLS version and cipher support

The NFM-P includes a tool for managing the supported TLS versions and ciphers. A TLS version or cipher may be required for compatibility with an older OSS, or may be considered unsecure and need to be disabled if a security vulnerability is identified. You can configure the NFM-P to enable or disable the support for specific versions and ciphers, as required.

Note: An NFM-P system upgrade does not preserve custom TLS version and cipher support settings. You must reconfigure the TLS support after an upgrade.

See “To update the supported NFM-P TLS versions and ciphers” in the NSP NFM-P System Administrator Guide for information about using the tool.
Automated TLS deployment procedures

6.6 Workflow for automated TLS deployment

6.6.1 Description

**CAUTION**

Service Disruption

An incorrect TLS configuration prevents communication between system components and may seriously affect network management.

An operator who performs a procedure in this section must have TLS implementation knowledge and experience. Contact technical support for TLS configuration assistance.

The following is the sequence of high-level actions required to configure automated TLS deployment for an NFM-P system. You can use the workflow to:

- deploy TLS in a new system
- deploy TLS to new components in an existing system
- update an expired TLS certificate

6.6.2 Stages

1

Configure and enable the NSP PKI server to do one of the following:

- Create a new TLS certificate.
- Import a TLS certificate that you provide.

See 6.7 “To configure and enable an NSP PKI server” (p. 91).

2

Configure each system component that requires the TLS configuration to use the PKI server. This may be required during a system installation, conversion to redundancy, or the addition of a new NSP module or NFM-P component to an existing system.

To configure an NFM-P main server to request a PKI-server TLS certificate, see 6.8 “To configure an NFM-P main server to request a PKI-server TLS certificate” (p. 94).

To configure an NFM-P auxiliary server to request a PKI-server TLS certificate, see 6.9 “To configure an NFM-P auxiliary server to request a PKI-server TLS certificate” (p. 97).

To configure an NSP Flow Collector to request a PKI-server TLS certificate, see 6.10 “To configure an NSP Flow Collector to request a PKI-server TLS certificate” (p. 101).

3

If the OSS clients do not use TLS, disable TLS on the XML API; see 6.17 “To disable TLS for XML API clients” (p. 123).
4 If required, enable TLS for the OSS clients; see 6.18 "To enable TLS for XML API clients" (p. 125).

5 If you are using a TLS certificate signed by a private root CA such as the PKI server, and want to prevent the display of browser security warnings for NSP pages, import the certificate to your browser or computer certificate store; see 6.19 “To suppress security warnings in NFM-P browser sessions” (p. 128).

6 Open each GUI client to automatically update the client TLS configuration.

6.7 To configure and enable an NSP PKI server

6.7.1 Description

The following steps describe the following, after which the PKI server is enabled and listens for TLS certificate requests:

• how to configure the parameters for TLS certificate generation on a PKI server
• how to import an existing TLS certificate to the PKI server for distribution to requestors

Note: You require root user privileges on a station.

Note: The Bash shell is the supported command shell for RHEL CLI operations.

Note: A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

6.7.2 Steps

1 A PKI server is installed by default on an NFM-P main server or an NSP server station. You can run the utility from the default installation location, or can copy the utility to another station that is reachable by all requestors. The PKI server file path is:

```
/opt/nsp/os/install/tools/pki/pki-server
```

If you want to run the utility from another location, copy the pki-server file to the location.

2 Log in as the root user on the station on which you want to run the PKI server.

3 Open a console window.
4 Navigate to the directory that contains the pki-server file. On an NFM-P main server or an NSP server station, the path is:
/opt/nsp/os/install/tools/pki

5 If you have a set of signed certificate files that you want the PKI server to import and distribute to requestors, copy the files to the directory that contains the pki-server file. The files must be named:
- ca.key—private RSA key of the CA
- ca.pem—X.509 public key certificate signed using ca.key

**Note:** The files must be located in the same directory as the pki-server file, and the user that invokes the PKI server requires read access to the files.

6 Perform one of the following.
   a. Enter the following to use the default PKI server port:
      ```bash
      # ./pki-server
      ```
   b. Enter the following to specify a port other than the default:
      ```bash
      # ./pki-server -port port
      ```
      where *port* is the port to use for receiving and responding to requests

   **Note:** If you specify a port other than the default, you must specify the non-default port number when you configure each requestor using samconfig.

7 Perform one of the following.
   a. If you are importing a certificate, as described in Step 5, go to Step 14.
   b. If you have previously configured the TLS certificate parameters, go to Step 14.
   c. If this is the first time that the PKI server is run on the station, the following message and prompt are displayed:
      ```
      ********************************************************************************
      No Root CA detected on the filesystem. This should only happen on initial installation of an NSP module!
      ********************************************************************************
      Create new Root CA Identity [y/n]?
      ```

8 Enter *y*. The following prompt is displayed:
   ```
   Organization Name (eg, company) []:
   ```
Enter your company name.
The following prompt is displayed:

Country Name (2 letter code) []:

Enter the two-letter ISO alpha-2 code for your country.
The following prompt is displayed:

State or Province Name (full name) []:

Enter your state or province name.
The following prompt is displayed:

Validity (days) [3650]:

Enter the length of time, in days, for which the TLS certificate is valid, or press Enter to accept the default.
The following messages are displayed as the PKI server creates a local TLS root CA and begins to listen for TLS certificate requests:

date time Root CA generated successfully.
date time Using Root CA from disk, and serving requests on port port

Make a backup copy of the following private root CA files, which are in the current directory; store the files in a secure and remote location, such as a separate physical facility:

• ca.key
• ca.pem

When the PKI server receives a certificate request from a requestor, the following is displayed:

date time Received request for CA cert from IP_address:port

If the PKI server successfully responds to the request, the following is displayed:

date time Successfully returned a signed certificate valid for IPs: [IP_address_1...IP_address_n] and hostnames: [hostname_1...hostname_n]

When all requestors have received a signed certificate, enter CTRL+C to close the PKI server utility.
6.8 To configure an NFM-P main server to request a PKI-server TLS certificate

6.8.1 Description

**CAUTION**

Service Disruption

Performing the procedure requires that you shut down the main server, which may be service-affecting.

If the main server is in service, ensure that you perform the procedure only during a scheduled maintenance period.

The following steps describe how to configure an NFM-P main server to request a new TLS certificate from a PKI server. This may be required during the initial installation of a main server, or whenever a new certificate is required.

**Note:** The system installation and conversion to redundancy procedures in this guide describe the parameter settings that enable certificate generation.

6.8.2 Steps

1. Ensure that the PKI server is configured and running; see 6.7 “To configure and enable an NSP PKI server” (p. 91).

2. Log in to the main server station as the nsp user.

3. Open a console window.

4. Stop the main server.
   1. Enter the following:
      
      ```bash
      bash$ cd /opt/nsp/nfmp/server/nms/bin
      ```
   2. Enter the following:
      
      ```bash
      bash$ ./nmsserver.bash stop
      ```
3. Enter the following:

```
bash$ ./nmsserver.bash appserver_status
```

The main server is stopped when the following message is displayed:

```
Main Server is stopped
```

If the command output indicates that the server is not completely stopped, wait five minutes and then re-enter the command in this step to check the server status.

Do not proceed to the next step until the server is completely stopped.

5

Enter the following to switch to the root user:

```
bash$ su
```

6

Enter the following:

```
# samconfig -m main
```

The following is displayed:

```
Start processing command line inputs...
<main>
```

7

Enter the following:

```
<main> configure tls
```

The prompt changes to `<main configure tls>`.

8

Enter the following:

```
<main configure tls> no keystore-file
```

9

Enter the following:

```
<main configure tls> no truststore-file
```

10

Perform one of the following:

a. Enter the following to use the default keystore password, which is available from technical support:

```
<main configure tls> no keystore-pass
```

b. Enter the following to assign a keystore password:

```
<main configure tls> keystore-pass password
```
where password is the password to assign

Perform one of the following:

a. Enter the following to use the default truststore password, which is available from technical support:
   <main configure tls> no truststore-pass

b. Enter the following to assign a truststore password:
   <main configure tls> truststore-pass password
   where password is the password to assign

Enter the following:
   <main configure tls> alias alias
   where alias is the keystore alias to assign

Enter the following:
   <main configure tls> pki-server server
   where server is the PKI server IP address or hostname

If the PKI server is to use a port other than the default for servicing requests, enter the following:
   <main configure tls> pki-server-port port
   where port is the PKI server port number

Enter the following:
   <main configure tls> exit
   The prompt changes to <main>.

Enter the following:
   <main> apply
   The configuration is applied.
   The main server:
   • generates a TLS certificate
   • sends a CSR to the PKI server
• receives from the PKI server the signed TLS certificate

17

Enter the following:

*main* `exit`

The samconfig utility closes.

18

Enter the following to return to the nsp user:

```
# exit
```

19

Start the main server.

1. Enter the following:

```
bash$ ./nmsserver.bash start
```

2. Enter the following:

```
bash$ ./nmsserver.bash appserver_status
```

The server status is displayed; the server is fully initialized if the status is the following:

Application Server process is running. See `nms_status` for more detail.

If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

20

Close the console window.

**END OF STEPS**

---

**6.9 To configure an NFM-P auxiliary server to request a PKI-server TLS certificate**

**6.9.1 Description**

**CAUTION**

*Service Disruption*

*Performing the procedure requires that you shut down the auxiliary server, which may be service-affecting.*

*If the auxiliary server is in service, ensure that you perform the procedure only during a scheduled maintenance period.*
The following steps describe how to configure an NFM-P auxiliary server to request a new TLS certificate from a PKI server. This may be required during the initial installation of an auxiliary server, or whenever a new certificate is required.

Note: The auxiliary server installation procedure in this guide describes the parameter settings that enable certificate generation.

6.9.2 Steps

1. Ensure that the PKI server is configured and running; see 6.7 “To configure and enable an NSP PKI server” (p. 91).

2. Log in to the auxiliary server station as the nsp user.

3. Open a console window.

4. Stop the auxiliary server.
   1. Enter the following:
      
      ```bash
      cd /opt/nsp/nfmp/auxserver/nms/bin
      ```
   2. Enter the following:
      
      ```bash
      ./auxnmsserver.bash auxstop
      ```
   3. Enter the following:
      
      ```bash
      ./auxnmsserver.bash auxappserver_status
      ```
      The auxiliary server is stopped when the following message is displayed:
      Auxiliary Server is stopped
      If the command output indicates that the server is not completely stopped, wait five minutes and then re-enter the command in this step to check the server status.
      Do not proceed to the next step until the server is completely stopped.

5. Enter the following to switch to the root user:
   
   ```bash
   su -
   ```

6. Enter the following:
   
   ```bash
   # samconfig -m aux
   ```
   The following is displayed:
Start processing command line inputs...
<aux>

7

Enter the following:
<aux> configure tls
The prompt changes to <aux configure tls>.

8

Enter the following:
<aux configure tls> no keystore-file

9

Perform one of the following:
a. Enter the following to use the default keystore password, which is available from technical support:
<aux configure tls> no keystore-pass
b. Enter the following to assign a keystore password:
<aux configure tls> keystore-pass password
where password is the password to assign

10

Enter the following:
<aux configure tls> pki-server server
where server is the PKI server IP address or hostname

11

If the PKI server is to use a port other than the default for servicing requests, enter the following:
<aux configure tls> pki-server-port port
where port is the PKI server port number

12

Enter the following:
<aux configure tls> exit
The prompt changes to <aux>.

13

Enter the following:
<aux> apply
The configuration is applied.
The auxiliary server:
• generates a TLS certificate
• sends a CSR to the PKI server
• receives from the PKI server the signed TLS certificate

14

Enter the following:
<aux> exit ↓
The samconfig utility closes.

15

Enter the following to return to the nsp user:
# exit ↓

16

Start the auxiliary server.
1. Enter the following:
bash$ ./auxnmsserver.bash auxstart ↓
2. Enter the following:
bash$ ./auxnmsserver.bash auxappserver_status ↓
The server status is displayed; the server is fully initialized if the status is the following:
Auxiliary Server process is running. See auxnms_status for more detail.
If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

17

Close the console window.

END OF STEPS
6.10 To configure an NSP Flow Collector to request a PKI-server TLS certificate

6.10.1 Description

**CAUTION**

Service Disruption

Performing the procedure requires that you shut down the NSP Flow Collector, which may be service-affecting.

If the NSP Flow Collector is in service, ensure that you perform the procedure only during a scheduled maintenance period.

The following steps describe how to configure an NSP Flow Collector to request a new TLS certificate from a PKI server. This may be required during the initial installation of an NSP Flow Collector, or whenever a new certificate is required.

**Note:** The NSP Flow Collector installation procedure in this guide describes the parameter settings that enable certificate generation.

6.10.2 Steps

1. Ensure that the PKI server is configured and running; see 6.7 “To configure and enable an NSP PKI server” (p. 91).

2. Log in to the NSP Flow Collector station as the root user.

3. Open a console window.

4. Stop the NSP Flow Collector; enter the following:
   
   ```
   # /opt/nsp/flow/dcp/bin/dcpctl.sh stop
   ```
   
   The command displays a series of status messages as the NSP Flow Collector stops.

   **Note:** To stop the NSP Flow Collector without displaying status messages, you can use the following command:
   
   ```
   # systemctl stop nsp-flow-collector.service
   ```

5. Enter the following:

   ```
   # samconfig -m flow
   ```
The following is displayed:
Start processing command line inputs...
<flow>

6

Enter the following:
<flow> configure tls
The prompt changes to <flow configure tls>.

7

Enter the following:
<flow configure tls> no keystore-file

8

Enter the following:
<flow configure tls> no truststore-file

9

Perform one of the following:
 a. Enter the following to use the default keystore password, which is available from technical support:
    <flow configure tls> no keystore-pass
 b. Enter the following to assign a keystore password:
    <flow configure tls> keystore-pass password
    where password is the password to assign

10

Perform one of the following:
 a. Enter the following to use the default truststore password, which is available from technical support:
    <flow configure tls> no truststore-pass
 b. Enter the following to assign a truststore password:
    <flow configure tls> truststore-pass password
    where password is the password to assign

11

Enter the following:
<flow configure tls> pki-server server
where server is the PKI server IP address or hostname
If the PKI server is to use a port other than the default for servicing requests, enter the following:

```bash
<flow configure tls> pki-server-port port
```

where `port` is the PKI server port number.

Enter the following:

```bash
<flow configure tls> exit
```

The prompt changes to `<aux>`.

Enter the following:

```bash
<flow> apply
```

The configuration is applied.

The NSP Flow Collector:
- generates a TLS certificate
- sends a CSR to the PKI server
- receives the signed TLS certificate from the PKI server

Enter the following:

```bash
<flow> exit
```

The `samconfig` utility closes.

Enter the following to return to the `nsp` user:

```bash
# exit
```

Start the NSP Flow Collector; enter the following:

```bash
# /opt/nsp/flow/dcp/bin/dcpctl.sh start
```

The command displays a series of status messages as the NSP Flow Collector starts.

**Note:** To start the NSP Flow Collector without displaying status messages, you can use the following command:

```bash
# systemctl start nsp-flow-collector.service
```
18

Close the console window.

END OF STEPS
6.11 Workflow for manual TLS deployment

6.11.1 Description

CAUTION

Service Disruption

An incorrect TLS configuration prevents communication between NFM-P components and may seriously affect network management.

An operator who performs a procedure in this chapter must have TLS implementation knowledge and experience. Contact technical support for TLS configuration assistance.

CAUTION

Service Disruption

Updating the TLS certificate in an operational NFM-P system requires one of the following, each of which causes a temporary network management outage:

• standalone system—main server shutdown
• redundant system—server activity switch

Ensure that you configure TLS in an NFM-P system only during a scheduled maintenance period.

The following is the sequence of high-level actions required to manually configure TLS in an NFM-P system. You can use the workflow to:

• configure TLS in a new deployment
• update an expired TLS certificate

6.11.2 Stages

1

Configure and distribute the required keystore and truststore files for the NFM-P system; see 6.12 “To perform the TLS preconfiguration” (p. 107).

2

To configure TLS in an existing system that is not being upgraded, go to Stage 4.

3

If you are performing an NFM-P system installation or upgrade, configure the required TLS parameters for each component during the installation or upgrade, and then go to Stage 12.
4 In a redundant system, configure TLS on the standby main server; see 6.13 “To manually configure TLS on a main server” (p. 111).

5 Configure TLS on each reserved auxiliary server; see 6.14 “To manually configure TLS on an auxiliary server” (p. 114).

6 In a redundant system, configure TLS on the primary main server; see 6.13 “To manually configure TLS on a main server” (p. 111).

7 In a standalone system, configure TLS on the standalone main server; see 6.13 “To manually configure TLS on a main server” (p. 111).

8 Configure TLS on each preferred auxiliary server; see 6.14 “To manually configure TLS on an auxiliary server” (p. 114).

9 Configure TLS on each NSP Flow Collector; see 6.15 “To manually configure TLS on an NSP Flow Collector” (p. 117).

10 Configure TLS on each NSP analytics server; see 6.16 “To manually configure TLS on an NSP analytics server” (p. 119).

11 If the XML API clients do not use TLS, disable TLS for the XML API clients; see 6.17 “To disable TLS for XML API clients” (p. 123).

12 If required, enable TLS for all XML API clients; see 6.18 “To enable TLS for XML API clients” (p. 125).

13 Open each GUI client to automatically update the client TLS configuration.
6.12 To perform the TLS preconfiguration

6.12.1 Description

The following steps describe how to prepare an NFM-P system for TLS communication.

ℹ️ Note: You require root user privileges on a station.

ℹ️ Note: The Bash shell is the supported command shell for RHEL CLI operations.

ℹ️ Note: A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

6.12.2 Steps

1. If you have a TLS certificate that you want to use, for example, a new certificate that replaces an expired certificate, go to Step 5.

2. If you have a set of TLS keystore and truststore files, go to Step 12.

ℹ️ Note: The keystore must be in the Java Key Store, or JKS, format. If your keystore has a different format, for example, PKCS12, you can use the Java keytool utility to convert the keystore to JKS format.

ℹ️ Note: Ensure that the keystore that you use contains only one private encryption key. An NFM-P main server uses only the first encryption key in a keystore, and ignores additional keys.

3. Log in as the root user on a main server station or another RHEL station, as required.

4. Open a console window.

5. Use the Java keytool utility on the station to generate a keystore file. See the Oracle website for keytool information, if required.

ℹ️ Note: The keytool utility that you use must be from the Java version that the NFM-P uses. After an NFM-P main server installation, you can find the keytool utility in /opt/nsp/nfmp/jre/bin. If the NFM-P is not yet installed on the main server station, ensure that you use the keytool utility from the supported Java version specified in the NSP NFM-P Planning Guide.
Note: If the NFM-P system includes one or more NSP analytics servers, each analytics server must be represented in the keystore file that you generate, as shown in this step.

Depending on the certificate type, you must specify the following main and NSP analytics server identifiers in the keytool command:

- **self-signed**
  - If IP addresses are to be used for client connections to the main and analytics servers, enter the main and analytics server IP addresses in the `san` field.
  - If hostnames are to be used, enter the main and analytics server DNS hostnames in the `san` field.

- **public-CA-signed**
  - Typically, a public-CA-signed certificate includes an FQDN, rather than a short hostname or IP address, in which case you must enter server FQDNs in the `CN` and `san` fields.

Note: The `san` field can include IP addresses and hostnames, for example:
```
san=IP:203.0.113.75,DNS:nfmpmain1.central.mycompany.com,IP:203.0.113.77,DNS:nfmpanalytics1.central.mycompany.com
```

Note: A file path in the `keystore_file` value, or in the name of any file generated in a subsequent step, must not include `/opt/nsp/os`. If you do not include a path, the file is generated in the current working directory, which must not be below `/opt/nsp/os`.

```
# path/keytool -genkeypair -alias alias -keyalg RSA -keypass password 
-storepass password -keystore keystore_file -validity days -dname 
"CN=server_name, OU=org_unit, O=org_name, L=locality, S=state, 
C=country" -ext bc=ca:true -ext san=IP:main_server_1_IP,DNS:main_server_1_hostname,IP:analytics_server_1_IP,DNS:analytics_server_1_hostname,IP:analytics_server_n_IP,DNS:analytics_server_n_hostname 
```

where
- `path` is the path to the keytool utility
- `alias` is a case-insensitive alias that is required for subsequent keytool operations
- `password` is the password for the key and keystore

Note: The keypass and storepass passwords must be identical.

- `keystore_file` is the name of the keystore file to generate
- `days` is the number of days for which the certificate is to be valid
- `server_name` is the main server hostname, FQDN or IP address
- `org_unit` is a department or division name
- `org_name` is a company name
- `locality` is a city name
- `state` is a state or region name
- `country` is a country code, for example, US
- `main_server_1_IP` is the public IP address of the standalone or primary main server
- `main_server_1_hostname` is the hostname or FQDN of the standalone or primary main server
**Note:** The `main_server_2` values in the `san` field are not required for a standalone system.

`main_server_2_IP` is the public IP address of the standby main server in a redundant deployment

`main_server_2_hostname` is the hostname or FQDN of the standby main server in a redundant deployment

`analytics_server_1_IP` and `analytics_server_n_IP` represent the public IP addresses of one or more NSP analytics servers

`analytics_server_1_hostname` and `analytics_server_n_hostname` represent the hostnames or FQDNs of one or more NSP analytics servers

---

6. Record the alias and password values that you specify.

7. If you do not require a TLS certificate that is signed by a CA, such as in a lab or trial deployment, perform the following steps.

   1. Enter the following to export the certificate from the keystore to a certificate file:

      ```
      # path/keytool -export -alias alias -keystore keystore_file
      -storepass password -file certificate_file
      ```

      where

      - `alias` is the alias specified during keystore creation
      - `keystore_file` is the source keystore file, for example, `/opt/samserver.keystore`
      - `password` is the keystore password
      - `certificate_file` is the name of the certificate file to generate

   2. Go to Step 10.

8. Generate a certificate signing request, or CSR.

   **Note:** The `main_server_2` values in the `san` field are not required for a standalone system.

   1. Enter the following:

      ```
      # path/keytool -certreq -alias alias -keystore keystore_file
      -file CSR_file -storetype JKS -ext
      san=IP:main_server_1_IP,DNS:main_server_1_hostname,
      IP:main_server_2_IP,DNS:main_server_2_hostname,
      IP:analytics_server_1_IP,DNS:analytics_server_1_hostname,
      IP:analytics_server_n_IP,DNS:analytics_server_n_hostname
      -ext ExtendedKeyUsage=serverAuth,clientAuth
      ```

      where

      - `alias` is a case-insensitive alias that is required for subsequent keytool operations
      - `keystore_file` is the keystore file generated in Step 5
CSR_file is the name of the CSR file to generate

The following prompt is displayed:

Enter keystore password:

2. Enter the keystore password. The following prompt is displayed:

Enter key password for alias

3. Enter the key password. The utility generates the CSR file.

Send the CSR file to a CA for authentication. The CA returns a certificate file that contains a trusted root certificate in a hierarchical certificate chain.

Enter the following to import the certificate to a truststore file:

Note: If the certificate is signed by a CA, you must import the entire CA chain of certificates to the truststore file; see the CA documentation for information about importing trusted certificates.

# path/keytool -import -trustcacerts -alias alias -file certificate_file -keystore truststore_file -storepass password

where

alias is the keystore alias

certificate_file is the self-signed or CA certificate file

truststore_file is the truststore file that is to hold the certificate

password is the truststore password

If the certificate is CA-signed, enter the following to import the certificate from the certificate file to a keystore file:

Note: You must import the entire CA chain of certificates to the keystore file; see the CA documentation for information about importing trusted certificates.

# path/keytool -import -trustcacerts -alias alias -file certificate_file -keystore keystore_file -storepass password

where

alias is the keystore alias

certificate_file is the CA certificate file

keystore_file is the keystore file that is to hold the certificate

password is the truststore password
If the NFM-P system is redundant, copy the keystore and truststore files to a temporary directory on the peer main server station.

**Caution:** You must not copy the files to the /opt/nsp/os/tls directory on the peer main server, or the TLS configuration on the peer main server fails.

**Note:** The nsp user must be the owner of the entire directory path to the location.

Copy the keystore file to a temporary location on each auxiliary server station.

**Note:** The nsp user must be the owner of the entire directory path to the location.

---

### 6.13 To manually configure TLS on a main server

#### 6.13.1 Description

The following steps describe how to manually configure TLS on an NFM-P main server for communication with other NFM-P components using a set of keystore and truststore files that you provide.

**CAUTION**

**Service Disruption**

*Configuring TLS on an NFM-P main server requires a main server shutdown and causes a temporary network management outage.*

*Ensure that you perform the procedure only during a scheduled maintenance period.*

**Note:** You must perform this procedure on each main server in a redundant system; see 6.11 "Workflow for manual TLS deployment" (p. 105) for information about the order in which the main servers must be configured.

**Note:** You require the following user privileges on the main server station:

- root
- nsp

**Note:** The Bash shell is the supported command shell for RHEL CLI operations.

**Note:** The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:

- # —root user
- bash$ —nsp user
6.13.2 Steps

1
Stop the main server.
1. Log in to the main server station as the nsp user.
2. Open a console window.
3. Enter the following:
   
   ```bash
   cd /opt/nsp/nfmp/server/nms/bin
   ```
4. Enter the following:
   
   ```bash
   ./nmsserver.bash stop
   ```
5. Enter the following:
   
   ```bash
   ./nmsserver.bash appserver_status
   ```

   The server status is displayed; the server is fully stopped if the status is the following:
   
   Application Server is stopped

   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform
   the next step until the server is fully stopped.

2
Enter the following to switch to the root user:

   ```bash
   su -
   ```

3
Enter the following:

   ```bash
   # samconfig -m main
   ```

   The following is displayed:
   
   Start processing command line inputs...
   
   <main>

4
Enter the following:

   ```bash
   <main> configure tls
   ```

   The prompt changes to <main configure tls>.

5
Configure each parameter in the following table.
Table 6-1  Main server tls parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keystore-file</td>
<td>The absolute path of the TLS keystore file</td>
</tr>
<tr>
<td>keystore-pass</td>
<td>The TLS keystore password</td>
</tr>
<tr>
<td>truststore-file</td>
<td>The absolute path of the TLS truststore file</td>
</tr>
<tr>
<td>truststore-pass</td>
<td>The TLS truststore password</td>
</tr>
<tr>
<td>alias</td>
<td>The alias specified during keystore generation</td>
</tr>
<tr>
<td></td>
<td>You must configure the parameter.</td>
</tr>
</tbody>
</table>

6

To enable WebDAV access to eNodeB activation data on the main server, enter the following:

```
<main configure tls> webdav
```

WebDAV access is enabled.

7

Enter the following:

```
<main configure tls> back
```

The prompt changes to `<main configure>`.

8

Verify the main server configuration.

1. Enter the following:

   ```
   <main configure> show-detail
   ```

   The main server configuration is displayed.

2. Review each parameter to ensure that the value is correct.

3. Configure one or more parameters, if required.

4. When you are certain that the configuration is correct, enter the following:

   ```
   <main configure> back
   ```

   The prompt changes to `<main>`.

9

If the configuration is correct, enter the following:

```
<main> apply
```

The configuration is applied.

10

Enter the following:
<main>

Thesamconfigutilitycloses.

11

Enter the following to switch back to the nsp user:

```
# exit
```

12

Start the main server.

1. Enter the following:

```
bash$ cd /opt/nsp/nfmp/server/nms/bin
```

2. Enter the following:

```
bash$ ./nmsserver.bash start
```

3. Enter the following:

```
bash$ ./nmsserver.bash appserver_status
```

The server status is displayed; the server is fully initialized if the status is the following:

Application Server process is running. See nms_status for more detail.

If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

13

Close the console window.

END OF STEPS

6.14 To manually configure TLS on an auxiliary server

6.14.1 Description

The following steps describe how to configure TLS on an NFM-P auxiliary server for secure communication with other NFM-P components using a keystore file that you provide.

Note: You require the following user privileges on the auxiliary server station:

- root
- nsp

Note: The Bash shell is the supported command shell for RHEL CLI operations.

Note: The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:

- # —root user
6.14.2 Steps

1

Stop the auxiliary server.
1. Log in to the auxiliary server station as the nsp user.
2. Open a console window.
3. Enter the following:
   bash$ cd /opt/nsp/nfmp/auxserver/nms/bin
4. Enter the following:
   bash$ ./auxnmsserver.bash auxstop
5. Enter the following:
   bash$ ./auxnmsserver.bash auxappserver_status
   The auxiliary server is stopped when the following message is displayed:
   Auxiliary Server is stopped
   If the command output indicates that the server is not completely stopped, wait five minutes
   and then re-enter the command in this step to check the server status.
   Do not proceed to the next step until the server is completely stopped.

2

Enter the following to switch to the root user:
bash$ su -

3

Enter the following:
# samconfig -m aux
The following is displayed:
Start processing command line inputs...
<aux>

4

Enter the following:
<aux> configure tls
The prompt changes to <aux configure tls>.

5

Configure the parameters in the following table.
Table 6-2  Auxiliary server tls parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keystore-file</td>
<td>The absolute path of the TLS keystore file</td>
</tr>
<tr>
<td>keystore-pass</td>
<td>The TLS keystore password</td>
</tr>
</tbody>
</table>

6

Enter the following:

```
<aux configure tls> back
```

The prompt changes to `<aux configure>`.

7

Verify the auxiliary server configuration.

1. Enter the following:

```
<aux configure> show-detail
```

The auxiliary server configuration is displayed.

2. Review each parameter to ensure that the value is correct.

3. Configure one or more parameters, if required.

4. When you are certain that the configuration is correct, enter the following:

```
<aux configure> back
```

The prompt changes to `<aux>`.

8

If the configuration is correct, enter the following:

```
<aux> apply
```

The configuration is applied.

9

Enter the following:

```
<aux> exit
```

The samconfig utility closes.

10

Enter the following to switch back to the nsp user:

```
# exit
```

11

Enter the following to start the auxiliary server:

```
bash$ /opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash auxstart
```
The auxiliary server starts.

12

Close the console window.

END OF STEPS

6.15 To manually configure TLS on an NSP Flow Collector

6.15.1 Description

The following steps describe how to configure TLS on an NSP Flow Collector for secure communication with one or more NFM-P main servers and web UI clients using a set of keystore and truststore files that you provide.

Note: You require root user privileges on the NSP Flow Collector station.

Note: The Bash shell is the supported command shell for RHEL CLI operations.

Note: A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

6.15.2 Steps

1

Transfer the TLS truststore and keystore files from the /opt/nsp/os/tls directory on an NFM-P main server station to the same directory on the NSP Flow Collector station.

2

Log in to the NSP Flow Collector station as the root user.

3

Open a console window.

4

Stop the NSP Flow Collector; enter the following:

```
# /opt/nsp/flow/dcp/bin/dcpctl.sh stop
```

The command displays a series of status messages as the NSP Flow Collector stops.

Note: To stop the NSP Flow Collector without displaying status messages, you can use the following command:

```
# systemctl stop nsp-flow-collector.service
```

5

Enter the following:
To manually configure TLS on an NSP Flow Collector

```
# samconfig -m flow
The following is displayed:
Start processing command line inputs...
<flow>
```

6 Enter the following:
<flow> configure
The prompt changes to <flow configure>.

7 Configure the tls parameters in the following table, and then enter back.

```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keystore-file</td>
<td>The absolute path of the TLS keystore file</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>keystore-pass</td>
<td>The TLS keystore password</td>
</tr>
<tr>
<td></td>
<td>Default: available from technical support</td>
</tr>
<tr>
<td>truststore-file</td>
<td>The absolute path of the TLS truststore file</td>
</tr>
<tr>
<td>truststore-pass</td>
<td>The TLS truststore password</td>
</tr>
</tbody>
</table>
```

8 Enter the following:
<flow configure> exit
The prompt changes to <flow>.

9 Enter the following:
<flow> apply
The configuration is applied.

10 Enter the following:
<flow> exit
The samconfig utility closes.
11

Start the NSP Flow Collector; enter the following:

```
# /opt/nsp/flow/dcp/bin/dcpctl.sh start
```

The command displays a series of status messages as the NSP Flow Collector starts.

**Note:** To start the NSP Flow Collector without displaying status messages, you can use the following command:

```
# systemctl start nsp-flow-collector.service
```

12

Configure the NSP Flow Collector to use HTTPS and SFTP for communication with the main servers, as described in 7.12 “To configure NSP Flow Collector communication” (p. 219).

END OF STEPS

---

6.16 To manually configure TLS on an NSP analytics server

6.16.1 Description

The following steps describe how to configure TLS on an NSP analytics server for secure communication with NFM-P components.

**Note:** You require the following user privileges on the analytics server station:

- root
- ns

**Note:** The Bash shell is the supported command shell for RHEL CLI operations.

**Note:** The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:

- `#` — root user
- `bash$` — ns user

6.16.2 Steps

1. Log in to the NSP analytics server station as the root user.

2. Open a console window.

3. Transfer the required TLS keystore and truststore files from the standalone or primary main server station to the analytics server station.
**Note:** The files must be located on a path that is owned by the nsp user.

4

Enter the following:

```
# chown nsp:nsp keystore_file
```

where `keystore_file` is the absolute path of the transferred keystore file

5

Enter the following:

```
# chown nsp:nsp truststore_file
```

where `truststore_file` is the absolute path of the transferred truststore file

6

Enter the following to switch to the nsp user:

```
# su nsp
```

7

If hostnames are used for NFM-P inter-component communication, perform the following steps.

1. Open the following file using a plain-text editor such as `vi`:
   `/opt/nsp/analytics/config/install.config`

2. Edit or add the following line:
   `zkRegistrationHostIp=hostname`
   where `hostname` is the hostname or FQDN specified for the analytics server in the TLS certificate

3. Enter the following to stop the analytics server:
   `bash$ /opt/nsp/analytics/bin/AnalyticsAdmin.sh stop`
   The following is displayed:
   Stopping Analytics Server
   When the analytics server is completely stopped, the following message is displayed:
   Analytics Server is not running

4. Enter the following to start the analytics server:
   `bash$ /opt/nsp/analytics/bin/AnalyticsAdmin.sh start`
   The following message is displayed:
   Starting Analytics Server
   When the analytics server is started, the following message is displayed.
   Analytics Server successfully started!

8

Enter the following:
bash$ cd /opt/nsp/analytics/bin

9
Enter the following:
bash$ ./AnalyticsAdmin.sh updateTLS

The script displays the following messages and prompt:
This Action requires Analytic Server Restart.
Please type 'YES' to continue

10
Enter YES.
The script displays the following messages and prompt:
Stopping Analytics Application
Do you have existing TLS certificates?(yes/no)

11
Enter yes.
The script displays the following prompt:
Enter TLS keystore Path, including filename:

12
Enter the absolute file path of the TLS keystore file.
The script displays the following messages and prompt:
/path/keystore_file found.
Enter TLS truststore Path, including filename:

13
Enter the absolute file path of the truststore file.
The script displays the following messages and prompt:
/path/truststore_file found.
Set the keystore Password:

14
Enter the keystore password.
Messages like the following are displayed:
Verifying TLS Keystore...
Certificate loading...
Verified TLS Certificate
The following prompt is displayed:
Set the truststore Password:

15

Enter the truststore password.

Messages like the following are displayed as the configuration is applied and the analytics server starts:

Verifying TLS Truststore...
Certificate loading...
Verified TLS Certificate
TLS Config has been updated
Analytic Server TLS configuration has been added
date time Starting Analytics Application
Waiting for Analytics Server to come up
date time Analytics Server is UP and Running

16

Close the console window.

END OF STEPS
General TLS configuration procedures

6.17 To disable TLS for XML API clients

6.17.1 Description

The following steps describe how to disable TLS for all XML API clients in order to support OSS applications in a non-secure environment.

Note: Disabling TLS on the XML API also disables TLS for all clients that use the XML API, and for NFM-P GUI clients. Browser-based clients are unaffected, and must use HTTPS for application access.

CAUTION

Service Disruption

Performing the procedure involves stopping and starting each main server, which is service-affecting.

You must perform the procedure only during a scheduled maintenance period of low network activity.

Note: You require the following user privileges on the main server station:

- root
- nsp

Note: The Bash shell is the supported command shell for RHEL CLI operations.

Note: The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:

- # — root user
- bash$ — nsp user

6.17.2 Steps

1. Perform the following steps on each main server station to stop the main server.

   Note: In a redundant system, you must stop the standby main server first.

   1. Log in to the main server station as the nsp user.
   2. Enter the following:

      bash$ cd /opt/nsp/nfmp/server/nms/bin

      bash$ ./nmsserver.bash stop
4. Enter the following:
   
   ```bash
   bash$ ./nmsserver.bash appserver_status
   ```
   
   The server status is displayed; the server is fully stopped if the status is the following:
   
   Application Server is stopped
   
   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

2

When the main servers are stopped, perform the following on each main server station.

1. Enter the following to switch to the root user:
   
   ```bash
   bash$ su -
   ```

2. Enter the following:
   
   ```bash
   # samconfig -m main
   ```
   
   The following is displayed:
   
   Start processing command line inputs...
   
   `<main>`

3. Enter the following:
   
   ```bash
   <main> configure oss no secure back
   ```
   
   The prompt changes to `<main configure>`.

4. Enter the following:
   
   ```bash
   <main configure> back
   ```
   
   The prompt changes to `<main>`.

5. Enter the following:
   
   ```bash
   <main> apply
   ```
   
   The configuration is applied.

6. Enter the following:
   
   ```bash
   <main> exit
   ```
   
   The samconfig utility closes.

3

Perform the following on each main server station to start the main server.

**Note:** In a redundant system, you must start the primary main server first.

1. Enter the following to switch back to the nsplib user:
   
   ```bash
   # exit
   ```

2. Enter the following:
   
   ```bash
   bash$ cd /opt/nsplib/nfmp/server/nms/bin
   ```

3. Enter the following:
4. Enter the following:

```bash
./nmsserver.bash appserver_status
```

The server status is displayed; the server is fully initialized if the status is the following:

Application Server process is running. See nms_status for more detail.

If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

4

Close the console window.

5

On each XML API client station, modify the URL that the client applications use to reach the main server.

1. Change https: to http:.
2. Change the URL port value from 8443 to 8080.

END OF STEPS

### 6.18 To enable TLS for XML API clients

#### 6.18.1 Description

The following steps describe how to enable TLS for all XML API client communication with the NFM-P.

For specific TLS implementation information, see:

- "Automated TLS deployment procedures" (p. 90)—automated TLS certificate generation and distribution using an NSP PKI server
- "Manual TLS deployment procedures" (p. 105)—manual TLS certificate generation and deployment

**CAUTION**

**Service Disruption**

Performing the procedure involves stopping and starting each main server, which is service-affecting.

You must perform the procedure only during a scheduled maintenance window.

**Note:** You require the following user privileges on the main server station:

- root
- nsp
i Note: The Bash shell is the supported command shell for RHEL CLI operations.

i Note: The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:
- # — root user
- bash$ — nsp user

6.18.2 Steps

1. Perform the following on each main server station to stop the main server.

   Note: In a redundant system, you must stop the standby main server first.
   1. Log in to the main server station as the nsp user.
   2. Enter the following:
      ```bash$
      cd /opt/nsp/nfmp/server/nms/bin
      ```
   3. Enter the following:
      ```bash$
      ./nmsserver.bash stop
      ```
   4. Enter the following:
      ```bash$
      ./nmsserver.bash appserver_status
      ```
      The server status is displayed; the server is fully stopped if the status is the following:
      - Application Server is stopped
      If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

2. When the main servers are stopped, perform the following on each main server station.
   1. Enter the following to switch to the root user:
      ```bash$
      su -
      ```
   2. Enter the following:
      ```bash$
      # samconfig -m main
      ```
      The following is displayed:
      - Start processing command line inputs...
      - <main>
   3. Enter the following:
      ```bash$
      <main> configure oss secure back
      ```
      The prompt changes to <main configure>.
   4. Enter the following:
      ```bash$
      <main configure> back
      ```
      The prompt changes to <main>.
5. Enter the following:

    <main> apply </main>

    The configuration is applied.

6. Enter the following:

    <main> exit </main>

    The samconfig utility closes.

3

Perform the following on each main server station to start the main server.

**Note:** In a redundant system, you must start the primary main server first.

1. Enter the following to switch back to the nsp user:

    # exit

2. Enter the following:

    bash$ cd /opt/nsp/nfmp/server/nms/bin

3. Enter the following:

    bash$ ./nmsserver.bash start

4. Enter the following:

    bash$ ./nmsserver.bash appserver_status

    The server status is displayed; the server is fully initialized if the status is the following:

    Application Server process is running. See nms_status for more detail.

    If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

4

Perform the following steps on each XML API client station.

1. If you deployed TLS using an NSP PKI server, perform one of the following.
   a. Transfer the ca.pem certificate file from the PKI server station to the OSS client station.
   b. Use the PKI server REST API to obtain the certificate; see the online NSP REST API documentation for information.

2. If you deployed TLS using the manual method, transfer your certificate file to the OSS client station.

3. Import the TLS certificate from the certificate file to the TLS certificate store of the client station OS; see the OS documentation for information about importing a certificate.

4. Modify each main server XML API URL on the OSS client station:
   - Change http: to https:.
   - Change the URL port value from 8080 to 8443.

END OF STEPS
6.19 To suppress security warnings in NFM-P browser sessions

6.19.1 Description

The following steps describe how to prevent the repeated display of security warnings in a browser that connects to the NFM-P using a private-CA-signed or self-signed TLS certificate.

**Note:** You do not need to perform the procedure if the certificate is signed by a public root CA, which is by default trusted.

6.19.2 Steps

1

Perform one of the following.

a. If you deployed TLS using an NSP PKI server, transfer the ca.pem certificate file from the PKI server station to each client station on which you want to suppress the browser warnings.

b. If you deployed TLS using the manual method, transfer your certificate file to each client station on which you want to suppress the browser warnings.

2

Perform one of the following.

a. Import the certificate to the certificate store of a client station OS.

   **Note:** This method suppresses the display of NFM-P-related security warnings for all browsers on the client station.

   Perform the appropriate procedure in the OS documentation to import the certificate; specify the certificate file as the certificate source.

   **Note:** Such a procedure varies by OS type and version.

b. Import the certificate to the certificate store of a client browser.

   Perform the appropriate procedure in the browser documentation to import the certificate; specify the certificate file as the certificate source.

   **Note:** Such a procedure varies by browser type and version.

3

Open a browser session and verify that the required NFM-P applications open without the display of security warnings.

**END OF STEPS**
Part II: NFM-P system deployment

Overview

Purpose
This part describes NFM-P system installation, upgrade, conversion to redundancy, and conversion from IPv4 inter-component communication to IPv6.

Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 7</td>
<td>NFM-P installation</td>
<td>131</td>
</tr>
<tr>
<td>Chapter 8</td>
<td>NFM-P qcw2 deployment</td>
<td>239</td>
</tr>
<tr>
<td>Chapter 9</td>
<td>5620 SAM upgrade to NFM-P</td>
<td>247</td>
</tr>
<tr>
<td>Chapter 10</td>
<td>NFM-P upgrade</td>
<td>367</td>
</tr>
<tr>
<td>Chapter 11</td>
<td>NFM-P conversion to redundancy</td>
<td>465</td>
</tr>
<tr>
<td>Chapter 12</td>
<td>NFM-P conversion to IPv6</td>
<td>501</td>
</tr>
<tr>
<td>Chapter 13</td>
<td>NFM-P uninstallation</td>
<td>545</td>
</tr>
</tbody>
</table>
7 NFM-P installation

7.1 Overview

7.1.1 Purpose
This chapter describes how to install and enable the components of a standalone or redundant NFM-P system.

7.1.2 Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1 Overview</td>
<td>131</td>
</tr>
<tr>
<td>Introduction</td>
<td>133</td>
</tr>
<tr>
<td>7.2 General information</td>
<td>133</td>
</tr>
<tr>
<td>Standalone NFM-P system installation</td>
<td>135</td>
</tr>
<tr>
<td>7.3 Standalone system installation workflow</td>
<td>135</td>
</tr>
<tr>
<td>7.4 To install a standalone NFM-P system</td>
<td>136</td>
</tr>
<tr>
<td>Redundant NFM-P system installation</td>
<td>156</td>
</tr>
<tr>
<td>7.5 Redundant system installation workflow</td>
<td>156</td>
</tr>
<tr>
<td>7.6 To install a redundant NFM-P system</td>
<td>157</td>
</tr>
<tr>
<td>Auxiliary server installation</td>
<td>201</td>
</tr>
<tr>
<td>7.7 Auxiliary server installation workflow</td>
<td>201</td>
</tr>
<tr>
<td>7.8 To install an NFM-P auxiliary server</td>
<td>202</td>
</tr>
<tr>
<td>7.9 To add auxiliary servers to an NFM-P system</td>
<td>208</td>
</tr>
<tr>
<td>NSP Flow Collector installation</td>
<td>215</td>
</tr>
<tr>
<td>7.10 NSP Flow Collector installation workflow</td>
<td>215</td>
</tr>
<tr>
<td>7.11 To install an NSP Flow Collector</td>
<td>216</td>
</tr>
<tr>
<td>7.12 To configure NSP Flow Collector communication</td>
<td>219</td>
</tr>
<tr>
<td>Auxiliary database installation</td>
<td>223</td>
</tr>
<tr>
<td>7.13 Auxiliary database installation workflow</td>
<td>223</td>
</tr>
<tr>
<td>7.14 To prepare a station for auxiliary database installation</td>
<td>224</td>
</tr>
<tr>
<td>7.15 To install the NFM-P auxiliary database software</td>
<td>226</td>
</tr>
<tr>
<td>7.16 To add an auxiliary database to an NFM-P system</td>
<td>228</td>
</tr>
</tbody>
</table>
7.17 To add a station to an NFM-P auxiliary database
Introduction

7.2 General information

7.2.1 Description

CAUTION

Support Liability

Failure to follow the requirements and restrictions that apply to NFM-P system deployment may violate a support agreement.

NFM-P software deployment is supported only under the conditions described in Chapter 2, “Before you begin”.

This chapter describes standalone and redundant NFM-P system installation, including the installation of the following:

- NFM-P auxiliary server
- NFM-P auxiliary database
- NSP Flow Collector

Note: For NSP analytics server installation information, see “To install an NSP analytics server” in the NSP Deployment and Installation Guide.


Note: It is strongly recommended that you verify the checksum of each software package or file that you download from OLCS. You can compare the checksum value on the download page with, for example, the output of the RHEL md5sum or sha256sum command. See the appropriate RHEL man page for information.

Component configuration

Most NFM-P component configuration is performed using the samconfig utility. See Chapter 3, “Using samconfig” for information.

Note: The Bash shell is the supported command shell for RHEL CLI operations.

NFM-P installation procedures

Table 7-1 NFM-P installation procedures list

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.4 “To install a standalone NFM-P system” (p. 136)</td>
<td>Install the database and server software in a standalone deployment on one or more stations.</td>
</tr>
<tr>
<td>Procedure</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>7.6  “To install a redundant NFM-P system” (p. 157)</td>
<td>Install the database and server software in a redundant deployment.</td>
</tr>
<tr>
<td>7.8  “To install an NFM-P auxiliary server” (p. 202)</td>
<td>Install the auxiliary server software on a station.</td>
</tr>
<tr>
<td>7.9  “To add auxiliary servers to an NFM-P system” (p. 208)</td>
<td>Add an auxiliary server to an NFM-P system.</td>
</tr>
<tr>
<td>7.11 “To install an NSP Flow Collector” (p. 216)</td>
<td>Install the NSP Flow Collector software on a station.</td>
</tr>
<tr>
<td>7.12 “To configure NSP Flow Collector communication” (p. 219)</td>
<td>Configure an NSP Flow Collector to communicate with NFM-P servers and NEs.</td>
</tr>
<tr>
<td>7.15 “To install the NFM-P auxiliary database software” (p. 226)</td>
<td>Install the auxiliary database software on a station.</td>
</tr>
<tr>
<td>7.16 “To add an auxiliary database to an NFM-P system” (p. 228)</td>
<td>Enable communication among the auxiliary database stations, and between the stations and other NFM-P components.</td>
</tr>
</tbody>
</table>
Standalone NFM-P system installation

7.3 Standalone system installation workflow

7.3.1 Description

The following is the sequence of high-level actions required to install a standalone NFM-P system.

7.3.2 Stages

1. Configure firewalls between components, as required; see “Check and configure firewalls” (p. 137).

2. Download the required NFM-P installation files; see “Download installation files” (p. 137).

3. Install the standalone database; see “Install standalone database” (p. 138).
   1. Run a script to prepare for the Oracle software installation.
   2. Install the database packages.
   3. Create the standalone database.

4. Install the standalone main server; see “Install standalone main server” (p. 144)
   1. Install the main server packages.
   2. Create and apply the main server configuration.

5. Start the main server; see “Start standalone main server” (p. 153).

6. Install one or more of the following optional components, as required; see “Install optional components” (p. 154):
   • auxiliary server
   • auxiliary database
   • NSP Flow Collector
   • NSP analytics server
7.4 To install a standalone NFM-P system

7.4.1 Description

The following steps describe how to install a collocated or distributed main database and main server in a standalone configuration. The steps also include information about installing optional NFM-P components.

Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

**Note:** You require root user privileges on the main database and main server stations.

**Note:** Performing the procedure creates the following user accounts:

- on the main database station—Oracle management
- on the main server station—nsp

**Note:** The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:

- # —root user
- bash$ —nsp user

7.4.2 Steps

**CAUTION**

Deployment failure

The RHEL OS of any NFM-P component requires specific versions of some RHEL packages. If the required package versions are not installed, the component installation fails.

See 4.10.4 “Special RHEL OS package requirements” (p. 59) for the required package versions.
Check and configure firewalls

1

Before you attempt to deploy an NFM-P system, you must ensure that each firewall between NFM-P components allows the required traffic to pass between the components, or is disabled. You can configure and enable the firewall after the installation, if required.

i Note: The RHEL Firewalld service is typically enabled by default in a new RHEL OS installation.

Perform one of the following.

a. Configure each firewall to allow the required traffic to pass. See the NSP NFM-P Planning Guide for a list of the ports that must be open on each component.

i Note: The RHEL Firewalld service must be configured using the Firewalld rules in the NSP NFM-P Planning Guide, which describes using NFM-P templates for rule creation.

b. Disable each firewall; see the external firewall documentation, or perform the following steps on each component station to disable Firewalld.

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following:
   
   ```
   # systemctl stop firewalld
   ```
4. Enter the following:
   
   ```
   # systemctl disable firewalld
   ```
5. Close the console window.

Download installation files

2

Download the following installation files to an empty directory on the main server station:

- nsp-nfmp-jre-R.r.p-rel.v.rpm
- nsp-nfmp-config-R.r.p-rel.v.rpm
- nsp-nfmp-nspos-R.r.p-rel.v.rpm
- nsp-nfmp-main-server-R.r.p-rel.v.rpm

where

R.r.p is the NSP release identifier, in the form MAJOR.minor.patch

v is a version identifier

i Note: In subsequent steps, the directory is called the NFM-P software directory.

3

Perform one of the following.
a. For a collocated NFM-P deployment, download the following files to the NFM-P software directory on the station that hosts the main server and database:
   • nsf-nfmp-oracle-R.r.p-rel.v.rpm
   • nsf-nfmp-main-db-R.r.p-rel.v.rpm

b. For a distributed NFM-P deployment, download the following files to an empty directory on the main database station:
   • nsf-nfmp-jre-R.r.p-rel.v.rpm
   • nsf-nfmp-config-R.r.p-rel.v.rpm
   • nsf-nfmp-oracle-R.r.p-rel.v.rpm
   • nsf-nfmp-main-db-R.r.p-rel.v.rpm

**Note:** In subsequent steps, the directory is called the NFM-P software directory.

4

Transfer the following downloaded file to an empty directory on the main database station:
• OracleSw_PreInstall.sh

**Install standalone database**

5

Log in as the root user on the main database station.

6

Open a console window.

7

Navigate to the directory that contains the OracleSw_PreInstall.sh file.

8

Enter the following:

```
# chmod +x OracleSw_PreInstall.sh
```

9

Enter the following:

```
# ./OracleSw_PreInstall.sh
```

**Note:** A default value is displayed in brackets []. To accept the default, press \[\].

**Note:** If you specify a value other than the default, you must record the value for use when the OracleSw_PreInstall.sh script is run during a software upgrade, or when the Oracle management user information is required by technical support.

The following prompt is displayed:
This script will prepare the system for a new install/restore of an NFM-P Version Release main database.

Do you want to continue? [Yes/No]:

Enter Yes. The following prompt is displayed:

Enter the Oracle dba group name [group]:

Enter a group name.

Note: To reduce the complexity of subsequent software upgrades and technical support activities, it is recommended that you accept the default.

The following messages and prompt are displayed:

Creating group group if it does not exist...
done

Enter the Oracle user name:

Enter a username.

Note: To reduce the complexity of subsequent software upgrades and technical support activities, it is recommended that you accept the default.

The following messages and prompt are displayed:

Oracle user [username] new home directory will be [/opt/nsp/nfmp/oracle12r1].
Checking or Creating the Oracle user home directory /opt/nsp/nfmp/oracle12r1...,
Checking user username...
Adding username...
Changing ownership of the directory /opt/nsp/nfmp/oracle12r1 to username:group.
About to unlock the UNIX user [username]
Unlocking password for user username.
passwd: Success
Unlocking the UNIX user [username] completed
Please assign a password to the UNIX user username..
New Password:

Enter a password. The following prompt is displayed:
Re-enter new Password:

14

Re-enter the password. The following is displayed if the password change is successful:

```
passwd: password successfully changed for username
```

The following message and prompt are displayed:

Specify whether an NFM-P Main Server will be installed on this workstation.

The database memory requirements will be adjusted to account for the additional load.

Will the database co-exist with an NFM-P Main Server on this workstation [Yes/No]:

15

Enter Yes or No, as required.

Messages like the following are displayed as the script execution completes:

```
INFO: About to set kernel parameters in /etc/sysctl.conf...
INFO: Completed setting kernel parameters in /etc/sysctl.conf...
INFO: About to change the current values of the kernel parameters
INFO: Completed changing the current values of the kernel parameters
INFO: About to set ulimit parameters in /etc/security/limits.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.conf...
INFO: Completed running Oracle Pre-Install Tasks
```

16

When the script execution is complete, enter the following to reboot the main database station:

```
# systemctl reboot
```

The station reboots.

17

When the reboot is complete, log in as the root user on the main database station.

18

Open a console window.

19

Navigate to the NFM-P software directory.

**Note:** Ensure that the directory contains only the installation files.
Enter the following:
# chmod +x *

Enter the following:
# yum install *.rpm

The yum utility resolves any package dependencies, and displays the following prompt:
Total size: nn G
Installed size: nn G
Is this ok [y/N]:

Enter y. The following and the installation status are displayed as each package is installed:
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction

The package installation is complete when the following is displayed:
Complete!

Enter the following:
# samconfig -m db

The following is displayed:
Start processing command line inputs...
<db>

Enter the following:
<db> show-detail

The database configuration is displayed.

To configure one or more parameters, enter the following; otherwise, go to Step 30:
<db> configure

The prompt changes to <db configure>. 
As required, configure the general parameters in the following table.

**Note:** The `instance` parameter is configurable only during database creation.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| ip        | Database IP address  
            | Default: IP address of primary network interface |
| instance  | Database instance name, which must:  
            | • contain 8 or fewer characters  
            | • consist of ASCII characters only  
            | • have a letter as the first character  
            | Default: maindb1 |

If required, configure one or more `passwords` parameters in the following table, and then enter `back`.

**Note:** After you save the configuration, you cannot use `samconfig` to change a database password; you must use the method described in the *NSP NFM-P System Administrator Guide*.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| user      | Database user password  
            | Default: available from technical support |
| sys       | Oracle SYS user password  
            | Default: available from technical support |

A password must:

• be between 4 and 30 characters long  
• contain at least three of the following:  
  – lower-case alphabetic character  
  – upper-case alphabetic character  
  – numeric character  
  – special character, which is one of the following: # $ _  
• not contain four or more of the same character type in sequence  
• not be the same as the user name, or the reverse of the user name
If required, enable IP validation to specify the server components that have access to the main database; configure the parameters in the following table, and then enter `back` ↓.

**Note:** When you enable IP validation on an NFM-P system that includes auxiliary servers, NSP Flow Collectors, or analytics servers, you must configure the `remote-servers` parameter; otherwise, the servers cannot reach the database.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| main-one       | IP address of main server
|                | Configuring the parameter enables IP validation.
|                | Default: —                                                                   |
| remote-servers | Comma-separated list of the IP addresses of each of the following components that must connect to the database:
|                | • auxiliary servers
|                | • NSP Flow Collectors
|                | • NSP analytics servers
|                | Default: —                                                                   |

Verify the database configuration.

1. Enter the following:
   ```
   <db configure> show-detail ↓
   ```
   The database configuration is displayed.

2. Review each parameter to ensure that the value is correct.

3. Configure one or more parameters, if required; see Chapter 3, “Using samconfig” for information about using the samconfig utility.

4. When you are certain that the configuration is correct, enter the following:
   ```
   <db configure> back ↓
   ```
   The prompt changes to `<db>`.

Enter the following to begin the database creation:

```
<db> apply ↓
```}

The database creation begins, and progress messages are displayed.

The following is displayed when the database creation is complete:

DONE
When the database creation is complete, enter the following:

```
<db> exit
```

The samconfig utility closes.

It is recommended that as a security measure, you limit the number of database user login failures that the NFM-P allows before the database user account is locked; see “NFM-P database management procedures” in the *NSP NFM-P System Administrator Guide*.

**Install standalone main server**

Log in as the root user on the main server station.

Open a console window.

Navigate to the NFM-P software directory.

**Note:** Ensure that the directory contains only the installation files.

Enter the following:

```
# chmod +x *
```

Enter the following:

```
# yum install *.rpm
```

The yum utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/N]:
```

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading packages:
Running transaction check
```
Running transaction test
Transaction test succeeded
Running transaction
The package installation is complete when the following is displayed:
Complete!

39

The initial NFM-P server installation on a station creates the nsp user account and assigns a randomly generated password.

If this is the first installation of a main server, auxiliary server, NSP analytics server, or NSP Flow Collector on the station, change the nsp password.

**Note:** The nsp password must not contain the @ symbol, or eNodeB device management may be compromised.

1. Enter the following:
   ```
   # passwd nsp
   ```
   The following prompt is displayed:
   New Password:

2. Enter a password.
   The following prompt is displayed:
   Confirm Password:

3. Re-enter the password.

4. Record the password and store it in a secure location.

40

Perform one of the following.

a. If you are deploying TLS using an NSP PKI server, perform 6.7 “To configure and enable an NSP PKI server” (p. 91).

b. If you are using the manual TLS deployment method, generate and distribute the required TLS files for the system, as described in 6.11 “Workflow for manual TLS deployment” (p. 105).

41

Enter the following:
```
# samconfig -m main
```
The following is displayed:
Start processing command line inputs...
<main>
Enter the following:

```
<main> configure
```

The prompt changes to `<main configure>`.

Enter the following:

```
<main configure> show-detail
```

The main server configuration is displayed.

As required, configure the general parameters in the following table.

**Table 7-5  Standalone main server parameters, general**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| ip        | The main server IP address  
 Default: IP address of primary network interface |
| domain    | The NFM-P system identifier  
 Default: NFM-P |
| license   | Absolute path of NFM-P license zip file  
 You cannot start a main server unless the main server configuration includes a current and valid license. You can use samconfig to specify the license file, or import a license, as described in “Software and license configuration procedures” in the *NSP NFM-P System Administrator Guide*.  
 Default: — |

As required, configure the `client` parameters in the following table, and then enter `back`.

**Table 7-6  Standalone main server parameters — client**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| nat       | Whether NAT is used between the main server and the GUI and XML API clients  
 Default: false |
### Table 7-6 Standalone main server parameters — client (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| hostname | The hostname of the main server, if NFM-P components are to use a hostname, rather than an IP address, to communicate with the main server. You must configure the parameter if one of the following is true:  
  - The main server is to use multiple interfaces for GUI and XML API client communication.  
  - NFM-P GUI and application clients are to connect to the main server using IPv4 and IPv6 interfaces.  
  - NAT is used.  
  - The NFM-P clients and the auxiliary or peer main servers use different main server interfaces.  
  If the TLS certificate contains the FQDN, you must specify the FQDN as the parameter value.  
  Default: main server hostname |
| public-ip | The IP address that the GUI and XML API clients must use to reach the main server. The parameter is configurable when the hostname parameter is unconfigured.  
  Default: — |
| jndi-port | The TCP port on the main server station to use for EJB JNDI messaging to GUI clients. It is recommended that you accept the default unless another application uses the port, or there is a firewall between the GUI clients and the main server.  
  Default: 1099 |
| delegates | A list of the client delegate servers in the NFM-P system. Use the following list format; a path value is the absolute file path of the client installation location on the client delegate server station:  
  address1;path1,address2;path2...addressN;pathN  
  **Note:** Before you can install a client delegate server using a browser, the main server configuration must include the client delegate server address and file path.  
  Default: — |

As required, configure the database parameters in the following table, and then enter **back**.

---

**NFM-P installation**  
**Standalone NFM-P system installation**  
To install a standalone NFM-P system  

**NFM-P**
**Table 7-7  Standalone main server parameters — database**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>The IP address that the main server must use to reach the database; mandatory</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>instance</td>
<td>Database instance name</td>
</tr>
<tr>
<td></td>
<td>Default: maindb1</td>
</tr>
<tr>
<td>user-password</td>
<td>Database user password</td>
</tr>
<tr>
<td></td>
<td>Default: available from technical support</td>
</tr>
<tr>
<td>backup-dest</td>
<td>The backup directory on the main database station</td>
</tr>
<tr>
<td></td>
<td>It is recommended that you specify a directory that can hold at least five times the expected database size, and can accommodate the database growth associated with network growth</td>
</tr>
<tr>
<td></td>
<td>Default: /opt/nsp/nfmp/dbbackup</td>
</tr>
<tr>
<td>backup-interval</td>
<td>How frequently, in hours, to back up the main database</td>
</tr>
<tr>
<td></td>
<td>Default: 24</td>
</tr>
<tr>
<td>backup-sets</td>
<td>The number of main database backup sets to retain</td>
</tr>
<tr>
<td></td>
<td>Default: 3</td>
</tr>
</tbody>
</table>

If the NFM-P system is to include auxiliary servers, configure the aux parameters in the following table, and then enter `back` ↓.

**Note:** At least one auxiliary server that you specify must be a Preferred auxiliary server.

**Table 7-8  Standalone main server parameters — aux**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stats</td>
<td>If enabled, specifies that one or more auxiliary servers are to be used for statistics collection</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td>calltrace</td>
<td>If enabled, specifies that one or more auxiliary servers are to be used for call-trace data collection</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td>pcmd</td>
<td>If enabled, specifies that one or more auxiliary servers are to be used for PCMD record collection</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
</tbody>
</table>
Table 7-8  Standalone main server parameters — aux  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-to-auxes</td>
<td>The main server IP address that the auxiliary servers must use to reach the main server</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>preferred-list</td>
<td>Comma-separated list of Preferred auxiliary server IP addresses</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>reserved-list</td>
<td>Comma-separated list of Reserved auxiliary server IP addresses</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>peer-list</td>
<td>Comma-separated list of Remote Standby auxiliary server IP addresses</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>calltrace-pairs</td>
<td>List of Preferred and Reserved call-trace auxiliary server pairs, in the following format; configurable when the calltrace parameter is enabled: Preferred_address1,Reserved_address1</td>
</tr>
<tr>
<td></td>
<td>If a pair includes no Reserved auxiliary server, specify the pair as shown below without the comma separator: Preferred_address</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>pcmd-pairs</td>
<td>List of Preferred and Reserved PCMD auxiliary server pairs, in the following format; configurable when the pcmd parameter is enabled: Preferred_address1,Reserved_address1</td>
</tr>
<tr>
<td></td>
<td>If a pair includes no Reserved auxiliary server, specify the pair as shown below without the comma separator: Preferred_address</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
</tbody>
</table>

As required, configure the mediation parameters in the following table, and then enter back.

Note: Some device types do not support an SNMP port value other than 162. Before you configure the snmp-port parameter to a value other than the default, you must ensure that each device type in the managed network supports the port value.
### Table 7-9  Standalone main server parameters — mediation

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nat</td>
<td>Whether NAT is used between the main server and the managed NEs</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td>snmp-ipv4</td>
<td>The IPv4 address that the managed NEs must use to reach the main server</td>
</tr>
<tr>
<td></td>
<td>Default: IPv4 address of primary network interface</td>
</tr>
<tr>
<td>snmp-ipv6</td>
<td>The IPv6 address that the managed NEs must use to reach the main server</td>
</tr>
<tr>
<td></td>
<td>Default: IPv6 address of primary network interface</td>
</tr>
<tr>
<td>snmp-port</td>
<td>The TCP port on the main server station that the managed NEs must use to</td>
</tr>
<tr>
<td></td>
<td>reach the main server</td>
</tr>
<tr>
<td></td>
<td>Default: 162</td>
</tr>
<tr>
<td>traplog-id</td>
<td>The SNMP trap log ID associated with the main server</td>
</tr>
<tr>
<td></td>
<td>Default: 98</td>
</tr>
</tbody>
</table>

Configure the `tls` parameters in the following table, and then enter `back`.

### Table 7-10  Standalone main server parameters — tls

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keystore-file</td>
<td>The absolute path of the TLS keystore file</td>
</tr>
<tr>
<td></td>
<td>To enable automated TLS deployment, enter <code>no keystore-file</code>.</td>
</tr>
<tr>
<td></td>
<td>Default: /opt/nsp/os/tls/nsp.keystore</td>
</tr>
<tr>
<td>keystore-pass</td>
<td>The TLS keystore password</td>
</tr>
<tr>
<td></td>
<td>Default: available from technical support</td>
</tr>
<tr>
<td>truststore-file</td>
<td>The absolute path of the TLS truststore file</td>
</tr>
<tr>
<td></td>
<td>To enable automated TLS deployment, enter <code>no truststore-file</code>.</td>
</tr>
<tr>
<td></td>
<td>Default: /opt/nsp/os/tls/nsp.truststore</td>
</tr>
<tr>
<td>truststore-pass</td>
<td>The TLS truststore password</td>
</tr>
<tr>
<td></td>
<td>Default: available from technical support</td>
</tr>
<tr>
<td>alias</td>
<td>The alias specified during keystore generation</td>
</tr>
<tr>
<td></td>
<td>You must configure the parameter.</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
</tbody>
</table>
### Table 7-10 Standalone main server parameters — tls (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pki-server</td>
<td>If you are using the automated TLS deployment method, the IP address or hostname of the PKI server. You must configure the parameter if no keystore-file value is specified. Default: —</td>
</tr>
<tr>
<td>pki-server-port</td>
<td>If you are using the automated TLS deployment method, the TCP port on which the PKI server listens for and services requests. Default: 2391</td>
</tr>
<tr>
<td>webdav</td>
<td>Whether WebDAV access to eNodeB activation data is enabled on the main server. Default: false</td>
</tr>
</tbody>
</table>

As required, configure the `oss` parameters in the following table, and then enter `back ↓`.

![Note: The parameters are configurable only if no auxiliary servers are specified in Step 47. Otherwise, OSS access is restricted to the auxiliary servers, which require the configuration of OSS access parameters during installation.](image)

### Table 7-11 Standalone main server parameters — oss

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>secure</td>
<td>Whether communication between the main servers and the XML API clients is secured using TLS. Default: secure</td>
</tr>
<tr>
<td>public-ip</td>
<td>The IP address that the XML API clients must use to reach the main server. Default: IP address of primary network interface</td>
</tr>
<tr>
<td>corba-3gpp</td>
<td>Whether to enable the NFM-P 3GPP interface. Default: false</td>
</tr>
<tr>
<td>xml-output</td>
<td>The directory that is to contain the output of XML API file export operations. Default: /opt/nsp/nfmp/server/xml_output</td>
</tr>
</tbody>
</table>

If the NFM-P includes an auxiliary database, configure the `auxdb` parameters in the following table, and then enter `back ↓`.
Table 7-12  Standalone main server parameters — auxdb

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enabled</td>
<td>Whether the auxiliary database is enabled in the main server configuration</td>
</tr>
<tr>
<td>ip-list</td>
<td>A comma-separated list of the auxiliary database station IP addresses that are accessible to the main server</td>
</tr>
<tr>
<td>oam-test-results</td>
<td>Whether the auxiliary database is to store OAM test results</td>
</tr>
<tr>
<td>redundancy-level</td>
<td>Boolean value that specifies whether the auxiliary database is to replicate data among multiple stations. If the auxiliary database is deployed on a single station, you must set the parameter to 0. Caution: After you configure an auxdb parameter and start the main server, you cannot modify the redundancy-level parameter. Default: 1</td>
</tr>
</tbody>
</table>

As required, configure the aa-stats parameters in the following table, and then enter back.

Table 7-13  Standalone main server parameters — aa-stats

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enabled</td>
<td>Whether the NFM-P is to collect AA accounting statistics</td>
</tr>
<tr>
<td>formats</td>
<td>AA accounting statistics file formats; the options are the following:</td>
</tr>
<tr>
<td></td>
<td>• ipdr — IPDR format</td>
</tr>
<tr>
<td></td>
<td>• ram — 5670 RAM format</td>
</tr>
<tr>
<td></td>
<td>• ipdr,ram — IPDR and 5670 RAM formats</td>
</tr>
<tr>
<td></td>
<td>The parameter is configurable when the enabled parameter is set to true.</td>
</tr>
<tr>
<td></td>
<td>Default: ram</td>
</tr>
<tr>
<td>aux-db storage</td>
<td>Whether the NFM-P is to store the statistics in an auxiliary database</td>
</tr>
<tr>
<td></td>
<td>The parameter is configurable when the enabled parameter is set to true.</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
</tbody>
</table>
Perform one of the following to specify the registry servers for NSP inter-module communication:

a. If the NSP system includes the NSD and NRC, specify the IP address of each NSD and NRC server; enter the following:

```
<main configure> registry ip-list address1;address2 back
```

where `address1` and `address2` are the public IP addresses of the NSD and NRC servers

**Note:** If the NSD and NRC system is standalone, only `address1` is required.

b. If the NSP system includes only the NFM-P, enter the following:

```
<main configure> registry ip-list address back
```

where `address` is the main server private IP address

---

Verify the main server configuration.

1. Enter the following:

```
<main configure> show-detail
```

The main server configuration is displayed.

2. Review each parameter to ensure that the value is correct.

3. Configure one or more parameters, if required.

4. When you are certain that the configuration is correct, enter the following:

```
<main configure> back
```

The prompt changes to `<main>`.

---

Enter the following:

```
<main> apply
```

The configuration is applied.

---

Enter the following:

```
<main> exit
```

The samconfig utility closes.

**Start standalone main server**

Start the main server.
Note: If you did not specify a license file during the installation, you cannot start the main server until you import a license; see “Software and license configuration procedures” in the *NSP NFM-P System Administrator Guide* for information about importing a license.

1. Log in as the nsp user on the main server station.
2. Open a console window.
3. Enter the following:
   
   bash$ cd /opt/nsp/nfmp/server/nms/bin

4. Enter the following:
   
   bash$ ./nmsserver.bash start

5. Enter the following:
   
   bash$ ./nmsserver.bash appserver_status

   The server status is displayed; the server is fully initialized if the status is the following:

   Application Server process is running. See nms_status for more detail.

   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

If the NFM-P is to manage wireless NEs, enter the following to update the memory configuration accordingly for GUI clients:

bash$ ./nmsdeploytool.bash clientmem -l

Close the console window.

Install optional components

Install and enable one or more auxiliary servers, if required; see "Auxiliary server installation" (p. 201).

Install and enable an auxiliary database, if required; see "Auxiliary database installation" (p. 223).

Install and enable one or more NSP Flow Collectors, if required; see "NSP Flow Collector installation" (p. 215).

Install and enable one or more NSP analytics servers, if required; see the NSP documentation for information.
Install GUI clients

Perform the appropriate procedures in the following chapters to install NFM-P single-user GUI clients and client delegate servers, as required:

- Chapter 14, "Single-user client deployment" — single-user client
- Chapter 15, "Client delegate server deployment" — client delegate server

See “Procedures for using the GUI” in the *NSP NFM-P User Guide* for information about using the NFM-P GUI to view and manage objects.

Stop PKI server

If you are deploying TLS using an NSP PKI server, stop the PKI server, as described at the end of 6.7 “To configure and enable an NSP PKI server” (p. 91).

Configure and enable firewalls

If you intend to use any firewalls between the NFM-P components, and the firewalls are disabled, configure and enable each required firewall.

Perform one of the following.

a. Configure each external firewall to allow the required traffic using the port assignments in the *NSP NFM-P Planning Guide*, and enable the firewall.

b. Configure and enable Firewalld on each component station, as required.
   1. Use an NFM-P template to create the Firewalld rules for the component, as described in the *NSP NFM-P Planning Guide*.
   2. Log in to the station as the root user.
   3. Open a console window.
   4. Enter the following:
      ```
      # systemctl enable firewalld
      ```
   5. Enter the following:
      ```
      # systemctl start firewalld
      ```
   6. Close the console window.

END OF STEPS
Redundant NFM-P system installation

7.5 Redundant system installation workflow

7.5.1 Description

The following is the sequence of high-level actions required to install a redundant NFM-P system.

**Note:** The link in each stage leads to a section in 7.6 “To install a redundant NFM-P system” (p. 157).

7.5.2 Stages

1. Configure firewalls between components, as required; see “Check and configure firewalls” (p. 158).

2. Download the required NFM-P installation files; see “Download installation files” (p. 159).

3. Install the primary database; see “Install primary database” (p. 159).
   1. Run a script to prepare for the Oracle software installation.
   2. Install the database packages.
   3. Create the primary database.

4. Install the standby database; see “Install standby database” (p. 166).
   1. Run a script to prepare for the Oracle software installation.
   2. Install the database packages.
   3. Create the standby database.

5. Install the primary main server; see “Install primary main server” (p. 172).
   1. Install the main server packages.
   2. Create and apply the primary main server configuration.

6. Start the primary main server; see “Start primary main server” (p. 184).

7. Install a single-user GUI client or client delegate server; see “Install GUI client” (p. 185).
8. Instantiate the standby database; see “Instantiate standby database” (p. 185).

9. Install the standby main server; see “Install standby main server” (p. 185).
   1. Install the main server packages.
   2. Create and apply the standby main server configuration.

10. Start the standby main server; see “Start standby main server” (p. 198).

11. Install one or more of the following optional components, as required; see “Install optional components” (p. 199):
   • auxiliary server
   • auxiliary database
   • NSP Flow Collector
   • NSP analytics server

12. If you are using a PKI server to deploy TLS, stop the PKI server; see “Stop PKI server” (p. 199).

13. Install additional single-user GUI clients and client delegate servers, as required; see “Install additional GUI clients” (p. 199).

14. If any required firewalls between components are disabled, enable the firewalls, as required; see “Configure and enable firewalls” (p. 199).

7.6 To install a redundant NFM-P system

7.6.1 Description
The following steps describe how to install a collocated or distributed NFM-P system in a redundant configuration. The steps also include information about installing optional NFM-P components.

Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

Note: You require root user privileges on the main database and main server stations.

Note: Performing the procedure creates the following user accounts:
7.6.2 Steps

CAUTION

Deployment failure

The RHEL OS of any NFM-P component requires specific versions of some RHEL packages. If the required package versions are not installed, the component installation fails.

See 4.10.4 “Special RHEL OS package requirements” (p. 59) for the required package versions.

Check and configure firewalls

1 Before you attempt to deploy an NFM-P system, you must ensure that each firewall between NFM-P components allows the required traffic to pass between the components, or is disabled. You can configure and enable the firewall after the installation, if required.

Note: The RHEL Firewalld service is typically enabled by default in a new RHEL OS installation.

Perform one of the following.

a. Configure each firewall to allow the required traffic to pass. See the NSP NFM-P Planning Guide for a list of the ports that must be open on each component.

Note: The RHEL Firewalld service must be configured using the Firewalld rules in the NSP NFM-P Planning Guide, which describes using NFM-P templates for rule creation.

b. Disable each firewall; see the external firewall documentation, or perform the following steps on each component station to disable Firewalld.

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following:

   # systemctl stop firewalld

4. Enter the following:

   # systemctl disable firewalld

5. Close the console window.
Download installation files

2

Download the following installation files to an empty directory on each main server station:
• nsp-nfmp-jre-\textit{R}.\textit{r}.\textit{p}-rel.\textit{v}.rpm
• nsp-nfmp-config-\textit{R}.\textit{r}.\textit{p}-rel.\textit{v}.rpm
• nsp-nfmp-nspos-\textit{R}.\textit{r}.\textit{p}-rel.\textit{v}.rpm
• nsp-nfmp-main-server-\textit{R}.\textit{r}.\textit{p}-rel.\textit{v}.rpm

where
\textit{R}.\textit{r}.\textit{p} is the NSP release identifier, in the form \textit{MAJOR}.\textit{minor}.\textit{patch}
\textit{v} is a version identifier

\textbf{i} Note: In subsequent steps, the directory is called the NFM-P software directory.

3

Perform one of the following.

a. For a collocated NFM-P deployment, download the following files to the NFM-P software directory on each station that hosts a main server and database:
• nsp-nfmp-oracle-\textit{R}.\textit{r}.\textit{p}-rel.\textit{v}.rpm
• nsp-nfmp-main-db-\textit{R}.\textit{r}.\textit{p}-rel.\textit{v}.rpm

b. For a distributed NFM-P deployment, download the following files to an empty directory on each main database station:
• nsp-nfmp-jre-\textit{R}.\textit{r}.\textit{p}-rel.\textit{v}.rpm
• nsp-nfmp-config-\textit{R}.\textit{r}.\textit{p}-rel.\textit{v}.rpm
• nsp-nfmp-oracle-\textit{R}.\textit{r}.\textit{p}-rel.\textit{v}.rpm
• nsp-nfmp-main-db-\textit{R}.\textit{r}.\textit{p}-rel.\textit{v}.rpm

\textbf{i} Note: In subsequent steps, the directory is called the NFM-P software directory.

4

Transfer the following downloaded file to an empty directory on each main database station:
• OracleSw\_PreInstall.sh

Install primary database

5

Log in as the root user on the primary main database station.

6

Open a console window.
Navigate to the directory that contains the OracleSw_PreInstall.sh file.

Enter the following:
```
# chmod +x OracleSw_PreInstall.sh
```

Enter the following:
```
#/OracleSw_PreInstall.sh
```

Note: A default value is displayed in brackets []. To accept the default, press Enter.

Note: If you specify a value other than the default, you must record the value for use when the OracleSw_PreInstall.sh script is run during a software upgrade, or when the Oracle management user information is required by technical support.

The following prompt is displayed:

This script will prepare the system for a new install/restore of an NFM-P Version Release main database.

Do you want to continue? [Yes/No]:

Enter Yes. The following prompt is displayed:

Enter the Oracle dba group name [group]:

Enter a group name.

Note: To reduce the complexity of subsequent software upgrades and technical support activities, it is recommended that you accept the default for this parameter.

The following messages and prompt are displayed:

Creating group group if it does not exist...
done

Enter the Oracle user name:

Enter a username.

Note: To reduce the complexity of subsequent software upgrades and technical support activities, it is recommended that you accept the default.

The following messages and prompt are displayed:
Oracle user [username] new home directory will be
[/opt/nsp/nfmp/oracle12r1].
Checking or Creating the Oracle user home directory
/opt/nsp/nfmp/oracle12r1..,
Checking user username...
Adding username...
Changing ownership of the directory /opt/nsp/nfmp/oracle12r1 to
username:group.
About to unlock the UNIX user [username]
Unlocking password for user username.
passwd: Success
Unlocking the UNIX user [username] completed
Please assign a password to the UNIX user username..
New Password:

Enter a password. The following prompt is displayed:
Re-enter new Password:

Re-enter the password. The following is displayed if the password change is successful:
passwd: password successfully changed for username

The following message and prompt are displayed:
Specify whether an NFM-P Main Server will be installed on this
workstation.
The database memory requirements will be adjusted to account for the
additional load.
Will the database co-exist with an NFM-P Main Server on this
workstation [Yes/No]:

Enter Yes or No, as required.
Messages like the following are displayed as the script execution completes:
INFO: About to set kernel parameters in /etc/sysctl.conf...
INFO: Completed setting kernel parameters in /etc/sysctl.conf...
INFO: About to change the current values of the kernel parameters
INFO: Completed changing the current values of the kernel parameters
INFO: About to set ulimit parameters in /etc/security/limits.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.conf...
INFO: Completed running Oracle Pre-Install Tasks

16
When the script execution is complete, enter the following to reboot the primary main database station:

```bash
# systemctl reboot
```
The station reboots.

17
When the reboot is complete, log in as the root user on the primary main database station.

18
Open a console window.

19
Navigate to the NFM-P software directory.

ℹ️ Note: Ensure that the directory contains only the installation files.

20
Enter the following:

```bash
# chmod +x *
```

21
Enter the following:

```bash
# yum install *.rpm
```
The yum utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/N]:
```

22
Enter y. The following and the installation status are displayed as each package is installed:

- Downloading packages:
- Running transaction check
- Running transaction test
- Transaction test succeeded
- Running transaction

The package installation is complete when the following is displayed:

```
Complete!
```
Enter the following:

```bash
# samconfig -m db
```

The following is displayed:

```
Start processing command line inputs...
<db>
```

Enter the following:

```
<db> show-detail
```

The primary database configuration is displayed.

Enter the following:

```
<db> configure
```

The prompt changes to `<db configure>`.

As required, configure the general parameters in the following table.

**Note:** The `instance` parameter is configurable only during database creation.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>Primary database IP address&lt;br&gt;Default: IP address of primary network interface</td>
</tr>
<tr>
<td>instance</td>
<td>Primary database instance name, which must:&lt;br&gt;• contain 8 or fewer characters&lt;br&gt;• consist of ASCII characters only&lt;br&gt;• have a letter as the first character&lt;br&gt;Default: maindb1</td>
</tr>
</tbody>
</table>

Configure the `redundant` parameters in the following table, and then enter `back`.

**Note:** The `instance` parameter is configurable only during database creation.
Table 7-15  Primary database parameters — redundant

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| ip        | Standby database IP address  
Default: — |
| instance  | Standby database instance name, which must:  
• contain 8 or fewer characters  
• consist of ASCII characters only  
• have a letter as the first character  
Default: maindb2 |

If required, configure one or more passwords parameters in the following table, and then enter back ".

Note: After you save the configuration, you cannot use samconfig to change a database password; you must use the method described in the NSP NFM-P System Administrator Guide.

Table 7-16  Primary database parameters — passwords

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| user      | Database user password  
Default: available from technical support |
| sys       | Oracle SYS user password  
Default: available from technical support |

A password must:  
• be between 4 and 30 characters long  
• contain at least three of the following:  
  – lower-case alphabetic character  
  – upper-case alphabetic character  
  – numeric character  
  – special character, which is one of the following: # $ _  
• not contain four or more of the same character type in sequence  
• not be the same as the user name, or the reverse of the user name  
• not contain a space character
If required, configure the \texttt{ip-validation} parameters in the following table to enable IP validation, which restricts database access to only the specified servers, and then enter \texttt{back}.

\begin{itemize}
  \item \textbf{Note:} When you enable IP validation on an NFM-P system that includes auxiliary servers, NSP Flow Collectors, or analytics servers, you must configure the \texttt{remote-servers} parameter; otherwise, the servers cannot reach the database.
\end{itemize}

\textbf{Table 7-17} Primary database parameters — \texttt{ip-validation}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>main-one</td>
<td>IP address of primary main server Configuring the parameter enables IP validation. Default:—</td>
</tr>
<tr>
<td>main-two</td>
<td>IP address of standby main server Default:—</td>
</tr>
</tbody>
</table>
| remote-servers | Comma-separated list of the IP addresses of each of the following components that must connect to the database:  
  - auxiliary servers  
  - NSP Flow Collectors  
  - NSP analytics servers Default:— |

Verify the database configuration.

1. Enter the following:
   \begin{verbatim}
   <db configure> show-detail
   \end{verbatim}
   The database configuration is displayed.

2. Review each parameter to ensure that the value is correct.

3. Configure one or more parameters, if required; see Chapter 3, “Using \texttt{samconfig}” for information about using the \texttt{samconfig} utility.

4. When you are certain that the configuration is correct, enter the following:
   \begin{verbatim}
   <db configure> back
   \end{verbatim}
   The prompt changes to \texttt{<db>}. 

Enter the following to begin the database creation:

\begin{verbatim}
<db> apply
\end{verbatim}

The database creation begins, and progress messages are displayed.

The following is displayed when the database creation is complete:
DONE

32

When the database creation is complete, enter the following:

\texttt{<db> exit \downarrow}

The samconfig utility closes.

33

It is recommended that as a security measure, you limit the number of database user login failures that the NFM-P allows before the database user account is locked; see "NFM-P database management procedures" in the \textit{NSP NFM-P System Administrator Guide}.

\textbf{Install standby database}

34

Log in as the root user on the standby main database station.

35

Open a console window.

36

Navigate to the directory that contains the OracleSw_PreInstall.sh file.

37

Enter the following:

\texttt{# chmod +x OracleSw_PreInstall.sh \downarrow}

38

Enter the following:

\texttt{# ./OracleSw_PreInstall.sh \downarrow}

\textbf{Note:} A default value is displayed in brackets []. To accept the default, press \texttt{\downarrow}.

\textbf{Note:} If you specify a value other than the default, you must record the value for use when the OracleSw_PreInstall.sh script is run during a software upgrade, or when the Oracle management user information is required by technical support.

The following prompt is displayed:

\textit{This script will prepare the system for a new install/restore of an NFM-P Version Release main database. Do you want to continue? [Yes/No]:}
Enter Yes. The following prompt is displayed:

Enter the Oracle dba group name [group]:

Enter a group name.

Note: The group name must match the group name specified during the primary database installation.

The following messages and prompt are displayed:

Creating group group if it does not exist... done

Enter the Oracle user name:

Enter a username.

Note: The username must match the username specified during the primary database installation.

The following messages and prompt are displayed:

Oracle user [username] new home directory will be [/opt/nsp/nfmp/oracle12r1].
Checking or Creating the Oracle user home directory /opt/nsp/nfmp/oracle12r1...,
Checking user username...,
Adding username...,
Changing ownership of the directory /opt/nsp/nfmp/oracle12r1 to username:group.
About to unlock the UNIX user [username]
Unlocking password for user username.
passwd: Success
Unlocking the UNIX user [username] completed
Please assign a password to the UNIX user username..
New Password:

Enter a password.

Note: The password must match the password specified during the primary database installation.

The following prompt is displayed:
Re-enter new Password:

43

Re-enter the password. The following is displayed if the password change is successful:

```
passwd: password successfully changed for username
```

The following message and prompt are displayed:

Specify whether an NFM-P Main Server will be installed on this workstation.

The database memory requirements will be adjusted to account for the additional load.

Will the database co-exist with an NFM-P Main Server on this workstation [Yes/No]:

44

Enter Yes or No, as required.

Messages like the following are displayed as the script execution completes:

```
INFO: About to set kernel parameters in /etc/sysctl.conf...
INFO: Completed setting kernel parameters in /etc/sysctl.conf...
INFO: About to change the current values of the kernel parameters
INFO: Completed changing the current values of the kernel parameters
INFO: About to set ulimit parameters in /etc/security/limits.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.conf...
INFO: Completed running Oracle Pre-Install Tasks
```

45

When the script execution is complete, enter the following to reboot the standby main database station:

```
# systemctl reboot
```

The station reboots.

46

When the reboot is complete, log in as the root user on the standby main database station.

47

Open a console window.

48

Navigate to the NFM-P software directory.

Note: Ensure that the directory contains only the installation files.
Enter the following:
# chmod +x *

Enter the following:
# yum install *.rpm
The yum utility resolves any package dependencies, and displays the following prompt:
Total size: nn G
Installed size: nn G
Is this ok [y/N]:

Enter y. The following and the installation status are displayed as each package is installed:
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
The package installation is complete when the following is displayed:
Complete!

Enter the following:
# samconfig -m db
The following is displayed:
Start processing command line inputs...
<db>

Enter the following:
<db> configure type standby
The prompt changes to <db configure>.

If required, configure the ip parameter; enter the following:

Note: The default is the IP address of the primary network interface on the station.
<db configure> ip address
where *address* is the IP address of this database

55

Enter the following:

```
<db configure> redundant ip address 
```

where *address* is the IP address of the primary database

The prompt changes to `<db configure redundant>`.

56

Enter the following, and then enter `back` ↓:

```
<db configure redundant> instance instance_name 
```

where *instance_name* is the primary database instance name

57

If required, configure one or more passwords parameters in the following table, and then enter `back` ↓.

**Note:** After you save the configuration, you cannot use `samconfig` to change a database password; you must use the method described in the *NSP NFM-P System Administrator Guide*.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| user | Database user password; the password must match the password specified during the primary database installation  

Default: available from technical support |
| sys | Oracle SYS user password; the password must match the password specified during the primary database installation  

Default: available from technical support |

58

If required, enable IP validation to specify the server components that have access to the main database; configure the parameters in the following table, and then enter `back` ↓.

**Note:** When you enable IP validation on an NFM-P system that includes auxiliary servers, NSP Flow Collectors, or analytics servers, you must configure the `remote-servers` parameter; otherwise, the servers cannot reach the database.
Table 7-19  Standby database parameters — ip-validation

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| main-one       | IP address of primary main server  
Configuring the parameter enables IP validation.  
Default: — |
| main-two       | IP address of standby main server  
Default: — |
| remote-servers | Comma-separated list of the IP addresses of each of the following components that must connect to the database:  
• auxiliary servers  
• NSP Flow Collectors  
• NSP analytics servers  
Default: — |

59 Verify the database configuration.
1. Enter the following:
   `<db configure> show-detail`  
The database configuration is displayed.
   **Note:** The `instance` value is not set until the database is reinstated later in the procedure.
2. Review each parameter to ensure that the value is correct.
3. Configure one or more parameters, if required; see Chapter 3, “Using samconfig” for information about using the samconfig utility.
4. When you are certain that the configuration is correct, enter the following:
   `<db configure> back`  
The prompt changes to `<db>`.  

60 Enter the following to begin the database creation:
   `<db> apply`  
The database creation begins, and progress messages are displayed.  
The following is displayed when the database creation is complete:
   **DONE**  
   `db configurations updated`.  

61 When the database creation is complete, enter the following:
Install primary main server

Log in as the root user on the primary main server station.

Open a console window.

Navigate to the NFM-P software directory.

Note: Ensure that the directory contains only the installation files.

Enter the following:

```
# chmod +x *
```

Enter the following:

```
# yum install *.rpm
```

The yum utility resolves any package dependencies, and displays the following prompt:

```
Total size:nnG
Installed size:nnG
Is this ok [y/N]:
```

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
```

The package installation is complete when the following is displayed:

```
Complete!
```
The initial NFM-P server installation on a station creates the nsp user account and assigns a randomly generated password.

If this is the first installation of a main server, auxiliary server, NSP analytics server, or NSP Flow Collector on the station, change the nsp password.

**Note:** The nsp password must not contain the @ symbol, or eNodeB device management may be compromised.

1. Enter the following:
   ```
   # passwd nsp
   ```
   The following prompt is displayed:
   ```
   New Password:
   ```
2. Enter a password.
   The following prompt is displayed:
   ```
   Confirm Password:
   ```
3. Re-enter the password.
4. Record the password and store it in a secure location.

Perform one of the following.

a. If you are deploying TLS using an NSP PKI server, perform 6.7 “To configure and enable an NSP PKI server” (p. 91).

b. If you are using the manual TLS deployment method, generate and distribute the required TLS files for the system, as described in 6.11 “Workflow for manual TLS deployment” (p. 105).

Enter the following:
```
# samconfig -m main
```

The following is displayed:
```
Start processing command line inputs...
<main>
```

Enter the following:
```
<main> configure
```

The prompt changes to `<main configure>`.

As required, configure the general parameters in the following table.
Table 7-20  Primary main server parameters, general

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>The primary main server IP address&lt;br&gt;Default: IP address of primary network interface</td>
</tr>
<tr>
<td>domain</td>
<td>The NFM-P system identifier&lt;br&gt;Default: NFM-P</td>
</tr>
<tr>
<td>license</td>
<td>Absolute path of NFM-P license zip file&lt;br&gt;You cannot start a main server unless the main server configuration includes a current and valid license. You can use samconfig to specify the license file, or import a license, as described in &quot;Software and license configuration procedures&quot; in the NSP NFM-P System Administrator Guide.&lt;br&gt;Default: —</td>
</tr>
</tbody>
</table>

As required, configure the client parameters in the following table, and then enter back ↓.

Table 7-21  Primary main server parameters — client

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nat</td>
<td>Whether NAT is used between the main servers and the GUI and XML API clients&lt;br&gt;Default: false</td>
</tr>
<tr>
<td>hostname</td>
<td>The primary main server hostname, if NFM-P components are to use hostnames, rather than IP addresses, for communication with the main servers&lt;br&gt;You must configure the parameter if one of the following is true:&lt;br&gt;• The main server is to use multiple interfaces for GUI and XML API client communication.&lt;br&gt;• NFM-P GUI and application clients are to connect to the main server using IPv4 and IPv6 interfaces.&lt;br&gt;• NAT is used.&lt;br&gt;• The NFM-P clients and the auxiliary or peer main servers use different main server interfaces.&lt;br&gt;If the TLS certificate contains the FQDN, you must specify the FQDN as the parameter value.&lt;br&gt;Default: main server hostname</td>
</tr>
</tbody>
</table>
Table 7-21  Primary main server parameters — client  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>public-ip</td>
<td>The IP address that the GUI and XML API clients must use to reach the primary main server&lt;br&gt;The parameter is configurable when the hostname parameter is unconfigured.&lt;br&gt;Default: —</td>
</tr>
<tr>
<td>jndi-port</td>
<td>The TCP port on the primary main server station to use for EJB JNDI messaging to GUI clients&lt;br&gt;It is strongly recommended that you accept the default unless another application uses the port, or there is a firewall between the GUI clients and the primary main server.&lt;br&gt;Default: 1099</td>
</tr>
<tr>
<td>delegates</td>
<td>A list of the client delegate servers in the NFM-P system&lt;br&gt;Use the following list format; a path value is the absolute file path of the client installation location on the client delegate server station: address1;path1,address2;path2...addressN;pathN&lt;br&gt;Note: Before you can install a client delegate server using a browser, each main server configuration must include the client delegate server address and file path.&lt;br&gt;Default: —</td>
</tr>
</tbody>
</table>

Configure the database parameters in the following table, and then enter back ↓.

Table 7-22  Primary main server parameters — database

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>The IP address that the primary main server must use to reach the primary database&lt;br&gt;Default: —</td>
</tr>
<tr>
<td>instance</td>
<td>Primary database instance name&lt;br&gt;Default: maindb1</td>
</tr>
<tr>
<td>user-password</td>
<td>Primary database user password&lt;br&gt;Default: available from technical support</td>
</tr>
<tr>
<td>backup-dest</td>
<td>The backup directory on the primary main database station&lt;br&gt;It is recommended that you specify a directory that can hold at least five times the expected database size, and can accommodate the database growth associated with network growth&lt;br&gt;Default: /opt/nsp/nfmp/dbbackup</td>
</tr>
</tbody>
</table>
Table 7-22  Primary main server parameters — database  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backup-interval</td>
<td>How frequently, in hours, to back up the main database</td>
</tr>
<tr>
<td></td>
<td>Default: 24</td>
</tr>
<tr>
<td>backup-sets</td>
<td>The number of main database backup sets to retain</td>
</tr>
<tr>
<td></td>
<td>Default: 3</td>
</tr>
</tbody>
</table>

If the NFM-P system is to include auxiliary servers, configure the aux parameters in the following table, and then enter back ↓.

**Note:** At least one auxiliary server that you specify must be a Preferred auxiliary server.

Table 7-23  Primary main server parameters — aux

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stats</td>
<td>If enabled, specifies that one or more auxiliary servers are to be used for statistics collection</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td>calltrace</td>
<td>If enabled, specifies that one or more auxiliary servers are to be used for call-trace data collection</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td>pcmd</td>
<td>If enabled, specifies that one or more auxiliary servers are to be used for PCMD record collection</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td>ip-to-auxes</td>
<td>The primary main server IP address that the auxiliary servers must use to reach the primary main server</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>preferred-list</td>
<td>Comma-separated list of Preferred auxiliary server IP addresses</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>reserved-list</td>
<td>Comma-separated list of Reserved auxiliary server IP addresses</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>peer-list</td>
<td>Comma-separated list of Remote auxiliary server IP addresses</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
</tbody>
</table>
Table 7-23  Primary main server parameters — aux (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| calltrace-pairs | List of Preferred and Reserved call-trace auxiliary server pairs, in the following format; configurable when the calltrace parameter is enabled:  
Preferred_address1,Reserved_address1|Preferred_address2,Reserved_address2...Preferred_addressN,Reserved_addressN  
If a pair includes no Reserved auxiliary server, specify the pair as shown below without the comma separator:  
Preferred_address| Default: — |
| pcmd-pairs | List of Preferred and Reserved PCMD auxiliary server pairs, in the following format; configurable when the pcmd parameter is enabled:  
Preferred_address1,Reserved_address1|Preferred_address2,Reserved_address2...Preferred_addressN,Reserved_addressN  
If a pair includes no Reserved auxiliary server, specify the pair as shown below without the comma separator:  
Preferred_address| Default: — |

Enter the following:
<main> configure redundancy enabled</main>

The prompt changes to <main configure redundancy>.

Configure the general redundancy parameters in the following table.

Table 7-24  Primary main server parameters — redundancy

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| ip-to-peer | The primary main server IP address that the standby main server must use for general communication  
Default: IP address of primary network interface |
| rsync-ip  | The primary main server IP address that the standby main server must use for data synchronization  
Default: IP address of primary network interface |

Configure the database redundancy parameters in the following table, and then enter back ↓.
### Table 7-25 Primary main server parameters — redundancy, database

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>The IP address that the primary main server must use to reach the standby database. Default: —</td>
</tr>
<tr>
<td>instance</td>
<td>The standby database instance name. Default: —</td>
</tr>
<tr>
<td>backup-sync</td>
<td>Whether database backup file synchronization is enabled. When the parameter is enabled, each database backup file set is copied to the peer main database station after the backup completes. You must ensure that there is sufficient network bandwidth between the main database stations before you enable this parameter. See the <em>NSP NFM-P Planning Guide</em> for information about the bandwidth requirements of database backup file synchronization. You must set the parameter to the same value on each main server. Default: false</td>
</tr>
<tr>
<td>alignment</td>
<td>Whether automatic database alignment is enabled. If automatic database alignment is enabled, a main server and database attempt to assume a common role, primary or standby, after an event such as a server activity switch or database failover. In a geographically dispersed system, the function helps to ensure that a main server communicates with the local database in order to reduce the network latency between the components. For more information about database alignment, see the <em>NSP NFM-P System Administrator Guide</em>. Default: false</td>
</tr>
<tr>
<td>prefer-instance</td>
<td>The name of the database instance with which the primary main server is to align. The parameter is configurable when the alignment parameter is enabled. Default: —</td>
</tr>
<tr>
<td>reinstatement-delay</td>
<td>The delay, in minutes, between the completion of a database failover and the automatic reinstatement of the standby database. A value of 0 disables automatic database reinstatement. Default: 60</td>
</tr>
</tbody>
</table>

Configure the peer-server redundancy parameters in the following table, and then enter back ↓.
Table 7-26  Primary main server parameters — redundancy, peer-server

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>The standby main server IP address that the primary main server uses for general communication. Default: —</td>
</tr>
<tr>
<td>hostname</td>
<td>The standby main server hostname that the primary main server uses for general communication. The parameter is configurable and mandatory when the hostname parameter in Step 73 is configured. If the TLS certificate contains the FQDN, you must specify the FQDN as the parameter value. Default: —</td>
</tr>
<tr>
<td>rsync-ip</td>
<td>The standby main server IP address that the primary main server uses for data synchronization. Default: —</td>
</tr>
<tr>
<td>public-ip</td>
<td>The IP address that the GUI and XML API clients must use to reach the standby main server. Default: —</td>
</tr>
<tr>
<td>jndi-port</td>
<td>The TCP port on the standby main server station used for EJB JNDI messaging to GUI clients. It is recommended that you accept the default unless another application uses the port, or there is a firewall between the GUI clients and the standby main server. Default: 1099</td>
</tr>
<tr>
<td>ip-to-auxes</td>
<td>The standby main server IP address that the auxiliary servers must use to reach the standby main server. You must configure the parameter if the NFM-P system includes one or more auxiliary servers. Default: —</td>
</tr>
<tr>
<td>snmp-ipv4</td>
<td>The IPv4 address that the managed NEs must use to reach the standby main server</td>
</tr>
<tr>
<td>snmp-ipv6</td>
<td>The IPv6 address that the managed NEs must use to reach the standby main server</td>
</tr>
<tr>
<td>snmp-port</td>
<td>The TCP port on the standby main server station used for SNMP communication with the managed NEs. Default: 162</td>
</tr>
<tr>
<td>traplog-id</td>
<td>The SNMP trap log ID associated with the standby main server. Default: 98</td>
</tr>
</tbody>
</table>
Enter `back ↓`. The prompt changes to `<main configure>`.

As required, configure the `mediation` parameters in the following table, and then enter `back ↓`.

**Note:** Some device types do not support an SNMP port value other than 162. Before you configure the `snmp-port` parameter to a value other than the default, you must ensure that each device type in the managed network supports the port value.

**Table 7-27** Primary main server parameters — mediation

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nat</td>
<td>Whether NAT is used between the main servers and the managed NEs</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td>snmp-ipv4</td>
<td>The IPv4 address that the managed NEs must use to reach the primary main</td>
</tr>
<tr>
<td></td>
<td>server</td>
</tr>
<tr>
<td></td>
<td>Default: IPv4 address of primary network interface</td>
</tr>
<tr>
<td>snmp-ipv6</td>
<td>The IPv6 address that the managed NEs must use to reach the primary main</td>
</tr>
<tr>
<td></td>
<td>server</td>
</tr>
<tr>
<td></td>
<td>Default: IPv6 address of primary network interface</td>
</tr>
<tr>
<td>snmp-port</td>
<td>The TCP port on the primary main server station that the managed NEs</td>
</tr>
<tr>
<td></td>
<td>must use to reach the primary main server</td>
</tr>
<tr>
<td></td>
<td>Default: 162</td>
</tr>
<tr>
<td>traplog-id</td>
<td>The SNMP trap log ID associated with the primary main server</td>
</tr>
<tr>
<td></td>
<td>Default: 98</td>
</tr>
</tbody>
</table>

If required, configure the `tls` parameters in the following table, and then enter `back ↓`.

**Table 7-28** Primary main server parameters — tls

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keystore-file</td>
<td>The absolute path of the TLS keystore file</td>
</tr>
<tr>
<td></td>
<td>To enable automated TLS deployment, enter <code>no keystore-file</code>.</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>keystore-pass</td>
<td>The TLS keystore password</td>
</tr>
<tr>
<td></td>
<td>Default: available from technical support</td>
</tr>
</tbody>
</table>
Table 7-28  Primary main server parameters — tls  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>truststore-file</td>
<td>The absolute path of the TLS truststore file</td>
</tr>
<tr>
<td></td>
<td>To enable automated TLS deployment, enter no truststore-file.</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>truststore-pass</td>
<td>The TLS truststore password</td>
</tr>
<tr>
<td></td>
<td>Default: available from technical support</td>
</tr>
<tr>
<td>alias</td>
<td>The alias specified during keystore generation</td>
</tr>
<tr>
<td></td>
<td>You must configure the parameter.</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>pki-server</td>
<td>If you are using the automated TLS deployment method, the IP address or host name of the PKI server</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>pki-server-port</td>
<td>If you are using the automated TLS deployment method, the TCP port on which the PKI server listens for and services requests</td>
</tr>
<tr>
<td></td>
<td>Default: 2391</td>
</tr>
<tr>
<td>webdav</td>
<td>Whether WebDAV access to eNodeB activation data is enabled</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
</tbody>
</table>

As required, configure the oss parameters in the following table, and then enter back.

Table 7-29  Primary main server parameters — oss

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>secure</td>
<td>Whether communication between the main servers and the XML API clients is secured using TLS</td>
</tr>
<tr>
<td></td>
<td>Default: secure</td>
</tr>
<tr>
<td>public-ip</td>
<td>The IP address that the XML API clients must use to reach the primary main server</td>
</tr>
<tr>
<td></td>
<td>Default: IP address of primary network interface</td>
</tr>
<tr>
<td>corba-3gpp</td>
<td>Whether the NFM-P 3GPP interface is enabled</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
</tbody>
</table>
If the NFM-P includes an auxiliary database, configure the `auxdb` parameters in the following table, and then enter `back` ↓.

**Table 7-30 Primary main server parameters — auxdb**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enabled</td>
<td>Whether the auxiliary database is enabled in the main server configuration</td>
</tr>
<tr>
<td>ip-list</td>
<td>A comma-separated list of the auxiliary database station IP addresses that are accessible to the main server</td>
</tr>
<tr>
<td>oam-test-results</td>
<td>Whether the auxiliary database is to store OAM test results</td>
</tr>
<tr>
<td>redundancy-level</td>
<td>Boolean value that specifies whether the auxiliary database is to replicate data among multiple stations</td>
</tr>
<tr>
<td></td>
<td>If the auxiliary database is deployed on a single station, you must set the parameter to 0.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution:</strong> After you configure an <code>auxdb</code> parameter and start the main server, you cannot modify the <code>redundancy-level</code> parameter.</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
</tbody>
</table>

---

As required, configure the `aa-stats` parameters in the following table, and then enter `back` ↓.

**Table 7-31 Primary main server parameters — aa-stats**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enabled</td>
<td>Whether the NFM-P is to collect AA accounting statistics</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
</tbody>
</table>
Table 7-31 Primary main server parameters — aa-stats (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>formats</td>
<td>AA accounting statistics file formats; the options are the following:</td>
</tr>
<tr>
<td></td>
<td>• ipdr — IPDR format</td>
</tr>
<tr>
<td></td>
<td>• ram — 5670 RAM format</td>
</tr>
<tr>
<td></td>
<td>• ipdr,ram — IPDR and 5670 RAM formats</td>
</tr>
<tr>
<td></td>
<td>The parameter is configurable when the enabled parameter is set to true.</td>
</tr>
<tr>
<td></td>
<td>Default: ram</td>
</tr>
<tr>
<td>aux-db storage</td>
<td>Whether the NFM-P is to store the statistics in an auxiliary database</td>
</tr>
<tr>
<td></td>
<td>The parameter is configurable when the enabled parameter is set to true.</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
</tbody>
</table>

Perform one of the following to specify the registry servers for NSP inter-module communication:

a. If the NSP system includes the NSD and NRC, specify the IP address of each NSD and NRC server; enter the following:

```
<main configure> registry ip-list address1;address2 back
```

where address1 and address2 are the public IP addresses of the NSD and NRC servers

**Note:** If the NSD and NRC system is standalone, only address1 is required.

b. If the NSP system includes only the NFM-P, enter the following:

```
<main configure> registry ip-list address1;address2 back
```

where address1 and address2 are the IP addresses that the NFM-P main servers use to communicate with each other

Verify the main server configuration.

1. Enter the following:

```
<main configure> show-detail
```

The main server configuration is displayed.

2. Review each parameter to ensure that the value is correct.

3. Configure one or more parameters, if required.

4. When you are certain that the configuration is correct, enter the following:

```
<main configure> back
```

The prompt changes to <main>.
Enter the following:
<main> apply <
The configuration is applied.

Enter the following:
<main> exit <
The samconfig utility closes.

Start primary main server

Start the primary main server.

**Note:** If you did not specify a license file during the installation, you cannot start the main server until you import a license. See “Software and license configuration procedures” in the *NSP NFM-P System Administrator Guide* for information about importing a license.

1. Log in as the nsp user on the main server station.
2. Open a console window.
3. Enter the following:
   bash$ cd /opt/nsp/nfmp/server/nms/bin <
4. Enter the following:
   bash$ ./nmsserver.bash start <
5. Enter the following:
   bash$ ./nmsserver.bash appserver_status <
The server status is displayed; the server is fully initialized if the status is the following:

Application Server process is running. See nms_status for more detail.

If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

If the NFM-P is to manage wireless NEs, enter the following to update the memory configuration accordingly for GUI clients:

bash$ ./nmsdeploytool.bash clientmem -l

Close the console window.
Install GUI client

Performs the appropriate procedure in one of the following chapters to install an NFM-P single-user GUI client or client delegate server:

- **Chapter 14, “Single-user client deployment”** — single-user client
- **Chapter 15, “Client delegate server deployment”** — client delegate server

See “Procedures for using the GUI” in the *NSP NFM-P User Guide* for information about using the NFM-P GUI to view and manage objects.

Instantiate standby database

Opens an NFM-P GUI client as the admin user.

Choose Administration→System Information from the main menu. The System Information form opens.

Click Re-Instantiate Standby.

Click Yes to confirm the action. The instantiation begins, and the GUI status bar displays the current phase of the operation.

**Note:** Database instantiation takes considerable time if the database contains a large amount of statistics data.

You can also use the System Information form to monitor the operation progress. The Last Attempted Standby Re-instantiation Time is the start time; the Standby Re-instantiation State changes from In Progress to Success when the instantiation is complete.

When the instantiation is complete, close the System Information form.

Install standby main server

Logs in as the root user on the standby main server station.

Open a console window.
Navigate to the NFM-P software directory.

Note: Ensure that the directory contains only the installation files.

Enter the following:

```
# chmod +x *
```

Enter the following:

```
# yum install *.rpm
```

The `yum` utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/N]:
```

Enter `y`. The following and the installation status are displayed as each package is installed:

- Downloading packages:
- Running transaction check
- Running transaction test
- Transaction test succeeded
- Running transaction

The package installation is complete when the following is displayed:

```
Complete!
```

The initial NFM-P server installation on a station creates the `nsp` user account and assigns a randomly generated password.

If this is the first installation of a main server, auxiliary server, NSP analytics server, or NSP Flow Collector on the station, change the `nsp` password.

Note: The `nsp` password must not contain the `@` symbol, or eNodeB device management may be compromised.

1. Enter the following:

```
# passwd nsp
```

The following prompt is displayed:

```
New Password:
```

2. Enter a password.
The following prompt is displayed:

```
Confirm Password:
```

3. Re-enter the password.
4. Record the password and store it in a secure location.

---

Enter the following:
```
# samconfig -m main
```

The following is displayed:
```
Start processing command line inputs...
<main>
```

---

Enter the following:
```
<main> configure
```

The prompt changes to `<main configure>`.

---

As required, configure the general parameters in the following table.

**Table 7-32  Standby main server parameters, general**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| ip        | The standby main server IP address  
Default: IP address of primary network interface |
| domain    | The NFM-P system identifier  
Default: NFM-P |
| license   | Absolute path of NFM-P license zip file  
You cannot start a main server unless the main server configuration includes a current and valid license. You can use samconfig to specify the license file, or import a license, as described in “Software and license configuration procedures” in the **NSP NFM-P System Administrator Guide**.  
Default: — |

---

As required, configure the **client** parameters in the following table, and then enter `back`.

---
### Table 7-33  Standby main server parameters — client

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| nat        | Whether NAT is used between the main servers and the GUI and XML API clients  
            | Default: false |
| hostname   | The standby main server hostname, if NFM-P components are to use hostnames, rather than IP addresses, for communication with the main servers  
            | You must configure the parameter if one of the following is true:  
            | • The main server is to use multiple interfaces for GUI and XML API client communication.  
            | • NFM-P GUI and application clients are to connect to the main server using IPv4 and IPv6 interfaces.  
            | • NAT is used.  
            | • The NFM-P clients and the auxiliary or peer main servers use different main server interfaces.  
            | If the TLS certificate contains the FQDN, you must specify the FQDN as the parameter value.  
            | Default: main server hostname |
| public-ip  | The IP address that the GUI and XML API clients must use to reach the standby main server  
            | The parameter is configurable when the hostname parameter is unconfigured.  
            | Default: — |
| jndi-port  | The TCP port on the standby main server station to use for EJB JNDI messaging to GUI clients  
            | It is recommended that you accept the default unless another application uses the port, or there is a firewall between the GUI clients and the standby main server.  
            | Default: 1099 |
| delegates  | A list of the client delegate servers in the NFM-P system  
            | Use the following list format; a path value is the absolute file path of the client installation location on the client delegate server station:  
            | address1;path1,address2;path2...addressN;pathN  
            | **Note:** Before you can install a client delegate server using a browser, each main server configuration must include the client delegate server address and file path.  
            | Default: — |

Configure the **database** parameters in the following table, and then enter `back` ↓.
### Table 7-34  Standby main server parameters — database

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>The IP address that the standby main server must use to reach the standby database</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>instance</td>
<td>Standby database instance name</td>
</tr>
<tr>
<td></td>
<td>You must set this parameter to the same value as the instance parameter in step <a href="#">Step 78</a>.</td>
</tr>
<tr>
<td></td>
<td>Default: maindb1</td>
</tr>
<tr>
<td>user-password</td>
<td>Standby database user password</td>
</tr>
<tr>
<td></td>
<td>Default: available from technical support</td>
</tr>
<tr>
<td>backup-dest</td>
<td>The backup directory on the primary main database station</td>
</tr>
<tr>
<td></td>
<td>It is recommended that you specify a directory that can hold at least five times the expected database size, and can accommodate the database growth associated with network growth</td>
</tr>
<tr>
<td></td>
<td>Default: /opt/nsp/nfmp/dbbackup</td>
</tr>
<tr>
<td>backup-interval</td>
<td>How frequently, in hours, to back up the main database</td>
</tr>
<tr>
<td></td>
<td>Default: 24</td>
</tr>
<tr>
<td>backup-sets</td>
<td>The number of main database backup sets to retain</td>
</tr>
<tr>
<td></td>
<td>Default: 3</td>
</tr>
</tbody>
</table>

If the NFM-P system is to include auxiliary servers, configure the aux parameters in the following table, and then enter `back 5`.

**Note:** At least one auxiliary server that you specify must be a Preferred auxiliary server.

### Table 7-35  Standby main server parameters — aux

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stats</td>
<td>If enabled, specifies that one or more auxiliary servers are to be used for statistics collection</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td>calltrace</td>
<td>If enabled, specifies that one or more auxiliary servers are to be used for call-trace data collection</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td>pcmd</td>
<td>If enabled, specifies that one or more auxiliary servers are to be used for PCMD record collection</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
</tbody>
</table>
### Table 7-35  Standby main server parameters — aux  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-to-auxes</td>
<td>The standby main server IP address that the auxiliary servers must use to reach the standby main server</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>preferred-list</td>
<td>Comma-separated list of Preferred auxiliary server IP addresses</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>reserved-list</td>
<td>Comma-separated list of Reserved auxiliary server IP addresses</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>peer-list</td>
<td>Comma-separated list of Remote auxiliary server IP addresses</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>calltrace-pairs</td>
<td>List of Preferred and Reserved call-trace auxiliary server pairs, in the following format; configurable when the calltrace parameter is enabled:</td>
</tr>
<tr>
<td></td>
<td>Preferred_address1,Reserved_address1</td>
</tr>
<tr>
<td></td>
<td>If a pair includes no Reserved auxiliary server, specify the pair as shown below without the comma separator:</td>
</tr>
<tr>
<td></td>
<td>Preferred_address</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>pcmd-pairs</td>
<td>List of Preferred and Reserved PCMD auxiliary server pairs, in the following format; configurable when the pcmd parameter is enabled:</td>
</tr>
<tr>
<td></td>
<td>Preferred_address1,Reserved_address1</td>
</tr>
<tr>
<td></td>
<td>If a pair includes no Reserved auxiliary server, specify the pair as shown below without the comma separator:</td>
</tr>
<tr>
<td></td>
<td>Preferred_address</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
</tbody>
</table>

112 Enter the following:

```
<main> configure redundancy enabled
```

The prompt changes to `<main configure redundancy>.

113 Configure the general redundancy parameters in the following table.
Table 7-36  Standby main server parameters — redundancy

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-to-peer</td>
<td>The standby main server IP address that the primary main server must use for general communication</td>
</tr>
<tr>
<td></td>
<td>Default: IP address of primary network interface</td>
</tr>
<tr>
<td>rsync-ip</td>
<td>The standby main server IP address that the primary main server must use for data synchronization</td>
</tr>
<tr>
<td></td>
<td>Default: IP address of primary network interface</td>
</tr>
</tbody>
</table>

Configure the **database** redundancy parameters in the following table, and then enter `back`

Table 7-37  Standby main server parameters — redundancy, database

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>The IP address that the standby main server must use to reach the primary database</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>instance</td>
<td>Primary database instance name</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>backup-sync</td>
<td>Whether database backup file synchronization is enabled</td>
</tr>
<tr>
<td></td>
<td>When the parameter is enabled, each database backup file set is copied to the peer main database station after the backup completes.</td>
</tr>
<tr>
<td></td>
<td>You must ensure that there is sufficient network bandwidth between the main database stations before you enable this parameter. See the NSP NFM-P Planning Guide for information about the bandwidth requirements of database backup file synchronization.</td>
</tr>
<tr>
<td></td>
<td>You must set the parameter to the same value on each main server.</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
</tbody>
</table>
### Table 7-37  Standby main server parameters — redundancy, database  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alignment</td>
<td>Whether automatic database alignment is enabled</td>
</tr>
<tr>
<td></td>
<td>If automatic database alignment is enabled, a main server</td>
</tr>
<tr>
<td></td>
<td>and database attempt to assume a common role, primary</td>
</tr>
<tr>
<td></td>
<td>or standby, after an event such as a server activity switch</td>
</tr>
<tr>
<td></td>
<td>or database failover. In a geographically dispersed system,</td>
</tr>
<tr>
<td></td>
<td>the function helps to ensure that a main server</td>
</tr>
<tr>
<td></td>
<td>communicates with the local database in order to reduce</td>
</tr>
<tr>
<td></td>
<td>the network latency between the components.</td>
</tr>
<tr>
<td></td>
<td>For more information about database alignment, see the</td>
</tr>
<tr>
<td></td>
<td><a href="#">NSP NFM-P System Administrator Guide</a></td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td>prefer-instance</td>
<td>The name of the database instance with which the standby</td>
</tr>
<tr>
<td></td>
<td>main server is to align</td>
</tr>
<tr>
<td></td>
<td>The parameter is configurable when the alignment parameter</td>
</tr>
<tr>
<td></td>
<td>is enabled.</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>reinstatiation-delay</td>
<td>The delay, in minutes, between the completion of a database failover</td>
</tr>
<tr>
<td></td>
<td>and the automatic reinstatiation of the standby database</td>
</tr>
<tr>
<td></td>
<td>A value of 0 disables automatic database reinstatiation.</td>
</tr>
<tr>
<td></td>
<td>Default: 60</td>
</tr>
</tbody>
</table>

Configure the peer-server redundancy parameters in the following table, and then enter back "\".

### Table 7-38  Standby main server parameters — redundancy, peer-server

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>The primary main server IP address that the standby main server</td>
</tr>
<tr>
<td></td>
<td>must use for general communication</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>hostname</td>
<td>The primary main server hostname that the standby main server</td>
</tr>
<tr>
<td></td>
<td>must use for general communication</td>
</tr>
<tr>
<td></td>
<td>The parameter is configurable and mandatory when the hostname parameter in Step 109 is configured.</td>
</tr>
<tr>
<td></td>
<td>If the TLS certificate contains the FQDN, you must specify the FQDN as the parameter value.</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>rsync-ip</td>
<td>The primary main server IP address that the standby main server must use for data synchronization. Default: —</td>
</tr>
<tr>
<td>public-ip</td>
<td>The IP address that the GUI clients, XML API clients, and auxiliary servers must use to reach the primary main server. Default: —</td>
</tr>
<tr>
<td>jndi-port</td>
<td>The TCP port on the primary main server station used for EJB JNDI messaging to GUI clients. It is recommended that you accept the default unless another application uses the port, or there is a firewall between the GUI clients and the primary main server. Default: 1099</td>
</tr>
<tr>
<td>ip-to-auxes</td>
<td>The primary main server IP address that the auxiliary servers must use to reach the primary main server. You must configure the parameter if the NFM-P system includes one or more auxiliary servers. Default: —</td>
</tr>
<tr>
<td>snmp-ipv4</td>
<td>The IPv4 address that the managed NEs must use to reach the primary main server</td>
</tr>
<tr>
<td>snmp-ipv6</td>
<td>The IPv6 address that the managed NEs must use to reach the primary main server</td>
</tr>
<tr>
<td>snmp-port</td>
<td>The TCP port on the primary main server station used for SNMP communication with the managed NEs. Default: 162</td>
</tr>
<tr>
<td>traplog-id</td>
<td>The SNMP trap log ID associated with the primary main server. Default: 98</td>
</tr>
</tbody>
</table>

Enter `back ↵`. The prompt changes to `<main configure>.

As required, configure the mediation parameters in the following table, and then enter `back ↵`.  

**Note:** Some device types do not support an SNMP port value other than 162. Before you configure the `snmp-port` parameter to a value other than the default, you must ensure that each device type in the managed network supports the port value.
Table 7-39  Standby main server parameters — mediation

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| nat       | Whether NAT is used between the main servers and the managed NEs  
            Default: false |
| snmp-ipv4 | The IPv4 address that the managed NEs must use to reach the standby main server  
            Default: IPv4 address of primary network interface |
| snmp-ipv6 | The IPv6 address that the managed NEs must use to reach the standby main server  
            Default: IPv6 address of primary network interface |
| snmp-port | The TCP port on the standby main server station that the managed NEs must use to reach the standby main server  
            Default: 162 |
| traplog-id| The SNMP trap log ID associated with the standby main server  
            Default: 98 |

If you are not using the PKI server to configure TLS, the standby main server requires a copy of the NFM-P TLS keystore and truststore files that are used by the primary main server. Ensure that the required TLS keystore and truststore files are in a temporary location on the standby main server station.

Caution: The files must not be in the /opt/nsp/os/tls directory on the standby main server station, or the TLS configuration fails.

Note: The nsp user must be the owner of the directory path to the location.

If required, configure the tls parameters in the following table, and then enter back ↓.

Table 7-40  Standby main server parameters — tls

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| keystore-file| The absolute path of the TLS keystore file  
              To enable automated TLS deployment, enter no keystore-file.  
              Default: — |
| keystore-pass| The TLS keystore password  
              Default: available from technical support |
### Table 7-40  Standby main server parameters — tls (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| truststore-file | The absolute path of the TLS truststore file  
To enable automated TLS deployment, enter `no truststore-file`.  
Default: — |
| truststore-pass | The TLS truststore password  
Default: available from technical support |
| alias | The alias specified during keystore generation  
You must configure the parameter.  
Default: — |
| pki-server | If you are using the automated TLS deployment method, the IP address or hostname of the PKI server  
Default: — |
| pki-server-port | If you are using the automated TLS deployment method, the TCP port on which the PKI server listens for and services requests  
Default: 2391 |
| webdav | Whether WebDAV access to eNodeB activation data is enabled  
Default: false |

As required, configure the **oss** parameters in the following table, and then enter **back**.

<i>Note:** The parameters are configurable only if no auxiliary servers are specified in **Step 111**. Otherwise, OSS access is restricted to the auxiliary servers, which require the configuration of OSS access parameters during installation.

### Table 7-41  Standby main server parameters — oss

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| secure      | Whether communication between the main servers and the XML API clients is secured using TLS  
Default: secure |
| public-ip   | The IP address that the XML API clients must use to reach the standby main server  
Default: IP address of primary network interface |
| corba-3gpp  | Whether the NFM-P 3GPP interface is enabled  
Default: false |
Table 7-41  Standby main server parameters — oss  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>xml-output</td>
<td>The directory in which to store the output of XML API file export operations</td>
</tr>
<tr>
<td></td>
<td>Default: /opt/nsp/nfmp/server/xml_output</td>
</tr>
</tbody>
</table>

If the NFM-P includes an auxiliary database, configure the `auxdb` parameters in the following table, and then enter `back ↵`.

Table 7-42  Standby main server parameters — auxdb

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enabled</td>
<td>Whether the auxiliary database is enabled in the main server configuration</td>
</tr>
<tr>
<td>ip-list</td>
<td>A comma-separated list of the auxiliary database station IP addresses that are accessible to the main server</td>
</tr>
<tr>
<td>oam-test-results</td>
<td>Whether the auxiliary database is to store OAM test results</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>redundancy-level</td>
<td>Boolean value that specifies whether the auxiliary database is to replicate data among multiple stations</td>
</tr>
<tr>
<td></td>
<td>If the auxiliary database is deployed on a single station, you must set the parameter to 0.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution:</strong> After you configure an <code>auxdb</code> parameter and start the main server, you cannot modify the <code>redundancy-level</code> parameter.</td>
</tr>
<tr>
<td></td>
<td>Default: 1</td>
</tr>
</tbody>
</table>

As required, configure the `aa-stats` parameters in the following table, and then enter `back ↵`.

Table 7-43  Standby main server parameters — aa-stats

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enabled</td>
<td>Whether the NFM-P is to collect AA accounting statistics</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
</tbody>
</table>
Table 7-43  Standby main server parameters — aa-stats (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>formats</td>
<td>AA accounting statistics file formats; the options are the following:  &lt;br&gt;• ipdr — IPDR format  &lt;br&gt;• ram — 5670 RAM format  &lt;br&gt;• ipdr,ram — IPDR and 5670 RAM formats  &lt;br&gt;The parameter is configurable when the enabled parameter is set to true.  &lt;br&gt;Default: ram</td>
</tr>
<tr>
<td>aux-db storage</td>
<td>Whether the NFM-P is to store the statistics in an auxiliary database  &lt;br&gt;The parameter is configurable when the enabled parameter is set to true.  &lt;br&gt;Default: false</td>
</tr>
</tbody>
</table>

Perform one of the following to specify the registry servers for NSP inter-module communication:

a. If the NSP system includes the NSD and NRC, specify the IP address of each NSD and NRC server; enter the following:

```<main configure> registry ip-list address1;address2 back```

where `address1` and `address2` are the public IP addresses of the NSD and NRC servers

**Note:** If the NSD and NRC system is standalone, only `address1` is required.

b. If the NSP system includes only the NFM-P, enter the following:

```<main configure> registry ip-list address1;address2 back```

where `address1` and `address2` are the IP addresses that the NFM-P main servers use to communicate with each other

Verify the main server configuration.

1. Enter the following:

```<main configure> show-detail```

The main server configuration is displayed.

2. Review each parameter to ensure that the value is correct.

3. Configure one or more parameters, if required.

4. When you are certain that the configuration is correct, enter the following:

```<main configure> back```

The prompt changes to `<main>`. 

---

123

124
Enter the following:
<main> apply</main>
The configuration is applied.

Enter the following:
<main> exit</main>
The samconfig utility closes.

Start standby main server

Start the standby main server.

**Note:** If you did not specify a license file during the installation, you cannot start the main server until you import a license. See “Software and license configuration procedures” in the *NSP NFM-P System Administrator Guide* for information about importing a license.

1. Log in as the nsp user on the main server station.
2. Open a console window.
3. Enter the following:
   bash$ cd /opt/nsp/nfmp/server/nms/bin
4. Enter the following:
   bash$ ./nmsserver.bash start
5. Enter the following:
   bash$ ./nmsserver.bash appserver_status
   The server status is displayed; the server is fully initialized if the status is the following:
   Application Server process is running. See nms_status for more detail.
   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

If the NFM-P is to manage wireless NEs, enter the following to update the memory configuration accordingly for GUI clients:

bash$ ./nmsdeploytool.bash clientmem -l

Close the console window.
Install optional components

130 Install and enable one or more auxiliary servers, if required; see “Auxiliary server installation” (p. 201).

131 Install and enable an auxiliary database, if required; see “Auxiliary database installation” (p. 223).

132 Install and enable one or more NSP Flow Collectors, if required; see “NSP Flow Collector installation” (p. 215).

133 Install and enable one or more NSP analytics servers, if required; see the NSP documentation for information.

Stop PKI server

134 If you are deploying TLS using an NSP PKI server, stop the PKI server, as described at the end of 6.7 “To configure and enable an NSP PKI server” (p. 91).

Install additional GUI clients

135 Perform the appropriate procedures in the following chapters to install additional single-user GUI clients and client delegate servers, as required:
- Chapter 14, “Single-user client deployment” —single-user client
- Chapter 15, “Client delegate server deployment” —client delegate server

Configure and enable firewalls

136 If you intend to use any firewalls between the NFM-P components, and the firewalls are disabled, configure and enable each firewall.

Perform one of the following.
- a. Configure each external firewall to allow the required traffic using the port assignments in the NSP NFM-P Planning Guide, and enable the firewall.
- b. Configure and enable Firewalld on each component station, as required.
1. Use an NFM-P template to create the Firewalld rules for the component, as described in the NSP NFM-P Planning Guide.
2. Log in to the station as the root user.
3. Open a console window.
4. Enter the following:
   # systemctl enable firewalld
5. Enter the following:
   # systemctl start firewalld
6. Close the console window.
Auxiliary server installation

7.7 Auxiliary server installation workflow

7.7.1 Description

CAUTION

Deployment Restriction

An NFM-P auxiliary server requires a dedicated station.

You cannot install the auxiliary server software on a station if another NFM-P component is installed on the station.

CAUTION

Service Disruption

If the NFM-P system uses a firewall, you must ensure that the firewall allows the required traffic to pass between the auxiliary server and other NFM-P components before you attempt to install the auxiliary server.

See the NSP NFM-P Planning Guide for port assignment and firewall configuration information.

This section describes how to install and enable an auxiliary server in a standalone or redundant NFM-P system.

7.7.2 Stages

The following is the sequence of high-level actions required to install and enable an auxiliary server in an NFM-P system.

1. Perform 7.8 “To install an NFM-P auxiliary server” (p. 202) on the auxiliary server station.

2. Perform 7.9 “To add auxiliary servers to an NFM-P system” (p. 208) to configure the auxiliary server communication with each main server.

3. An auxiliary server can use multiple interfaces for network management. The default network-management interface address is the public IP address of the interface that is used for main server communication. If you need to configure a different or additional network-management interface, see “To configure an additional management interface on an auxiliary server” in the NSP NFM-P User Guide.
7.8 To install an NFM-P auxiliary server

7.8.1 Purpose

The following steps describe how to install the NFM-P auxiliary server software on a station. Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

Note: An auxiliary server is dedicated to only one of the following functions:
- statistics collection
- call-trace data collection
- PCMD record collection

Note: You require root user privileges on the auxiliary server station.

Note: Performing the procedure creates the nsp user account on the auxiliary server station.

Note: The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:
- # — root user
- bash$ — nsp user

7.8.2 Steps

1. Log in as the root user on the auxiliary server station.

2. Download the following installation files to an empty local directory:
   - nsp-nfmp-jre-R.r.p-rel.v.rpm
   - nsp-nfmp-config-R.r.p-rel.v.rpm
   - nsp-nfmp-aux-server-R.r.p-rel.v.rpm
   
   where
   
   R.r.p is the NSP release identifier, in the form MAJOR.minor.patch
   
   v is a version identifier

   Note: In subsequent steps, the directory is called the NFM-P software directory.

3. Navigate to the NFM-P software directory.

   Note: Ensure that the directory contains only the installation files.
4. Enter the following:
   
   ```
   # chmod +x *
   ```

5. Enter the following:
   
   ```
   # yum install *.rpm
   ```
   The yum utility resolves any package dependencies, and displays the following prompt:

   - Total size: nn G
   - Installed size: nn G
   - Is this ok [y/N]:

6. Enter y. The following and the installation status are displayed as each package is installed:
   - Downloading packages:
   - Running transaction check
   - Running transaction test
   - Transaction test succeeded
   - Running transaction
   - The package installation is complete when the following is displayed:
     - Complete!

7. The initial NFM-P server installation on a station creates the nsp user account and assigns a randomly generated password.

   If this is the first installation of a main server, auxiliary server, NSP analytics server, or NSP Flow Collector on the station, change the nsp password.

   **Note:** The nsp password must not contain the @ symbol, or eNodeB device management may be compromised.

   1. Enter the following:
      
      ```
      # passwd nsp
      ```
      The following prompt is displayed:
      - New Password:

   2. Enter a password.
      The following prompt is displayed:
      - Confirm Password:

   3. Re-enter the password.

   4. Record the password and store it in a secure location.
Enter the following:
```bash
# samconfig -m aux
```
The following is displayed:
```
Start processing command line inputs...
<aux>
```

Enter the following:
```
<aux> configure
```
The prompt changes to <aux configure>.

Enter the following:
```
<aux configure> show-detail
```
The auxiliary server configuration is displayed.

If the default ip value is not the correct IP address of the auxiliary server, configure the ip parameter.

If the auxiliary server is to perform call-trace data collection, perform the following steps.
1. Enter the following:
   ```
   <aux configure> service type calltrace
   ```
The prompt changes to <aux configure service>.
2. Enter the following:
   ```
   <aux configure service> calltrace
   ```
The prompt changes to <aux configure service calltrace>.
3. Configure the parameters in the following table.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| ipv4      | The IPv4 address that the managed NEs must use to reach the auxiliary server  
Default: —  |
| ipv6      | The IPv6 address that the managed NEs must use to reach the auxiliary server  
Default: —  |
If the auxiliary server is to perform PCMD record collection, perform the following steps.

1. Enter the following:
   
   `<aux configure> service type pcmd
   
   The prompt changes to `<aux configure service>`.

2. Enter the following:
   
   `<aux configure service> pcmd
   
   The prompt changes to `<aux configure service pcmd>`.

3. Configure the parameters in the following table.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| ipv4      | The IPv4 address that the managed NEs must use to reach the auxiliary server  
             Default: — |
| ipv6      | The IPv6 address that the managed NEs must use to reach the auxiliary server  
             Default: — |
| nat       | Whether NAT is used between the managed NEs and the auxiliary server  
             Default: false |
| public-ip | The public IP address that the managed NEs must use to reach the auxiliary server when NAT is enabled  
             The parameter is configurable when the nat parameter is set to true.  
             Default: — |
| dir       | The absolute file path of the local directory in which to store the collected PCMD CSV files  
             Default: /opt/nsp/nfmp/pcmd_output |

4. Enter `back` ↓.

   The prompt changes to `<aux configure service>`. 
5. Enter `back ↓`.
   The prompt changes to `<aux configure>.

14
Configure the `main-server` parameters in the following table, and then enter `back ↓`.

Table 7-44  Auxiliary server parameters — main-server

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| domain | The NFM-P system identifier  
         | Default: NFM-P |
| ip-one | The primary main server IP address that the auxiliary server must use to reach the standalone main server, or the primary main server in a redundant system  
         | Default: — |
| ip-two | The standby main server IP address that the auxiliary server must use to reach the standby main server in a redundant system  
        | Default: — |

15
Configure the `data-sync` parameters in the following table, and then enter `back ↓`.

Table 7-45  Auxiliary server parameters — data-sync

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| local-ip | The IP address of the interface on this station that the other auxiliary server in an auxiliary server pair must use to reach this auxiliary server  
          | Default: IP address of primary network interface |
| peer-ip | The IP address of the interface on the other auxiliary server station in an auxiliary server pair that this auxiliary server must use to reach the other auxiliary server  
          | Default: — |

16
Configure the `tls` parameters in the following table, and then enter `back ↓`.

Table 7-46  Auxiliary server parameters — tls

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keystore-file</td>
<td>The absolute path of the TLS keystore file</td>
</tr>
<tr>
<td></td>
<td>To enable automated TLS deployment, enter no keystore-file.</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>keystore-pass</td>
<td>The TLS keystore password</td>
</tr>
<tr>
<td></td>
<td>Default: available from technical support</td>
</tr>
<tr>
<td>pki-server</td>
<td>If you are using the automated TLS deployment method, the IP address or hostname of the PKI server</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>pki-server-port</td>
<td>If you are using the automated TLS deployment method, the TCP port on which the PKI server listens for and services requests</td>
</tr>
<tr>
<td></td>
<td>Default: 2391</td>
</tr>
</tbody>
</table>

As required, configure the oss parameters in the following table, and then enter back ↓.

Table 7-47  Auxiliary server parameters — oss

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>public-ip</td>
<td>The IP address that the XML API clients must use to reach the auxiliary server</td>
</tr>
<tr>
<td></td>
<td>Default: IP address of primary network interface</td>
</tr>
<tr>
<td>xml-output</td>
<td>The directory that is to contain the output of XML API file export operations</td>
</tr>
<tr>
<td></td>
<td>Default: /opt/nsp/nfmp/server/xml_output</td>
</tr>
</tbody>
</table>

Verify the auxiliary server configuration.
1. Enter the following:
   `<aux configure> show-detail ↓`
   
The auxiliary server configuration is displayed.
2. Review each parameter to ensure that the value is correct.
3. Configure one or more parameters, if required.
4. When you are certain that the configuration is correct, enter the following:
   `<aux configure> back ↓`
   
The prompt changes to `<aux>`. 
19 Enter the following:
   <aux> apply
   The configuration is applied.

20 Enter the following:
   <aux> exit
   The samconfig utility closes.

21 Start the auxiliary server.
   1. Enter the following to switch to the nsp user.
      
      # su - nsp
   2. Enter the following to start the auxiliary server application:
      
      bash$ /opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash auxstart
      The auxiliary server starts.

22 Close the open console windows.

END OF STEPS

7.9 To add auxiliary servers to an NFM-P system

7.9.1 Purpose

The following steps describe how to add one or more NFM-P auxiliary servers to an NFM-P system. Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

CAUTION

Service Disruption

This procedure requires that you restart each main server, which is service-affecting.

Perform this procedure only during a scheduled maintenance period.

Note: You require the following user privileges:
   • on each main and auxiliary server station — root, nsp
   • on each main database station that has IP validation enabled — Oracle management

7.9 To add auxiliary servers to an NFM-P system
7.9.2 Steps

1

Perform one of the following.

a. If you are deploying TLS using an NSP PKI server, perform 6.7 “To configure and enable an NSP PKI server” (p. 91).

b. If you are using the manual TLS deployment method, generate and distribute the required TLS files for the system, as described in 6.11 “Workflow for manual TLS deployment” (p. 105).

2

If the NFM-P is deployed in a standalone configuration, go to Step 6.

3

Perform Step 6 to Step 17 on the standby main server, which is called Server B.

4

Perform Step 6 to Step 17 on the primary main server, which is called Server A.

Note: After you stop the primary main server in Step 1, a server activity switch occurs and Server B begins to manage the network. If required, you can revert to the previous primary and standby roles of Server A and Server B by performing the activity switch described in Step 18.

5

Go to Step 19.

6

Log in to the main server station as the root user.

7

Open a console window.

8

Stop the main server.

1. Enter the following to switch to the nsnp user:
   
   ```
   # su - nsnp
   ```

2. Enter the following:
   
   ```
   bash$ cd /opt/nsnp/nfmp/server/nms/bin
   ```

3. Enter the following:
   
   ```
   bash$ ./nmsserver.bash stop
   ```
bash$ ./nmsserver.bash appserver_status
down
The server status is displayed; the server is fully stopped if the status is the following:
  Application Server is stopped
If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform
the next step until the server is fully stopped.

9
Enter the following to switch back to the root user:
bash$ exit

10
Enter the following:
  # samconfig -m main
down
The following is displayed:
  Start processing command line inputs...
  <main>

11
Enter the following:
  <main> configure aux
down
The prompt changes to <main configure aux>.

12
Configure the parameters in the following table, and then enter back.

Note: At least one auxiliary server that you specify must be a Preferred auxiliary server.

Table 7-48  Main server aux parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| stats     | If enabled, specifies that one or more auxiliary servers are to be used for statistics collection  
            Default: false |
| calltrace | If enabled, specifies that one or more auxiliary servers are to be used for call-trace data collection  
            Default: false |
| pcmd      | If enabled, specifies that one or more auxiliary servers are to be used for PCMD record collection  
            Default: false |
### Table 7-48  Main server aux parameters  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| ip-to-auxes     | The main server IP address that the auxiliary servers must use to reach the main server  
|                 | Default: —                                                                  |
| preferred-list  | Comma-separated list of Preferred auxiliary server IP addresses             
|                 | Default: —                                                                  |
| reserved-list   | Comma-separated list of Reserved auxiliary server IP addresses              
|                 | Default: —                                                                  |
| peer-list       | Comma-separated list of Remote auxiliary server IP addresses                
|                 | Default: —                                                                  |
| calltrace-pairs | List of Preferred and Reserved call-trace auxiliary server pairs, in the following format; configurable when the calltrace parameter is enabled:  
|                 | Preferred_address1,Reserved_address1|Preferred_address2,  
|                 | Reserved_address2...Preferred_addressN,Reserved_addressN                   
|                 | If a pair includes no Reserved auxiliary server, specify the pair as shown below without the comma separator:  
|                 | Preferred_address|  
|                 | Default: —                                                                  |
| pcmd-pairs      | List of Preferred and Reserved PCMD auxiliary server pairs, in the following format; configurable when the pcmd parameter is enabled:  
|                 | Preferred_address1,Reserved_address1|Preferred_address2,  
|                 | Reserved_address2...Preferred_addressN,Reserved_addressN                   
|                 | If a pair includes no Reserved auxiliary server, specify the pair as shown below without the comma separator:  
|                 | Preferred_address|  
|                 | Default: —                                                                  |

13

Enter the following:

```
exit
```

The prompt changes to `<main>.

14

Verify the configuration; enter the following:

```
<main> show-detail
```

The main server configuration is displayed.
If the configuration is correct, enter the following:

```
<main> apply
```

The configuration is applied.

Enter the following:

```
<main> exit
```

The sameconfig utility closes.

Start the main server.

1. Enter the following to switch to the nsp user:
   
   ```
   # su - nsp
   ```

2. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin
   ```

3. Enter the following:

   ```
   bash$ ./nmsserver.bash start
   ```

4. Enter the following:

   ```
   bash$ ./nmsserver.bash appserver_status
   ```

   The server status is displayed; the server is fully initialized if the status is the following:

   Application Server process is running. See nms_status for more detail.

   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

To revert to the previous primary and standby main server roles in a redundant deployment, perform the following steps.

1. Log in to Server B as the nsp user.

2. Open a console window.

3. Enter the following to initiate a server activity switch:

   ```
   bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash force_restart
   ```

   The server activity switch begins; Server B restarts as the standby main server, and Server A begins to manage the network as the primary main server.

4. Log in to Server A as the nsp user.

5. Open a console window.

6. Enter the following:
bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash appserver_status

The command returns server status information.
If the main server is not completely started, the first line of status information is the following:
Main Server is not ready...
The main server is completely started when the command returns the following line of output:
-- Primary Server is UP

7. If the command output indicates that the server is not completely started, wait five minutes and then return to Step 18 6.
Do not proceed to the next step until the server is completely started.

If IP validation is enabled for database access, perform the following steps on each main database station to enable validation of each auxiliary server.

Note: In a redundant NFM-P system, you must perform the steps on the primary main database station first, and then on the standby main database station.
1. Log in to the main database station as the Oracle management user.
2. Open a console window.
3. Enter the following:
   bash$ cd /opt/nsp/nfmp/oracle12r1/network/admin
4. Create a backup copy of the sqlnet.ora file.
5. Open the sqlnet.ora file with a plain-text editor, for example, vi.
6. Locate the section that begins with the following:
   # IP Validation
7. Edit the following lines to read:
   • TCP.VALIDNODE_CHECKING = yes
   • TCP.INVITED_NODES = (aux_server_1,aux_server_2...aux_server_n...) where aux_server_1,aux_server_2...aux_server_n is a comma-separated list of the auxiliary server IP addresses
8. Save and close the sqlnet.ora file.
9. Enter the following to stop the Oracle database listener:
   bash$ /opt/nsp/nfmp/oracle12r1/bin/lsnrctl stop
10. Enter the following to start the Oracle database listener:
    bash$ /opt/nsp/nfmp/oracle12r1/bin/lsnrctl start
Close the open console windows.
NSP Flow Collector installation

7.10 NSP Flow Collector installation workflow

7.10.1 Description

**CAUTION**

**Deployment Restriction**

An NSP Flow Collector requires a dedicated station.

You cannot install the NSP Flow Collector software on a station if another NFM-P component is installed on the station.

**CAUTION**

**Service Disruption**

If the NFM-P system uses a firewall, you must ensure that the firewall allows the required traffic to pass between the NSP Flow Collector and other NFM-P components before you attempt to install the NSP Flow Collector.

See the NSP NFM-P Planning Guide for port assignment and firewall configuration information.

This section describes how to install and enable an NSP Flow Collector in a standalone or redundant NFM-P system.

See the NSP NFM-P Statistics Management Guide for information about configuring NSP Flow Collector statistics collection after the installation.

7.10.2 Stages

The following is the sequence of high-level actions required to install and enable an NSP Flow Collector in an NFM-P system.

1. Perform 7.11 “To install an NSP Flow Collector” (p. 216) on each NSP Flow Collector station.

2. Perform 6.15 “To manually configure TLS on an NSP Flow Collector” (p. 117) on each NSP Flow Collector station.

3. Perform 7.12 “To configure NSP Flow Collector communication” (p. 219) to configure the NSP Flow Collector communication with the main servers and IPDR target file servers.
7.11 To install an NSP Flow Collector

7.11.1 Purpose

The following steps describe how to install the NSP Flow Collector software on a station.

Note: You require root user privileges on the NSP Flow Collector station.

Note: A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

7.11.2 Steps

1. Log in as the root user on the NSP Flow Collector station.

2. Download the following installation files to an empty local directory:
   - nsp-nfmp-jre-R.r.p-rel.v.rpm
   - nsp-nfmp-config-R.r.p-rel.v.rpm
   - nsp-flow-collector-R.r.p-rel.v.rpm
   where
   R.r.p is the NSP release identifier, in the form MAJOR.minor.patch
   v is a version identifier

3. Open a console window.

4. Navigate to the directory that contains the NFM-P installation files.

   Note: Ensure that the directory contains only the installation files.

5. Enter the following:
   # chmod +x *

6. Enter the following:
   # yum install *.rpm
   The yum utility resolves any package dependencies, and displays the following prompt:
   Total size: nnn M
Installed size: nn M
Is this ok [y/d/N]:

7

Enter y. The following and the installation status are displayed as each package is installed:
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
The package installation is complete when the following is displayed:
Complete!

8

When the package installation is complete, enter the following:
# samconfig -m flow
The following is displayed:
Start processing command line inputs...
<flow>

9

Enter the following:
<flow> configure category category
where category is the NSP Flow Collector data category, which is one of the following:
• sys—system Cflowd statistics
• aa—AA Cflowd statistics
The prompt changes to <flow configure>.

10

Enter the following:
<flow configure> policy policy back
where policy is one of the NSP Flow Collector policy types listed in Table 7-49, “NSP Flow Collector policy types” (p. 218)

Note: You can view and configure the set of selected counters in the NSP Flow Collector web UI when the installation is complete.
Table 7-49  NSP Flow Collector policy types

<table>
<thead>
<tr>
<th>Policy type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aa-default</td>
<td>Only a default set of AA Cflowd counters is selected for collection.</td>
</tr>
<tr>
<td>aa-all</td>
<td>All AA Cflowd counters are selected for collection.</td>
</tr>
<tr>
<td>aa-edr</td>
<td>Only PGW-EDR AA Cflowd stats counters are selected for collection; the EDR record format is supported for 7750 MG AA Cflowd records.</td>
</tr>
<tr>
<td>sys-default</td>
<td>Only a default set of system Cflowd counters is selected for collection.</td>
</tr>
<tr>
<td>sys-all</td>
<td>All system Cflowd counters are selected for collection.</td>
</tr>
</tbody>
</table>

11

Configure the tls parameters in the following table, and then enter back ↓.

Table 7-50  NSP Flow Collector parameters — tls

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keystore-file</td>
<td>The absolute path of the TLS keystore file</td>
</tr>
<tr>
<td></td>
<td>To enable automated TLS deployment, enter no keystore-file.</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>keystore-pass</td>
<td>The TLS keystore password</td>
</tr>
<tr>
<td></td>
<td>Default: available from technical support</td>
</tr>
<tr>
<td>pki-server</td>
<td>If you are using the automated TLS deployment method, the IP address or</td>
</tr>
<tr>
<td></td>
<td>hostname of the PKI server</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>pki-server-port</td>
<td>If you are using the automated TLS deployment method, the TCP</td>
</tr>
<tr>
<td></td>
<td>port on which the PKI server listens for and services requests</td>
</tr>
<tr>
<td></td>
<td>Default: 2391</td>
</tr>
</tbody>
</table>

12

Enter the following:
<flow configure> exit ↓

The prompt changes to <flow>.

13

Enter the following:
<flow> apply ↓

The configuration is applied.
14

Enter the following:

<flow> exit

The sameconfig utility closes.

15

Start the NSP Flow Collector; enter the following:

```
# /opt/nsf/flow/dcp/bin/dcpctl.sh start
```

The command displays a series of status messages as the NSP Flow Collector starts.

**Note:** To start the NSP Flow Collector without displaying status messages, you can use the following command:

```
# systemctl start nsf-flow-collector.service
```

16

Close the console window.

**END OF STEPS**

7.12 To configure NSP Flow Collector communication

7.12.1 Description

The following steps describe how to configure NSP Flow Collector communication with each NFM-P main server and target file server.

**Note:** You can perform the procedure only if TLS is configured on the NSP Flow Collector as described in 6.15 “To manually configure TLS on an NSP Flow Collector” (p. 117).

7.12.2 Steps

1

Use a browser to open the following URL:

https://server:8443/dcp-admin/admin

where server is the NSP Flow Collector IP address or hostname

2

If a login form opens, enter the required user credentials and click OK.

**Note:** The default user credentials are available from technical support.

The NSP Flow Collector page opens.
Click the Collector Configuration link. The Configuration page is displayed.

Configure the Collection Port parameter to specify the TCP port on the NSP Flow Collector station that is to receive the statistics data from NEs.

Click Save Configuration.

**Configure NFM-P parameters**

Click on the NFM-P Configuration tab.

Configure the parameters in the following table.

---

### Table 7-51 NSP Flow Collector parameters, NFM-P Configuration tab

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XML API</td>
<td></td>
</tr>
<tr>
<td>User Name</td>
<td>The NFM-P username for XML API file transfers</td>
</tr>
<tr>
<td>Password</td>
<td>The NFM-P user password for XML API file transfers</td>
</tr>
<tr>
<td>Use Secure HTTP (HTTPS)</td>
<td>Whether HTTPS is used for file transfers</td>
</tr>
<tr>
<td>Redundant</td>
<td>Whether the NFM-P system is a redundant deployment</td>
</tr>
<tr>
<td>Reconnect</td>
<td>Whether the NSP Flow Collector attempts to reconnect to the NFM-P after a connection failure</td>
</tr>
<tr>
<td>Durable</td>
<td>Whether the NFM-P JMS subscription is durable</td>
</tr>
<tr>
<td>Reconnect Attempts</td>
<td>The number of times to attempt to reconnect to the NFM-P after a connection failure</td>
</tr>
<tr>
<td>Reconnect Delay</td>
<td>The time, in seconds, to wait between NFM-P reconnection attempts</td>
</tr>
<tr>
<td>Connection Timeout</td>
<td>The time, in seconds, to wait for a response to an NFM-P connection attempt</td>
</tr>
<tr>
<td>Transfer Option</td>
<td>The method to use for file transfers from an NFM-P main server</td>
</tr>
</tbody>
</table>

---

**Note:** You must ensure that the user specified for the SFTP User Name or FTP User Name parameter has read and write access to each target file server directory named in the NFM-P IPDR File Transfer Policy. See the *NSP NFM-P System Administrator Guide* for IPDR File Transfer Policy configuration information.

**Note:** In a redundant NFM-P system, you must ensure that you set the Redundant parameter in the XML API panel to true.
Table 7-51  NSP Flow Collector parameters, NFM-P Configuration tab  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFM-P Primary</td>
<td></td>
</tr>
<tr>
<td>NFM-P Standby</td>
<td>(required for redundant system)</td>
</tr>
<tr>
<td>IP Address/Host name</td>
<td>The public IP address or hostname of the main server</td>
</tr>
<tr>
<td>HTTP Port</td>
<td>The TCP port on the main server for non-secure communication</td>
</tr>
<tr>
<td>HTTPS Port</td>
<td>The TCP port on the main server for secure communication</td>
</tr>
<tr>
<td>JNDI Port</td>
<td>The TCP port on the main server for JMS communication</td>
</tr>
<tr>
<td>SFTP Port</td>
<td>The TCP port on the main server for file transfers, if TLS is enabled</td>
</tr>
<tr>
<td>SFTP User Name</td>
<td>The username required for secure file transfers from the main server</td>
</tr>
<tr>
<td>SFTP Password</td>
<td>The password required for secure file transfers from the main server</td>
</tr>
<tr>
<td>FTP Port</td>
<td>The TCP port on the main server for file transfers, if TLS is not enabled</td>
</tr>
<tr>
<td>FTP User Name</td>
<td>The username required for non-secure file transfers from the main server</td>
</tr>
<tr>
<td>FTP Password</td>
<td>The password required for non-secure file transfers from the main server</td>
</tr>
</tbody>
</table>

8

Click Save Configuration.

Configure IPDR file-transfer parameters

9

Click on the IPDR Transfer tab.

10

Configure the parameters in the following table.

Note: If you set the Transfer Protocol parameter to Secure (SFTP), you must set the Port parameter to 22.

Table 7-52  NSP Flow Collector parameters, IPDR Configuration tab

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Transfer</td>
<td>Specifies whether IPDR file transfers to the target file server are enabled</td>
</tr>
<tr>
<td>Transfer Protocol</td>
<td>Specifies the file-transfer protocol for IPDR transfers to the target file server</td>
</tr>
<tr>
<td>IP Address / Host name</td>
<td>The IP address or hostname of the target file server</td>
</tr>
<tr>
<td>Port</td>
<td>The TCP port that the target file server uses to receive IPDR file transfers</td>
</tr>
<tr>
<td>Location</td>
<td>A descriptive entry that uniquely identifies the location of the target file server</td>
</tr>
<tr>
<td>User</td>
<td>The username required for IPDR file transfers to the target file server</td>
</tr>
</tbody>
</table>
Table 7-52 NSP Flow Collector parameters, IPDR Configuration tab (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>The password required for IPDR file transfers to the target file server</td>
</tr>
</tbody>
</table>

11
Click Save Configuration.

Perform snapshot extraction

12
Click on the Operations tab. The Operations page is displayed.

13

CAUTION

Service Disruption

*The Force Snapshot Extraction option consumes NFM-P main server resources.*

*Ensure that you perform the step only during a period of low NFM-P system activity.*

Click Force Snapshot Extraction. The NSP Flow Collector extracts the managed network information from a main server specified on the NFM-P Configuration tab.

14
Close the browser.

End of steps
Auxiliary database installation

7.13 Auxiliary database installation workflow

7.13.1 Description

**CAUTION**

Deployment Requirement

An NFM-P auxiliary database requires one or more dedicated stations.

You cannot install the auxiliary database software on a station if another NFM-P component is installed on the station.

**CAUTION**

Service Disruption

If the NFM-P system uses a firewall, you must ensure that the firewall allows the required traffic to pass between the auxiliary database and other NFM-P components before you attempt to install the auxiliary database.

See the NSP NFM-P Planning Guide for port assignment and firewall configuration information.

This section describes how to do the following.

- Install and enable an auxiliary database in a new or existing NFM-P system; see 7.13.2 “Workflow for auxiliary database installation” (p. 223).
- Add a new station to an existing auxiliary database; see 7.17 “To add a station to an NFM-P auxiliary database” (p. 231).

**Note:** You must set CPU speed scaling, or CPUfreq, to “performance” in the BIOS of each auxiliary database station, or the auxiliary database installation fails. See the RHEL power management documentation for information about enabling the “performance” CPUfreq governor on a station. Setting CPUfreq to “performance” effectively disables CPU speed scaling, so may result in greater energy consumption by a station.

7.13.2 Workflow for auxiliary database installation

The following is the sequence of high-level actions required to install and enable an auxiliary database in an NFM-P system.

1. Perform 7.14 “To prepare a station for auxiliary database installation” (p. 224) on each auxiliary database station.

2. Perform 7.15 “To install the NFM-P auxiliary database software” (p. 226).
Perform 7.16 “To add an auxiliary database to an NFM-P system” (p. 228).

7.14 To prepare a station for auxiliary database installation

7.14.1 Purpose

The following steps describe how to configure a station in advance of NFM-P auxiliary database software installation.

Note: You require root user privileges on the auxiliary database station.

Note: A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

7.14.2 Steps

1. Log in as the root user on the auxiliary database station.

2. Add a hostname entry for the new station to the /etc/hosts file on the new station.

Note: The first entry for the station hostname in the /etc/hosts file must be the station IP address that is reachable by each main server.

Note: The hostname must be the fully qualified hostname, and not the short hostname.

Note: Hostnames are case-sensitive.

3. Download the following installation files to an empty local directory:
   - nsp-nfmp-jre-R.r.p-rel.v.rpm
   - vertica-V.w.x.y.rpm
   - nsp-nfmp-aux-db-R.r.p-rel.v.rpm
   - VerticaSw_PreInstall.sh

   where

   \textit{R}.r.p is the NSP release identifier, in the form \textit{MAJOR}.minor.patch

   V.w.x-y is a version number

   \textit{v} is a version identifier

4. Open a console window.
Navigate to the NFM-P software directory.

**Note:** Ensure that the directory contains only the installation files.

Enter the following:

```
# chmod +x *
```

Enter the following:

```
# ./VerticaSw_PreInstall.sh
```

The script displays configuration messages like the following:

```
INFO: About to set kernel parameters in /etc/sysctl.conf...
INFO: Completed setting kernel parameters in /etc/sysctl.conf...
INFO: About to change the current values of the kernel parameters
INFO: Completed changing the current values of the kernel parameters
INFO: About to set ulimit parameters in /etc/security/limits.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.conf...
Checking Vertica DBA group samauxdb...
Adding Vertica DBA group samauxdb...
Checking Vertica user samauxdb...
Adding Vertica user samauxdb...
Changing ownership of the directory /opt/nsp/nfmp/auxdb to samauxdb:samauxdb.
Adding samauxdb to sudoers file.
Changing ownership of /opt/nsp/nfmp/auxdb files.
INFO: About to add setting to /etc/rc.d/rc.local...
INFO: Completed adding setting to /etc/rc.d/rc.local...
```

If the script instructs you to perform a restart, perform the following steps.

1. Enter the following:
   
   ```
   # systemctl reboot
   ```
   
The station reboots.

2. When the reboot is complete, log in to the station as the root user.

3. Open a console window.
4. Navigate to the NFM-P software directory.

Enter the following:

```
# yum install *.rpm
```

The `yum` utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/N]:
```

Enter `y`. The following and the installation status are displayed as each package is installed:

- Downloading packages:
- Running transaction check
- Running transaction test
- Transaction test succeeded
- Running transaction

The package installation is complete when the following is displayed:

```
Complete!
```

When the package installation is complete, close the console window.

---

**7.15 To install the NFM-P auxiliary database software**

**7.15.1 Purpose**

The following steps describe how to install and initialize the NFM-P auxiliary database software.

**Note:** You require root user privileges on each auxiliary database station.

**Note:** A leading `#` character in a command line represents the root user prompt, and is not to be included in a typed command.

**7.15.2 Steps**

1. Log in to any auxiliary database station as the root user.
Open a console window.

Enter the following:
```
# cp /opt/nsp/nfmp/auxdb/install/config/install.config.default
/opt/nsp/nfmp/auxdb/install/config/install.config
```

Open the /opt/nsp/nfmp/auxdb/install/config/install.config file using a plain-text editor such as vi.

Edit the following lines in the file to read:
```
hosts=internal_IP1,internal_IP2...internal_IPn
export_hosts=internal_IP1[export_IP1],internal_IP2[export_IP2]...
internal_IPn[export_IPn]
```

where
- `internal_IP1, internal_IP2...internal_IPn` are the IP addresses that the stations use to communicate with each other
- `export_IP1, export_IP2...export_IPn` are the IP addresses that the stations use to communicate with the NFM-P servers

**Note:** If the `export_IP` entry for a station is omitted, the station uses the `internal_IP` address for communication with the NFM-P servers.

The following is an `export_hosts` configuration example:
```
export_hosts=10.1.1.10[198.51.100.10],10.1.1.11[198.51.100.11],10.1.1.12[198.51.100.12]
```

Save and close the install.config file.

Enter the following:
```
# /opt/nsp/nfmp/auxdb/install/bin/auxdbAdmin.sh install
```

The script sequentially prompts for the root user password of each auxiliary database station.

Enter the required password at each prompt. The script installs the software on the station.
When the script execution is complete, perform the following steps on each auxiliary database station.

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following:
   
   ```
   # systemctl start nfmp-auxdbproxy.service
   ```

4. Close the console window.

---

### 7.16 To add an auxiliary database to an NFM-P system

#### 7.16.1 Purpose

The following steps describe how to enable an auxiliary database in an NFM-P system and configure communication between the database and each main server.

**CAUTION**

**Service Disruption**

*This procedure requires a restart of each main server, which is service-affecting.*

*Perform this procedure only during a scheduled maintenance period.*

**Note:** You must perform the procedure on each main server. In a redundant system, you must perform the procedure on the standby main server first.

**Note:** The auxiliary database must be installed and running before you perform the procedure.

**Note:** After you perform the procedure:

- The existing AA statistics values are automatically transferred from the main database to the auxiliary database.
- The auxiliary database begins to store new data. However, no migration of current data, such as accounting or performance statistics, event timeline, or OAM results occurs, and the existing data are no longer retrievable.
- The initial collection for some data types does not include periodic values, as the previous values are not included in the data migration.

#### 7.16.2 Steps

1. Ensure that the auxiliary database is operational.
Note: After you add an auxiliary database to a main server configuration, you cannot start the main server unless the auxiliary database is reachable by the main server.

1. Log in to an auxiliary database station as the root user.
2. Open a console window.
3. Enter the following:
   ```bash
   # /opt/nsp/nfmp/auxdb/install/bin/auxdbAdmin.sh status
   ```
   The script displays the following:
   ```
   Database status
   Node | Host | State | Version | DB
   ------------+---------------+-------+---------+-------
   host_IP_1 | internal_IP_1 | STATE | version | db_name
   host_IP_2 | internal_IP_2 | STATE | version | db_name
   .
   .
   host_IP_n | internal_IP_n | STATE | version | db_name
   ```
   Output captured in log_file
4. View each STATE value; each must be UP. If this is not the case, contact technical support for assistance.

Log in to the main server station as the nsp user.

Open a console window.

Stop the main server.
1. Enter the following:
   ```bash
   bash$ cd /opt/nsp/nfmp/server/nms/bin
   ```
2. Enter the following:
   ```bash
   bash$ ./nmsserver.bash stop
   ```
3. Enter the following:
   ```bash
   bash$ ./nmsserver.bash appserver_status
   ```
   The server status is displayed; the server is fully stopped if the status is the following:
   Application Server is stopped
   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.
Enter the following to switch to the root user:

bash$ su -

Enter the following:

# samconfig -m main

The following is displayed:

Start processing command line inputs...

<main>

Enter the following:

<main> configure auxdb enabled ip-list address1,address2,addressN

where address1, address2...addressN are the IP addresses specified for NFM-P server communication in 7.15 “To install the NFM-P auxiliary database software” (p. 226).

The prompt changes to <main configure auxdb>.

Perform one of the following.

Caution: After you configure an auxdb parameter and start the main server, you cannot modify the redundancy-level parameter.

a. If the auxiliary database is distributed among multiple stations, enter the following:

<main configure auxdb> redundancy-level 1 exit

b. If the auxiliary database is deployed on one station, enter the following:

<main configure auxdb> redundancy-level 0 exit

Enter the following:

<main> apply

The configuration is applied.

Enter the following:

<main> exit

The samconfig utility closes.
Enter the following to start the main server:

```
bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash start
```

The main server creates the required database elements and begins the migration of statistics data, if any, from the main database to the auxiliary database.

In the event that a statistics migration fails on any auxiliary database station, the migration is retried up to 10 times. If after 10 retries the migration remains unsuccessful, the main server shuts down and displays the following message:

```
Failed to migrate Application Assurance statistics from main database to auxiliary database
```

If the migration fails, you must do the following:

1. Restore the main database.
2. Resolve the cause of the migration failure.
3. Start the main server.

Close the console window.

Regular database backups are typically not required for a multi-station auxiliary database, but are recommended in a single-station deployment.

If you are deploying a single-station auxiliary database, enable scheduled database backups to ensure minimal data loss in the event of a failure. See “To back up an auxiliary database” in the NSP NFM-P System Administrator Guide for information.

**7.17 To add a station to an NFM-P auxiliary database**

**7.17.1 Purpose**

The following steps describe how to add a new station to an auxiliary database, for example, to accommodate network growth.
CAUTION

Service Disruption

This procedure requires a restart of each main server, which is service-affecting.
Perform this procedure only during a scheduled maintenance period.

Note: You cannot add a station to a one-station auxiliary database.

7.17.2 Steps

1. Add a hostname entry for the new station to the /etc/hosts file on each existing auxiliary database station.
   
   Note: The hostname must be the fully qualified hostname, and not the short hostname.
   
   Note: Hostnames are case-sensitive.

2. Log in as the root user on the new auxiliary database station.

3. Add a hostname entry for the new station to the /etc/hosts file on the new station.
   
   Note: The first entry for the station hostname in the /etc/hosts file must be the station IP address that is reachable by each main server.
   
   Note: The hostname must be the fully qualified hostname, and not the short hostname.
   
   Note: Hostnames are case-sensitive.

4. Download the following installation files to an empty local directory:
   
   Note: The software release must match the software release of the existing auxiliary database.
   
   - nsp-nfmp-jre-R.r.p-rel.v.rpm
   - vertica-V.w.x-y.rpm
   - nsp-nfmp-aux-db-R.r.p-rel.v.rpm
   - VerticaSw_PreInstall.sh

   where

   *R.*p is the NSP release identifier, in the form MAJOR.minor.patch

   *V.w.x-y* is a version number
Note: In subsequent steps, the directory is called the NFM-P software directory.

5

Open a console window.

6

Navigate to the NFM-P software directory.

Note: Ensure that the directory contains only the installation files.

7

Enter the following:

```bash
# chmod +x *
```

8

Enter the following:

```bash
# ./VerticaSw_PreInstall.sh
```

The script displays output similar to the following:

INFO: About to set kernel parameters in /etc/sysctl.conf...
INFO: Completed setting kernel parameters in /etc/sysctl.conf...
INFO: About to change the current values of the kernel parameters...
INFO: Completed changing the current values of the kernel parameters...
INFO: About to set ulimit parameters in /etc/security/limits.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.conf...
Checking Vertica DBA group samauxdb...
Adding Vertica DBA group samauxdb...
Checking Vertica user samauxdb...
Adding Vertica user samauxdb...
Changing ownership of the directory /opt/nsp/nfmp/auxdb to samauxdb:samauxdb.
Adding samauxdb to sudoers file.
Changing ownership of /opt/nsp/nfmp/auxdb files.
INFO: About to add setting to /etc/rc.d/rc.local...
INFO: Completed adding setting to /etc/rc.d/rc.local...
If the script instructs you to perform a restart, perform the following steps.

1. Enter the following:
   
   ```
   # systemctl reboot
   ```
   
   The station restarts.

2. Log in to the station as the root user.

3. Open a console window.

4. Navigate to the NFM-P software directory.

Enter the following:

```
# yum install *.rpm
```

The `yum` utility resolves any package dependencies, and displays the following prompt:

- Total size: nn G
- Installed size: nn G
- Is this ok [y/N]:

Enter y. The following and the installation status are displayed as each package is installed:

- Downloading packages:
- Running transaction check
- Running transaction test
- Transaction test succeeded
- Running transaction

The package installation is complete when the following is displayed:

- Complete!

When the package installation is complete, log in to an existing auxiliary database station as the root user.

Open a console window.

Enter the following:

```
# /opt/nsp/nfmp/auxdb/install/bin/auxdbAdmin.sh addNode internal_IP external_IP
```

where
**internal_IP** is the IP address from which the station communicates with the other auxiliary database stations

**external_IP** is the IP address from which the station communicates with the NFM-P servers

The script displays the following:

```
Adding hosts(s) hostname to auxiliary database cluster ...
```

15. When you are prompted for the database user password, enter the password.

16. When you are prompted for the root password of the new station, enter the password.

17. **CAUTION**

   **Installation Failure**

   *If the addition of the station to the auxiliary database is interrupted, the installation fails and support intervention may be required.*

   *You must answer yes to the prompt described in this step.*

   If the auxiliary database contains a large amount of data, the addition of the station may take considerable time. In such a scenario, the following prompt is displayed:

   

   Do you want to continue waiting? (yes/no) [yes]

   Press ↵ to accept the default of yes.

   **Note:** The prompt may be displayed several times during the operation.

18. When the script execution is complete, open the /opt/nsp/nfmp/auxdb/config/install.config file using a plain-text editor such as vi.

19. Edit the following line in the file to read:

   `hosts=internal_IP1,internal_IP2,...internal_IPn,new_internal_IP`

   where

   `internal_IP1, internal_IP2,...internal_IPn` are the IP addresses of the existing auxiliary database stations

   `new_internal_IP` is the IP address from which the new station communicates with the other auxiliary database stations

20. Edit the following line in the file to read:
export_hosts=internal_IP1[export_IP1],internal_IP2[export_IP2]...internal_IPn[export_IPn],new_internal_IP[new_export_IP]

where

internal_IP1[export_IP1],internal_IP2[export_IP2],internal_IPn[export_IPn] are the IP addresses of the existing auxiliary database stations

new_internal_IP is the IP address from which the new station communicates with the other auxiliary database stations

new_export_IP is the IP address from which the new station communicates with the NFM-P servers

21

Save and close the install.config file.

22

Start the auxiliary database software on the station.

1. Enter the following:
   
   `# systemctl start nfmp-auxdbproxy.service`

2. Close the console window.

23

Enter the following:

`# cd /opt/nsp/nfmp/auxdb/install/bin`

24

Enter the following:

`# ./auxdbAdmin.sh distributeConfig`

The updated auxiliary database configuration is distributed to each auxiliary database station.

25

Enter the following:

`# ./auxdbAdmin.sh rebalance`

You are prompted for the database user password.

26

Enter the password.

You are prompted to confirm the rebalance operation.

27

Enter YES. The rebalance operation begins.

When the rebalance is complete, the following is displayed:
Cluster rebalance completed. Press a key to continue...

Press a key.

Perform the following steps on each main server station.

Note: In a redundant system, you must perform the steps on the standby main server station first.

1. Log in to the main server station as the nsp user.
2. Open a console window.
3. Enter the following:
   
   ```bash
   cd /opt/nsp/nfmp/server/nms/bin
   ```
4. Enter the following:
   
   ```bash
   ./nmsserver.bash stop
   ```
5. Enter the following:
   
   ```bash
   ./nmsserver.bash appserver_status
   ```
   The server status is displayed; the server is fully stopped if the status is the following:
   
   Application Server is stopped
   
   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.
6. Enter the following to switch to the root user:
   
   ```bash
   su -
   ```
7. Enter the following:
   
   ```
   # samconfig -m main
   ```
   The following is displayed:
   
   Start processing command line inputs...

   <main>

8. Enter the following:

   ```
   <main> configure auxdb ip-list address1,address2...addressN,new_address exit
   ```
   where

   address1,address2...addressN are the existing auxiliary database station IP addresses

   new_address is the IP address from which the new station communicates with the NFM-P servers

9. Enter the following:
    
    ```
    <main> apply
    ```
    The configuration is applied.
10. Enter the following:
   ```bash
   <main> exit 
   The samconfig utility closes.
   ```

11. Enter the following to switch back to the nsps user:
   ```bash
   # exit 
   ```

30
On the standalone or primary main server station, enter the following to start the main server:
```bash
bash$ ./nmsserver.bash start 
```
The main server starts, and the station is added to the auxiliary database.

31
If the NFM-P system is redundant, enter the following on the standby main server station to start the main server:
```bash
bash$ ./nmsserver.bash start 
```
The main server starts.

32
Close the open console windows.

END OF STEPS
8 NFM-P qcow2 deployment

8.1 Introduction

8.1.1 Description
You can deploy a collocated standalone NFM-P system in a VM from a set of qcow2 disk images. One image is for the RHELOS, and the other contains the NFM-P main server and database software.

After you deploy the qcow2 image set as described in 8.2 "To deploy a collocated standalone NFM-P system using a qcow2 image" (p. 239), the NFM-P system is operational.

Note: Only IPv4 addressing is supported for NFM-P system deployment using the image set.

8.2 To deploy a collocated standalone NFM-P system using a qcow2 image

8.2.1 Description
The following steps describe how to deploy a collocated standalone NFM-P system in a VM using a qcow2 disk image.

Note: The Bash shell is the supported command shell for RHEL CLI operations.

8.2.2 Steps

1. Log in to the VM host station as the root user.

2. Download the following files to a local directory on the station:
   • NSP_NFM-P_R_r_COLLOCATED_OS.qcow2
   • NSP_NFM-P_R_r_COLLOCATED_STANDALONE.qcow2
   where R_r is the NFM-P release identifier

3. Open a console window.

4. Convert the qcow2 files to raw format.
   1. Navigate to the directory that contains the qcow2 files.
   2. Enter the following:
NFM-P qcow2 deployment
To deploy a collocated standalone NFM-P system using a qcow2 image

```
# qemu-img convert -f qcow2 NSP_NFM-P_R_r_COLLOCATED_OS.qcow2 -O raw -S 0 raw_OS.img
```

3. Enter the following:
```
# qemu-img convert -f qcow2 NSP_NFM-P_R_r_COLLOCATED_STANDALONE.qcow2 -O raw -S 0 raw_software.img
```
where
- **R_r** is the NFM-P release identifier
- **raw_OS** is the name to assign to the raw OS image file
- **raw_software** is the name to assign to the raw software image file

5. Resize the raw software image.
   1. Navigate to the directory that contains the raw software image file created in Step 4.
   2. Enter the following:
```
# qemu-img resize raw_software.img sizeG
```
where
- **raw_software.img** is the file to resize
- **size** is the size value from your Platform Sizing Response

6. For live deployments and for optimal disk performance, convert the raw image file from sparse format to non-sparse format; enter the following:

   **Note:** The operation may take many minutes, depending on the file size.
```
# cp --sparse=never raw_software.img non-sparse_software.img
```
where
- **raw_software.img** is the raw software image file resized in Step 5
- **non-sparse_software.img** is the name to assign to the non-sparse software image file

7. Enter the following to deploy the VM:
```
# virt-install --connect qemu:///system --ram RAM --vcpus=cores --name instance --os-type=linux --os-variant=rhel7 --disk path=raw_OS.img,device=disk,bus=virtio,format=raw,io=native,cache=none --disk path=non-sparse_software.img,device=disk,bus=virtio,format=raw,io=native,cache=none --network bridge=bridge_name --import
```
where
- **bridge_name** is the name assigned to the VM network bridge
- **cores** is the required number of CPU cores in your Platform Sizing Response
- **instance** is the name to assign to the VM
non-sparse_software.img is the name of the non-sparse software image file created in Step 6. RAM is the required amount of VM RAM from your Platform Sizing Response, in Mbytes; for example, 64Gbytes is expressed as 65536, which is 64 x 1024Mbytes.

raw_OS.img is the name of the OS image file created in Step 4.

8

When the NFM-P VM is instantiated, log in as the root user on the VM; the default password is available from technical support.

9

Set a secure password for the root user.
1. Enter the following:
   \# passwd
   The following prompt is displayed:
   New Password:
2. Enter a secure password.
   The following prompt is displayed:
   Confirm Password:
3. Re-enter the password.
4. Record the password and store it in a secure location.

10

Enter the following:
\# pvresize /dev/vdb

11

Enter the following:
\# lsblk
Basic disk partition information is displayed; the value in the SIZE column is the partition size in Gbytes.

12

As required, enter one or more of the following commands to extend the logical volumes for the partitions.

**Note:** You need to enter a command only if the SIZE value is lower than the partition size in your Platform Sizing Response.

**Note:** The lvextend command does nothing if a partition size is equal to or greater than the associated Platform Sizing Response value. In such a case, the command returns a failure message that you can ignore.

\# lvextend -L sizeG /dev/vg2/lv_nsp
forcespaceextend -L sizeG /dev/vg2/lv_nsp
forcespaceextend -L sizeG /dev/vg2/lv_log
forcespaceextend -L sizeG /dev/vg2/lv_xmloutput
forcespaceextend -L sizeG /dev/vg2/lv_db
forcespaceextend -L sizeG /dev/vg2/lv_archivelog
forcespaceextend -L sizeG /dev/vg2/lv_dbbbackup
forcespaceextend -L sizeG /dev/vg2/lv_nebackup (required only if size is greater than 1Gbyte)
forcespaceextend -L sizeG /dev/vg2/lv_var_log
forcespaceextend -L sizeG /dev/vg2/lv_var_log_audit
forcespaceextend -L sizeG /dev/vg2/lv_extra

where size is the partition size, in Gbytes, from your Platform Sizing Response

13

For each partition modified in Step 12, enter the associated command in the following list:
# resize2fs /dev/mapper/vg2-lv_nsp
# resize2fs /dev/mapper/vg2-lv_nspos
# resize2fs /dev/mapper/vg2-lv_log
# resize2fs /dev/mapper/vg2-lv_xmloutput
# resize2fs /dev/mapper/vg2-lv_db
# resize2fs /dev/mapper/vg2-lv_archivelog
# resize2fs /dev/mapper/vg2-lv_dbbbackup
# resize2fs /dev/mapper/vg2-lv_nebackup
# xfs_growfs /dev/mapper/vg2-lv_var_log
# xfs_growfs /dev/mapper/vg2-lv_var_log_audit
# resize2fs /dev/mapper/vg2-lv_extra

14

Set a secure password for the VM nsp user.

1. Enter the following:
   # passwd nsp
The following prompt is displayed:
   New Password:

2. Enter a secure password.
The following prompt is displayed:
   Confirm Password:

3. Re-enter the password.

4. Record the password and store it in a secure location.
Plumb each required network interface with an IPv4 address, network mask, and gateway address. See the OS documentation for configuration information.

Enter the following to set the station hostname:

```
# hostnamectl set-hostname hostname
```

where `hostname` is a short hostname or FQDN, depending on your requirement

Update the `/etc/hosts` file to map the station hostname to the IP address of an interface, as described in 2.4 “Using hostnames in the management network” (p. 19).

Enter the following to configure and create the main database:

```
# samconfig -m db
```

The following is displayed:

Start processing command line inputs...

Enter the following to begin the database creation:

```
<db> apply
```

The database creation begins, and progress messages are displayed.

The following is displayed when the database creation is complete:

```
DONE
db configurations updated.
```
When the database creation is complete, enter the following:

```
<db> exit
```

The samconfig utility closes.

Enter the following to configure and enable the main server:

```
# samconfig -m main
```

The following is displayed:

```
Start processing command line inputs...
```

Verify the main server configuration.

1. Enter the following:
   
   ```
   <main> show-detail
   ```

   The main server configuration is displayed.

2. Review each parameter to ensure that the value is correct.

3. Configure one or more parameters, if required.

4. When you are certain that the configuration is correct, enter the following:
   
   ```
   <main configure> back
   ```

   The prompt changes to `<main>`.

Enter the following:

```
<main> apply
```

The configuration is applied.

Enter the following:

```
<main> exit
```

The samconfig utility closes.

Enter the following to switch to the nsp user:

```
# su - nsp
```

Enter the following:
bash$ cd /opt/nsp/nfmp/server/nms/bin

Enter the following to start the main server:
bash$ ./nmsserver.bash start

Enter the following:
bash$ ./nmsserver.bash appserver_status

The server status is displayed; the server is fully initialized if the status is the following:
Application Server process is running. See nms_status for more detail.

When the server is fully initialized, close the console window.

END OF STEPS
To deploy a collocated standalone NFM-P system using a qcow2 image
# 9 5620 SAM upgrade to NFM-P

## 9.1 Overview

### 9.1.1 Purpose

This chapter describes how to upgrade the components of a standalone or redundant 5620 SAM system to create an NFM-P system.

### 9.1.2 Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1 Overview</td>
<td>247</td>
</tr>
<tr>
<td>Introduction</td>
<td>248</td>
</tr>
<tr>
<td>9.2 General information</td>
<td>248</td>
</tr>
<tr>
<td>9.3 To perform the pre-upgrade tasks</td>
<td>249</td>
</tr>
<tr>
<td>Standalone 5620 SAM system upgrade to NFM-P</td>
<td>262</td>
</tr>
<tr>
<td>9.4 Standalone 5620 SAM system upgrade workflow</td>
<td>262</td>
</tr>
<tr>
<td>9.5 To upgrade a standalone 5620 SAM system to the NFM-P</td>
<td>264</td>
</tr>
<tr>
<td>Redundant 5620 SAM system upgrade to NFM-P</td>
<td>285</td>
</tr>
<tr>
<td>9.6 Component references</td>
<td>285</td>
</tr>
<tr>
<td>9.7 Redundant 5620 SAM system upgrade workflow</td>
<td>286</td>
</tr>
<tr>
<td>9.8 To upgrade a redundant 5620 SAM system to the NFM-P</td>
<td>291</td>
</tr>
<tr>
<td>5620 SAM auxiliary server upgrade</td>
<td>329</td>
</tr>
<tr>
<td>9.9 To upgrade a 5620 SAM auxiliary server</td>
<td>329</td>
</tr>
<tr>
<td>5620 SAM Cflowd auxiliary server upgrade</td>
<td>335</td>
</tr>
<tr>
<td>9.10 To upgrade a 5620 SAM Cflowd auxiliary server</td>
<td>335</td>
</tr>
<tr>
<td>5620 SAM auxiliary database upgrade</td>
<td>340</td>
</tr>
<tr>
<td>9.11 To upgrade a 5620 SAM auxiliary database</td>
<td>340</td>
</tr>
<tr>
<td>5620 SAM analytics server upgrade</td>
<td>351</td>
</tr>
<tr>
<td>9.12 To upgrade the 5620 SAM analytics servers</td>
<td>351</td>
</tr>
</tbody>
</table>
9.2 General information

9.2.1 Description

This chapter describes how to perform a complete 5620 SAM system upgrade to the NFM-P. One workflow and procedure describe a standalone 5620 SAM system upgrade, and another workflow and procedure describe a redundant upgrade.

Each workflow and procedure has links to upgrade procedures for the following optional 5620 SAM components:

- auxiliary server
- Cflowd auxiliary server
- auxiliary database
- analytics server

Chapter 14, “Single-user client deployment” and Chapter 15, “Client delegate server deployment” describe single-user GUI client and client delegate server installation and upgrade.

Note: It is strongly recommended that you verify the checksum of each software package or file that you download from OLCS. You can compare the checksum value on the download page with, for example, the output of the RHEL md5sum or sha256sum command. See the appropriate RHEL man page for information.

Note: Before you begin a 5620 SAM system upgrade, you must perform 9.3 “To perform the pre-upgrade tasks” (p. 249) to collect the required information and ensure that the required conditions are in place.

Special 5620 SAM upgrade requirements

A 5620 SAM-to-NFM-P system upgrade has the following special requirements.

- The upgrade requires a new RHEL OS installation, so is essentially a platform migration, although the existing hardware may be adequate. The migration preserves the component configurations and database content.

- You cannot use an SSL certificate from a 5620 SAM system in an NFM-P system. If your 5620 SAM system is SSL-secured, you must generate new TLS keystore and truststore files using one of the following methods described in Chapter 6, “TLS configuration and management”:
  - automated—see “Automated TLS deployment procedures” (p. 90)
  - manual—see “Manual TLS deployment procedures” (p. 105)

The samconfig utility is used for NFM-P component configuration and deployment; see Chapter 3, “Using samconfig” for information about using samconfig.

Note: If you are replacing any stations in the system as part of the upgrade, it is recommended that you commission the new stations in advance of the upgrade to reduce the upgrade duration.
Table 9-1  5620 SAM-to-NFM-P upgrade procedures list

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.3 “To perform the pre-upgrade tasks” (p. 249)</td>
<td>Prepare a standalone or redundant 5620 SAM system for an upgrade to an NFM-P system by backing up data and ensuring that the required upgrade conditions are in place.</td>
</tr>
<tr>
<td>9.5 “To upgrade a standalone 5620 SAM system to the NFM-P” (p. 264)</td>
<td>Upgrade all components of a standalone 5620 SAM system to create a standalone NFM-P system.</td>
</tr>
<tr>
<td>9.8 “To upgrade a redundant 5620 SAM system to the NFM-P” (p. 291)</td>
<td>Upgrade all components of a redundant 5620 SAM system to create a redundant NFM-P system.</td>
</tr>
<tr>
<td>9.9 “To upgrade a 5620 SAM auxiliary server” (p. 329)</td>
<td>Upgrade the 5620 SAM auxiliary server software on a station to the NFM-P.</td>
</tr>
<tr>
<td>9.10 “To upgrade a 5620 SAM Cflowd auxiliary server” (p. 335)</td>
<td>Upgrade the 5620 SAM Cflowd auxiliary server software on a station to create an NSP Flow Collector.</td>
</tr>
<tr>
<td>9.11 “To upgrade a 5620 SAM auxiliary database” (p. 340)</td>
<td>Upgrade a 5620 SAM auxiliary database to the NFM-P.</td>
</tr>
<tr>
<td>9.12 “To upgrade the 5620 SAM analytics servers” (p. 351)</td>
<td>Upgrade the analytics servers in a 5620 SAM system to NSP analytics servers.</td>
</tr>
</tbody>
</table>

9.3 To perform the pre-upgrade tasks

9.3.1 Description

CAUTION

Service Disruption

A system upgrade fails unless you strictly observe the requirements and restrictions in Chapter 2, “Before you begin” and the NSP NFM-P Planning Guide.

An NFM-P system upgrade requires a thorough understanding of the deployment restrictions and requirements.

It is essential that you plan, document, and test the upgrade procedure in advance on a lab system that is representative of the actual network. Contact technical support to assess the upgrade requirements of your system; in a large or complex network, it is strongly recommended that you engage the technical support upgrade service.

The following steps describe the actions that you must perform in advance of a standalone or redundant system upgrade.

Note: You require the following user privileges on each server station in the system:

- root
- samadmin

Note: The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:

- # —root user
• bash$ —nsp and samadmin users

Note: The Bash shell is the supported command shell for RHEL CLI operations.

9.3.2 Steps

CAUTION

Deployment failure

The RHEL OS of any NFM-P component requires specific versions of some RHEL packages. If the required package versions are not installed, the component upgrade fails.

See 4.10.4 “Special RHEL OS package requirements” (p. 59) for the required package versions.

Commission new stations, if required

1

If you are replacing one or more stations in the system, commission each replacement station according to the platform specifications in this guide and in the *NSP NFM-P Planning Guide*.

Check and configure firewalls

2

Before you attempt to upgrade a 5620 SAM system to the NFM-P, you must ensure that each firewall between the system components allows the required traffic to pass between the components, or is disabled. You can configure and enable the firewalls after the upgrade, if required.

Note: An upgrade from the 5620 SAM to the NFM-P requires a new RHEL OS installation, after which the RHEL Firewalld service is typically enabled by default.

If you are moving any NFM-P components to new stations, rather than re-using the existing stations, perform one of the following.

a. Configure each firewall to allow the required traffic to pass. See the *NSP NFM-P Planning Guide* for a list of the ports that must be open on each component.

    Note: The RHEL Firewalld service must be configured using the Firewalld rules in the *NSP NFM-P Planning Guide*, which describes using NFM-P templates for rule creation.

b. Disable each firewall; see the external firewall documentation, or perform the following steps on each component station to disable Firewalld.

   1. Log in to the station as the root user.
   2. Open a console window.
   3. Enter the following:

      ```
      # systemctl stop firewalld
      ```
   4. Enter the following:
# systemctl disable firewalld

5. Close the console window.

Download installation files

3

Download the following NFM-P installation files to an empty directory on a station that is not affected by the upgrade activity:

Note: The station must be reachable by each station that is to host an NFM-P main server or main database.

- linuxMigration.sh
- nsp-nfmp-jre-R.r.p-rel.v.rpm
- nsp-nfmp-config-R.r.p-rel.v.rpm
- nsp-nfmp-nspos-R.r.p-rel.v.rpm
- nsp-nfmp-main-server-R.r.p-rel.v.rpm
- nsp-nfmp-oracle-R.r.p-rel.v.rpm
- nsp-nfmp-main-db-R.r.p-rel.v.rpm
- OracleSw_PreInstall.sh

where

$R.r.p$ is the NSP release identifier, in the form MAJOR.minor.patch

$v$ is a version identifier

Validate database

4

Before you upgrade a main database, you must ensure that the main database contains only valid records, or the upgrade fails.

Note: In a redundant system, you must perform the validation on the primary main database station.

Log in as the root user on the main database station.

5

Transfer the following downloaded file to an empty directory on the main database station:

- OracleSw_PreInstall.sh

6

Navigate to the directory that contains the OracleSw_PreInstall.sh file.
Enter the following:

```
# chmod +x OracleSw_PreInstall.sh
```

Perform the following steps.

1. Enter the following:

```
# ./OracleSw_PreInstall.sh -check
```

   The following prompt is displayed:

   Enter the password for the "SYS" Oracle user (terminal echo is off):

2. Enter the SYS user password.

   The following messages are displayed:

   Logging Oracle pre install checks to log_file
   In upgrade check mode, this script does not modify the system.
   About to validate that the database can be upgraded to release.
   Found the database installation directory /opt/5620sam/db/install.

   If the validation is successful, the following messages and prompt are displayed:

   INFO: Database upgrade validation passed.

3. If the validation is successful, go to Step 9.

4. If the script detects one or more invalid items, for example, an NE at a release that the new NFM-P software does not support, an incomplete deployment, or other upgrade restriction, one line like the following is displayed for each item:

   ERROR: Error message

   The following is displayed as the script exits.

   ERROR: The database cannot be upgraded. Please fix the above errors and re-run this script.

   Remove the upgrade restriction. For example, clear an incomplete deployment, or upgrade an unsupported NE to a release that the new software supports.

5. Run the script again; go to substep 1.

Verify database archive log synchronization

If the system is redundant, ensure that no archive log gap exists between the primary and standby main databases.

**Note:** If you attempt a database upgrade when an archive log gap exists, the upgrade fails.

1. Open a 5620 SAM GUI client.
2. View the Standby DB entry in the GUI status bar.
3. If the entry reads “Database archive log gap”, you must reinstantiate the standby database. Otherwise, go to Step 10.
4. Choose Administration→System Information from the main menu. The System Information form opens.
5. Click Re-Instantiate Standby.
6. Click Yes to confirm the action. The reinstatement begins, and the GUI status bar displays reinstatement information.
   Note: Database reinstatement takes considerable time if the database contains a large amount of statistics data.
   You can also use the System Information form to monitor the reinstatement progress. The Last Attempted Standby Re-instantiation Time is the start time; the Standby Re-instantiation State changes from In Progress to Success when the reinstatement is complete.
7. When the reinstatement is complete, close the System Information form.

Back up database

10 Log in as the root user on the main database station.
   Note: In a redundant system, you must log in to the primary database station.

11 Open a console window.

12 CAUTION
   Data Loss
   The path of the database backup directory must not include the database installation directory, or data loss may occur.
   Ensure that the backup directory path that you specify does not include /opt/5620sam/samdb.
   Note: A database backup deletes the contents of the specified backup directory. Ensure that the backup directory that you specify does not contain files that you want to retain.
   Note: The backup directory that you specify must be a directory on a local mounted partition.
   Note: The Oracle management user requires read and write permissions on the backup directory that you specify.
Note: Depending on the database size, the backup operation may take considerable time. Enter the following:

Note: The compress option shown in the command specifies the use of file compression, and is optional.

```bash
# sambackupDb backup_directory compress
```

where `backup_directory` is the absolute path of the directory that is to contain the database backup file set.

The database backup begins, and status messages are displayed as the backup progresses:

The following is displayed when the backup is complete:

```
<date time> Database backup was successful
DONE
```

When the backup is complete, transfer the backup file set to a secure location on a separate station that is unaffected by the upgrade activity.

Perform 9500 MPR migration pre-upgrade tasks

If you are upgrading a Release 14.0 R6 or earlier 5620 SAM system that manages one or more 9500 MPR devices, perform “To perform pre-upgrade tasks” in the NSP NFM-P Wavence User Guide.

Note: The 9500 MPR is renamed Wavence in Release 18.0; the device name shown in the NFM-P client GUI may vary, depending on the device release.

Back up main server configuration

Perform the following steps on each main server station.

1. Log in as the root user on the main server station.
2. Transfer the following downloaded file to an empty directory on the main server station:
   - `linuxMigration.sh`
3. Open a console window.
4. Navigate to the directory that contains the `linuxMigration.sh` file.
5. Enter the following:
   ```bash
   # chmod +x linuxMigration.sh
   ```
6. Enter the following:
   ```bash
   # ./linuxMigration.sh -t main
   ```
   The following prompt is displayed:
Please specify a target directory for the backups (default is /opt/importConfigs):

7. Enter the absolute path of a target directory for the backup files, or press ↵ to accept the default.

   **Note:** The directory must exist, and the directory name must not contain a space character.

   If the directory does not have sufficient capacity for the backup files, you are prompted to enter a different directory name. Otherwise, the following is displayed and the backup begins:

   Backup NFM-P main config contents.

   When the backup is complete, the following is displayed:

   Please backup/transfer backup_dir/importConfigs/mainserverBackupConfigs.tar.gz to a secure location.

   You must restore this file to the /opt/importConfigs directory on the RHEL 7 station before installing the rpm(s).

The script creates the following file:

- `backup_dir/importConfigs/mainserverBackupConfigs.tar.gz`

  where `backup_dir` is the specified backup directory

Transfer the file to a secure location on a separate station that is unaffected by the upgrade activity.

**Note:** In a redundant system, you must ensure that you record which main server the file is from.

### Back up main server data files

Perform the following steps on each main server station to back up the NE configuration files.

**Note:** Although the backup uses file compression, the resulting file may consume a large amount of disk space. Although the `/opt/5620sam/nebackup` partition is typically of sufficient size to hold the backup file and the existing content, you can use the following command to display the amount of space, in Gbytes, that the uncompressed nebackup files currently consume:

```
du -hs /opt/5620sam/nebackup
```

**Note:** Backing up the NE configuration files may take considerable time.

1. Log in as the samadmin user on the main server station.
2. Open a console window.
3. Enter the following:

   ```
   bash$ cd /opt/5620sam/nebackup
   ```
4. Remove any previously created backups in the directory, for example, in /opt/5620sam/nebackup/backup.

5. Enter the following:
   
   ```bash
   tar zcvf nebackup_`date +%m-%d-%H-%M-%S` .tar.gz *
   ```
   
   The command creates a tar.gz file in the /opt/5620sam/nebackup directory; the file name includes a timestamp.

6. If the NFM-P system is redundant, record which main server the backup file is from.

7. Transfer the backup file to a secure location on a station that is unaffected by the upgrade activity.

---

**Perform the following steps on each main server station to back up the remaining data files.**

**Note:** Although the backup uses file compression, the resulting file set may consume a large amount of disk space. The backup location that you specify must be on a partition other than /opt/5620sam, and must be of sufficient size to hold the backup file set. To assist with sizing the backup location, you can use the following command to display the space, in Gbytes, that a directory to be backed up in the following steps consumes in uncompressed form:

```
du -hs directory
```

**Note:** The samadmin user requires read and write permissions on the backup location.

1. Log in as the samadmin user on the main server station.

2. Open a console window.

3. Enter the following:
   
   ```bash
   cd /opt/5620sam
   ```

4. Enter the following:
   
   ```bash
   tar zcvf backup_location/lte_`date +%m-%d-%H-%M-%S` .tar.gz lte/
   ```
   
   where `backup_location` is the absolute path of the backup location

5. Enter the following:
   
   ```bash
   tar zcvf backup_location/nelogs_`date +%m-%d-%H-%M-%S` .tar.gz nelogs/
   ```

6. Enter the following:
   
   ```bash
   tar zcvf backup_location/nesoftware_`date +%m-%d-%H-%M-%S` .tar.gz nesoftware/
   ```

7. Enter the following:
   
   ```bash
   tar zcvf backup_location/os_`date +%m-%d-%H-%M-%S` .tar.gz os/
   ```

8. Enter the following:
   
   ```bash
   tar zcvf backup_location/savedResults_`date +%m-%d-%H-%M-%S` .tar.gz server/script/savedResults/
   ```
9. Each tar command creates one .tar.gz file in the backup location. Each file name includes a timestamp.
   If the NFM-P system is redundant, record which main server the file set is from.
10. Transfer the .tar.gz file set to a secure location on a station that is unaffected by the upgrade activity.

Back up custom configuration files

CAUTION

Service Disruption

An NFM-P upgrade does not preserve all non-default settings in configuration files such as nms-server.xml.

If an NFM-P configuration file contains non-default settings that you want to retain after an upgrade, contact technical support for assistance before the upgrade.

Note: At the beginning of an NFM-P main or auxiliary server upgrade, specific configuration and log files are copied to a directory under the installation directory; the directory name includes a timestamp. The directories below the main server installation directory are then deleted. If you have created or customized a file below the main server installation directory, you risk losing the file unless you create a backup copy.

Make a backup copy of each file that you have created or customized in or below the /opt/5620sam/server directory on each main server station, and store the backup files on a separate station that is not affected by the NFM-P upgrade activity.

Back up Analytics report repository

The NSP Analytics application saves the most recent 5000 scheduled report results. If the Results folder in your Analytics application has more than 5000 saved report results, and you want to preserve the results, use the export function in the application to transfer the results to a secure location.

Verify compatibility with external systems

Ensure that the new NFM-P software is compatible with the software release of each external system that connects to the NFM-P. Contact technical support for information about external system compatibility.
Close LogViewer

22

Close the LogViewer utility, if it is open.

Validate main server and GUI client firewall configuration

23

Confirm that the firewalls between the main servers and the single-user GUI clients and client delegate servers allow traffic to the HTTP or HTTPS port required for client access. Otherwise, you cannot install or upgrade a single-user client or client delegate server.

See the *NSP NFM-P Planning Guide* for NFM-P port assignment information.

Verify NFM-P policy compatibility with managed NEs

24

You must confirm that the new NFM-P release supports the software release of each managed NE and pre-provisioned NE, as stated in the *NSP NFM-P and 5620 SAM Network Element Compatibility Guide*. Perform one of the following for each NE that is at an unsupported release.

**Note:** If the system that you are upgrading manages an NE as a GNE, and the new NFM-P release supports native management of the device type and release, you must unmanage and delete the GNE before you attempt the upgrade. After the upgrade, the NFM-P can discover and manage the device as a native NE instead of a GNE.

a. Upgrade the device software to a release that the new NFM-P software supports; see the appropriate device documentation and the *NSP NFM-P User Guide* for information about performing NE software upgrades.

b. Remove the NE from the NFM-P managed network; see the “Discovering devices using the NFM-P” chapter of the *NSP NFM-P User Guide* for information.
   1. Unmanage the NE.
   2. Delete the NE from the managed network.
   3. Administratively disable or remove the discovery rule element for the NE.

c. Delete the pre-provisioned NE using the NFM-P Pre-Provisioned NE Manager; see the “Self-configuration and discovery” chapter of the *NSP NFM-P LTE RAN User Guide*.

Gather required information

25

Choose Administration→System Information from the main menu. The System Information form opens.
Record the following information:

- Domain Name
- **Primary Server panel:**
  - IP Address
  - Host Name
  - Status
- **Primary Database Server panel:**
  - Database Name
  - Instance Name
  - IP Address
  - Host Name

If the system is redundant, record the following additional information:

- **Standby Server panel:**
  - IP Address
  - Host Name
  - Status
- **Standby Database Server panel:**
  - Database Name
  - Instance Name
  - IP Address
  - Host Name

If the system includes one or more auxiliary servers, click on the Auxiliary Services tab. A list of auxiliary servers is displayed. Otherwise, go to Step 31.

Perform the following steps for each auxiliary server listed on the form.

1. Select the auxiliary server and click Properties. The auxiliary server properties form opens.
2. Record the following information for use during the upgrade:
   - Host Name
   - Auxiliary Server Type
   - Server Status
   - Public IP address
   - Private IP address, if displayed
3. Close the auxiliary server properties form.
Record which auxiliary servers have a check mark in the Selected column.

**Note:** In 9.8 “To upgrade a redundant 5620 SAM system to the NFM-P” (p. 291), the Selected auxiliary servers are collectively referred to as [Aux1]; the remaining auxiliary servers are collectively referred to as [Aux2].

If the system includes one or more client delegate servers, click on the Client Delegate Servers tab. Otherwise, go to [Step 33](#).

Perform the following steps for each client delegate server listed on the form:
1. Select the client delegate server and click Properties. The client delegate server properties form opens.
2. Record the IP Address value for use during the upgrade.
3. Close the properties form.

Close the System Information form.

Obtain and record the following additional information for each main server:
- root user password
- samadmin user password
- additional IP addresses, if NAT or multiple interfaces are used:
  - IP address that each main database must use to reach the main server
  - IP address that the GUI and XML API clients must use to reach the main server; the public IP address, if NAT is used
  - IP address that the auxiliary servers must use to reach the main server
  - private IP address, if NAT is used

Obtain and record the following additional main database information:
- root user password
- Oracle management user information:
  - username; installation default is oracle
  - password
  - group name; installation default is dba
- Oracle database user information:
  - username; installation default is samuser
  - password
• Oracle SYS user password
• additional database IP addresses, if NAT or multiple interfaces are used:
  − IP address that each main server must use to reach the database
  − IP address that each auxiliary server must use to reach the database

Close client sessions

36

Close the open GUI and XML API client sessions, as required.
1. Open a GUI client using an account with security management privileges, such as admin.
3. Click on the Sessions tab.
4. Click Search. The form lists the open GUI and XML API client sessions.
5. Identify the GUI session that you are using based on the value in the Client IP column.
6. Select all sessions except for the following:
   • the session that you are using
   • the sessions required to monitor the network during a redundant system upgrade
7. Click Close Session.
8. Click Yes to confirm the action.
9. Click Search to refresh the list and verify that only the required sessions are open.

Uninstall Mac OS X clients

37

A Mac OS X single-user client upgrade from the 5620 SAM is not supported.
Uninstall each single-user client installed on Mac OS X.

Note: You are directed to install the new Mac OS X client software at the end of the system upgrade procedure.

Close GUI client

38

If the GUI client that you are using is not required for network monitoring during the upgrade, close the client.

END OF STEPS

Release 18.9
September 2018
Issue 1

3HE-14075-AAAC-TQZZA
Standalone 5620 SAM system upgrade to NFM-P

9.4 Standalone 5620 SAM system upgrade workflow

9.4.1 Description

The following is the sequence of high-level actions required to upgrade a standalone 5620 SAM / NFM-P system.

9.4.2 Stages

Note: The links in the "Upgrade standalone system" (p. 262) stages lead to sections in 9.5 "To upgrade a standalone 5620 SAM system to the NFM-P" (p. 264).

Prepare system for upgrade

1

Perform 9.3 "To perform the pre-upgrade tasks" (p. 249) to prepare for the upgrade.

Upgrade standalone system

2

If the system includes one or more analytics servers or Cflowd auxiliary servers, stop each; see "Stop analytics servers, Cflowd auxiliary servers" (p. 264).

3

Prepare the main server for the upgrade; see "Stop and disable standalone main server" (p. 265).
1. Stop the main server.
2. Disable automatic main server startup.

4

Upgrade the main database; see "Upgrade standalone main database" (p. 266).
1. Stop the main database.
2. If required, recommission the existing main database station.
3. Run a script on the new or recommissioned station to prepare for the Oracle software installation.
4. Install the required packages.
5. Restore the database.
6. Run the database upgrade script.
7. Verify and modify the database configuration, as required.

5
If the system includes one or more auxiliary servers, stop the auxiliary servers; see “Stop auxiliary servers” (p. 274).

Upgrade the main server; see “Upgrade standalone main server” (p. 275).

If the system includes one or more auxiliary servers, upgrade each auxiliary server; see “Upgrade auxiliary servers” (p. 280).

If the system includes one or more Cflowd auxiliary servers, upgrade each Cflowd auxiliary server; see “Upgrade Cflowd auxiliary servers” (p. 281).

If the system includes an auxiliary database, upgrade the auxiliary database; see “Upgrade auxiliary database” (p. 281).

If the system includes one or more auxiliary servers, start each auxiliary server; see “Start auxiliary servers” (p. 281).

Restore the main server data files; see “Restore standalone main server data files” (p. 279).

Start the main server; see “Start main server” (p. 281).

If the system includes one or more analytics servers, upgrade each analytics server; see “Upgrade analytics servers” (p. 282).

Install or upgrade single-user GUI clients, as required; see “Install or upgrade single-user GUI clients” (p. 282).

Install or upgrade client delegate servers, as required; see “Install or upgrade client delegate servers” (p. 282).

If you are using a PKI server to deploy TLS, stop the PKI server; see “Stop PKI server” (p. 283).
If the 5620 SAM system has customized TLS version and cipher support, restore the custom TLS support settings; see “Restore TLS version and cipher support configuration” (p. 283).

If required, perform the 9500 MPR migration post-upgrade tasks; see “Perform 9500 MPR migration post-upgrade tasks” (p. 283).

Configure and enable firewalls, if required; see “Configure and enable firewalls” (p. 283).

9.5 To upgrade a standalone 5620 SAM system to the NFM-P

9.5.1 Description

The following steps describe how to upgrade a collocated or distributed main database and main server in a standalone deployment. The steps include links to procedures for installing and upgrading optional NFM-P components.

Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

Note: You require the following user privileges:
• on each server station in the system — root, samadmin
• on the main database station — root, database_user

Note: The upgrade creates the nsp user on each server station in the system.

Note: The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:
• # — root user
• bash$ — nsp and samadmin users

9.5.2 Steps

1. Open at least one GUI client to monitor the network during the upgrade.

Stop analytics servers, Cflowd auxiliary servers

2. If the system includes one or more analytics servers, stop each analytics server.
   1. Log in to the analytics server station as the samadmin user.
   2. Open a console window.
3. Enter the following:

```
bash$ /opt/5620sam/analytics/bin/AnalyticsAdmin.sh stop
```

The following is displayed:

```
Stopping 5620 SAM Analytics Server
```

When the analytics server is completely stopped, the following message is displayed:

```
5620 SAM Analytics Server is not running
```

If the system includes one or more Cflowd auxiliary servers, stop each Cflowd auxiliary server.

1. Log in to the Cflowd auxiliary server station as the root user.
2. Open a console window.
3. Navigate to the Cflowd auxiliary server installation directory, which is one of the following:
   - Release 14.0 R5 or earlier—/opt/5620sam/dcp-R_rRn, where R_rRn is the software release identifier
   - Release 14.0 R6 or later—/opt/5620sam/dcp
4. Enter the following:

```
# ./bin/dcpctl.sh stop
```

Output like the following is displayed.

```
Stopping 5620 SAM Cflowd Auxiliary Server ... 5620 SAM Cflowd Auxiliary Server is stopped successfully
```

Stop and disable standalone main server

4. Stop the main server.

1. Log in to the main server station as the samadmin user.
2. Open a console window.
3. Enter the following:

```
bash$ cd /opt/5620sam/server/nms/bin
```
4. Enter the following:

```
bash$ ./nmsserver.bash stop
```
5. Enter the following:

```
bash$ ./nmsserver.bash appserver_status
```

The server status is displayed; the server is fully stopped if the status is the following:

```
Application Server is stopped
```

If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.
Disable the automatic main server startup so that the main server does not start in the event of a power disruption during the upgrade.
1. Enter the following to switch to the root user:
   ```bash
   su -
   ```
2. Enter the following:
   ```
   cd /etc/init.d
   ```
3. Enter the following to rename the main server startup daemon:
   ```
   mv 5620SAMServerWrapper inactive.5620SAMServerWrapper
   ```

Upgrade standalone main database

Stop the main database and proxy services.
1. Log in to the database station as the root user.
2. Open a console window.
3. Enter the following:
   ```
   cd /etc/rc3.d
   ```
4. Enter the following to stop the Oracle proxy:
   ```
   ./S965620SAMOracleProxyWrapper stop
   ```
5. Enter the following to stop the database:
   ```
   ./S95db5620sam stop
   ```

Disable the automatic database proxy startup.
1. Enter the following:
   ```
   cd /etc/init.d
   ```
2. Enter the following:
   ```
   mv 5620SAMOracleProxyWrapper inactive.5620SAMOracleProxyWrapper
   ```

If you are re-using the main database station, recommission the station according to the platform specifications in this guide and in the NSP NFM-P Planning Guide.

Log in as the root user on the station that is commissioned as the main database station.

Transfer the following downloaded files to an empty directory on the station:
- nsp-nfmp-jre-\textit{R}.\textit{r}.\textit{p}-rel.\textit{v}.rpm
Transfer the following downloaded file to an empty directory on the station:

- OracleSw_PreInstall.sh

Open a console window.

You must prepare the station for the Oracle software installation. Navigate to the directory that contains the OracleSw_PreInstall.sh file.

Enter the following:

```
# chmod +x OracleSw_PreInstall.sh
```

Enter the following:

```
./OracleSw_PreInstall.sh
```

Note: A default value is displayed in brackets []. To accept the default, press Enter. If you specify a value other than the default, you must record the value for use when the OracleSw_PreInstall.sh script is run during a software upgrade, or when the Oracle management user information is required by technical support.

The following prompt is displayed:

This script will prepare the system for a new install/restore of an NFM-P Version Release main database.

Do you want to continue? [Yes/No]:

Enter Yes. The following prompt is displayed:

Enter the Oracle dba group name [group]:

Enter a group name.
Note: To reduce the complexity of subsequent software upgrades and technical support activities, it is recommended that you accept the default.

The following messages and prompt are displayed:

Creating group group if it does not exist...
done
Enter the Oracle user name:

Enter a username.

Note: To reduce the complexity of subsequent software upgrades and technical support activities, it is recommended that you accept the default.

The following messages and prompt are displayed:

Oracle user [username] new home directory will be [/opt/nsp/nfmp/oracle12r1].
Checking or Creating the Oracle user home directory /opt/nsp/nfmp/oracle12r1...
Checking user username...
Adding username...
Changing ownership of the directory /opt/nsp/nfmp/oracle12r1 to username:group.
About to unlock the UNIX user [username]
Unlocking password for user username.
passwd: Success
Unlocking the UNIX user [username] completed
Please assign a password to the UNIX user username..
New Password:

Enter a password. The following prompt is displayed:

Re-enter new Password:

Re-enter the password. The following is displayed if the password change is successful:

passwd: password successfully changed for username

The following message and prompt are displayed:

Specify whether an NFM-P Main Server will be installed on this workstation.

The database memory requirements will be adjusted to account for the additional load.
Will the database co-exist with an NFM-P Main Server on this workstation [Yes/No]:

Enter Yes or No, as required.

Messages like the following are displayed as the script execution completes:

INFO: About to set kernel parameters in /etc/sysctl.conf...
INFO: Completed setting kernel parameters in /etc/sysctl.conf...
INFO: About to change the current values of the kernel parameters
INFO: Completed changing the current values of the kernel parameters
INFO: About to set ulimit parameters in /etc/security/limits.conf... 
INFO: Completed setting ulimit parameters in /etc/security/limits.conf...
INFO: Completed running Oracle Pre-Install Tasks, you *MUST* reboot your box.

When the script execution is complete, enter the following to reboot the station:

```
# systemctl reboot
```

The station reboots.

When the reboot is complete, log in as the root user on the main database station.

Open a console window.

Navigate to the NFM-P software directory.

**Note:** Ensure that the directory contains only the installation files.

Enter the following:

```
# chmod +x *
```

Enter the following:

```
# yum install *.rpm
```

The yum utility resolves any package dependencies, and displays the following prompt:

Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:

Enter y. The following and the installation status are displayed as each package is installed:

- Downloading packages:
- Running transaction check
- Running transaction test
- Transaction test succeeded
- Running transaction

The package installation is complete when the following is displayed:
Complete!

Transfer the database backup file set to the station.

**Note:** The path to the backup file set must be the same as the original backup path, which is named in the BACKUP_SUMMARY.INFO file from the backup file set; for example:

- Backup Path Name:
  /opt/5620sam/dbbackup/backupset_1

**Note:** Ensure that the Oracle management user has full access to the directory and contents.

Enter the following:

```
# samrestoreDb path -migrate
```

where `path` is the absolute path of the database backup file set

The database restore begins, and messages like the following are displayed as the restore progresses.

- Restore log is /opt/nsp/nfmp/db/install/NFM-P_Main_Database.restore. yyyy.mm.dd-hh.mm.ss.stdout.txt
- <date time> working..
- <date time> Performing Step 1 of 7 - Initializing ..
- <date time> Executing StartupDB.sql ...
- <date time> Performing Step 2 of 7 - Extracting backup files ..... 
- <date time> Performing Step 3 of 7 - Restoring archive log files ..
- <date time> Performing Step 4 of 7 - Executing restore.rcv .......... 
- <date time> Performing Step 5 of 7 - Restoring Accounting tablespaces .......
- <date time> Performing Step 6 of 7 - Opening database ..... 

5620 SAM upgrade to NFM-P
Standalone 5620 SAM system upgrade to NFM-P
To upgrade a standalone 5620 SAM system to the NFM-P

Release 18.9
September 2018
Issue 1
You must prepare the restored database for the upgrade.

Navigate to the directory that contains the OracleSw_PreInstall.sh file.

Enter the following:

```
# ./OracleSw_PreInstall.sh
```

**Note:** A default value is displayed in brackets []. To accept the default, press `s`.

**Note:** If you specify a value other than the default, you must record the value for use when the OracleSw_PreInstall.sh script is run during a software upgrade, or when the Oracle management user information is required by technical support.

The following prompt is displayed:

```
This script will prepare the system for an upgrade to NFM-P Version R.r Rn database.
Do you want to continue? [Yes/No]:
```

Enter Yes. The following messages and prompt are displayed:

About to validate that the database can be upgraded to release.
Found the database installation directory /opt/5620sam/samdb/install.
Existing NFM-P database version = version
Enter the password for the "SYS" Oracle user (terminal echo is off):

Enter the SYS user password.

The script begins to validate the database records, and displays the following:

Validating the database for upgrade. Please wait ...

If the validation is successful, the following messages and prompt are displayed:

```
INFO: Database upgrade validation passed.
```
Creating group group if it does not exist ...

Checking or Creating the Oracle user home directory
/opt/5620sam/oracle12r1...

Checking user username...
usermod: no changes

Changing ownership of the directory /opt/5620sam/oracle12r1 to username:group.

About to unlock the UNIX user [username]
Unlocking password for user username.
passwd: Success

Unlocking the UNIX user [username] completed

Do you want to change the password for the UNIX user username?
[Yes/No]:
Go to Step 36.

35

If the database contains an invalid item, for example, an NE at a release that the new NFM-P software does not support, the following is displayed and the script exits:

ERROR: Unsupported records found in database. Please remove the following unsupported items first:

Please remove the following unsupported items first:

item_1
item_2
.
.
item_n

ERROR: The database cannot be upgraded. Please fix the above errors and re-run this script.

Perform the following steps.

1. Use an NFM-P GUI client to remove or update the unsupported items, as required. For example, upgrade an unsupported NE to a release that the new software supports.

2. Run the script again; go to Step 32.

36

Perform one of the following.

a. Enter No to retain the current password.

b. Specify a new password.

   1. Enter Yes. The following prompt is displayed:

      New Password:
2. Enter a password. The following prompt is displayed:
   Re-enter new Password:

3. Re-enter the password. The following is displayed if the password change is successful:
   passwd: password successfully changed for username

The following message and prompt are displayed:
Specify whether an NFM-P server will be installed on this workstation. The database memory requirements will be adjusted to account for the additional load.
Will the database co-exist with an NFM-P server on this workstation [Yes/No]:

Enter Yes or No, as required.

Messages like the following are displayed as the script execution completes:
INFO: About to remove kernel parameters set by a previous run of this script from /etc/sysctl.conf
INFO: Completed removing kernel parameters set by a previous run of this script from /etc/sysctl.conf
INFO: About to set kernel parameters in /etc/sysctl.conf...
INFO: Completed setting kernel parameters in /etc/sysctl.conf...
INFO: About to change the current values of the kernel parameters
INFO: Completed changing the current values of the kernel parameters
INFO: About to remove ulimit parameters set by a previous run of this script from /etc/security/limits.conf
INFO: Completed removing ulimit parameters set by a previous run of this script from /etc/security/limits.conf
INFO: About to set ulimit parameters in etc/security/limits.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.conf...
INFO: Completed running Oracle Pre-Install Tasks

Enter the following to upgrade the database:
   # samupgradeDb

The following prompt is displayed:
Enter the password for the "user" database user (terminal echo is off):

Enter the database user password.
The following is displayed as the database upgrade begins:

Validating...

**Note:** A database upgrade may take considerable time.

When the upgrade is complete, verify the database configuration.

1. Enter the following:
   
   ```
   # samconfig -m db
   ```

   The following is displayed:
   
   Start processing command line inputs...
   
2. Enter the following:

   ```
   <db> show-detail
   ```

   The database configuration is displayed.

3. Review each parameter to ensure that the value is correct.

4. Configure one or more parameters, if required, and then enter `back`; see Chapter 3, “Using samconfig” for information about using the samconfig utility.

5. If you change one or more parameters, enter the following:

   ```
   <db> apply
   ```

   The configuration is applied.

6. Enter the following:

   ```
   <db> exit
   ```

   The samconfig utility closes.

It is recommended that as a security measure, you limit the number of database user login failures that the NFM-P allows before the database user account is locked; see “NFM-P database management procedures” in the *NSP NFM-P System Administrator Guide*.

**Note:** You do not need to perform the step if the database has been configured before the upgrade to limit the user login failures.

**Stop auxiliary servers**

If the system includes one or more auxiliary servers, stop each auxiliary server.

1. Log in to the auxiliary server station as the samadmin user.
2. Open a console window.
3. Enter the following:
bash$ /opt/5620sam/auxserver/nms/bin/auxnmsserver.bash auxstop

The auxiliary server stops.

**Upgrade standalone main server**

43

If the main server and database are on separate stations, and you are re-using the main server station, recommission the station according to the platform specifications in this guide and in the *NSP NFM-P Planning Guide*.

44

Log in as the root user on the station that is commissioned as the main server station.

45

Open a console window.

46

Enter the following:

```
# mkdir /opt/importConfigs
```

47

Transfer the mainserverBackupConfigs.tar.gz file created in 9.3 “To perform the pre-upgrade tasks” (p. 249) to the /opt/importConfigs directory.

48

Perform one of the following.

a. If the main server and database are collocated on one station, transfer the following downloaded installation files to the NFM-P software directory on the station:

   - nsp-nfmp-nspos-\textit{R}.\textit{r}.\textit{p}.rpm
   - nsp-nfmp-main-server-\textit{R}.\textit{r}.\textit{p}.rpm

b. If the main server and database are on separate stations, transfer the following downloaded installation files to an empty directory on the main server station:

   - nsp-nfmp-nspos-\textit{R}.\textit{r}.\textit{p}.rpm
   - nsp-nfmp-jre-\textit{R}.\textit{r}.\textit{p}+rel.\textit{v}.rpm
   - nsp-nfmp-config-\textit{R}.\textit{r}.\textit{p}+rel.\textit{v}.rpm
   - nsp-nfmp-main-server-\textit{R}.\textit{r}.\textit{p}.rpm

**Note:** In subsequent steps, the directory is called the NFM-P software directory.

49

Navigate to the NFM-P software directory.
**Note:** Ensure that the directory contains only the installation files.

50

Enter the following:

```bash
# chmod +x *
```

51

Enter the following:

```bash
# yum install *.rpm
```

The `yum` utility resolves any package dependencies, and displays the following prompt:

- **Total size:** nn G
- **Installed size:** nn G
- **Is this ok [y/d/N]:**

52

Enter `y`. The following and the installation status are displayed as each package is installed:

- **Downloading packages:**
- **Running transaction check**
- **Running transaction test**
- **Transaction test succeeded**
- **Running transaction**

The package installation is complete when the following is displayed:

**Complete!**

53

When all packages are installed, perform one of the following.

**Note:** You cannot use a 5620 SAM TLS certificate or keystore in an NFM-P system.

- **a.** If you are deploying TLS using an NSP PKI server, perform 6.7 “To configure and enable an NSP PKI server” (p. 91).

- **b.** If you are using the manual TLS deployment method, generate and distribute the required TLS files for the system, as described in 6.11 “Workflow for manual TLS deployment” (p. 105).

54

Enter the following; see Chapter 3, “Using samconfig” for information about using samconfig:

**Note:** Regardless of whether you intend to modify the main server configuration, you must apply the main server configuration, as described in the following steps.

```bash
# samconfig -m main
```
The following is displayed:
Start processing command line inputs...
<main>

Enter the following:
<main> configure  

The prompt changes to <main configure>.

To apply an NFM-P license, enter the following, and then enter back ↓:

Note: You cannot start a main server unless the main server configuration includes a current and valid license. You can use samconfig to specify the license file, or import the license, as described in “Software and license configuration procedures” in the NSP NFM-P System Administrator Guide.

<main configure> license license_file  

where license_file is the absolute path and file name of the NSP license bundle

Configure the tls parameters in the following table, and then enter back ↓.

Note: You cannot use a 5620 SAM TLS certificate or keystore in an NFM-P system.

Table 9-2  Standalone main server parameters — tls

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keystore-file</td>
<td>The absolute path of the TLS keystore file</td>
</tr>
<tr>
<td></td>
<td>To enable automated TLS deployment, enter no keystore-file. Default: /opt/nsp/os/tls/nsp.keystore</td>
</tr>
<tr>
<td>keystore-pass</td>
<td>The TLS keystore password</td>
</tr>
<tr>
<td></td>
<td>Default: available from technical support</td>
</tr>
<tr>
<td>truststore-file</td>
<td>The absolute path of the TLS truststore file</td>
</tr>
<tr>
<td></td>
<td>To enable automated TLS deployment, enter no truststore-file. Default: /opt/nsp/os/tls/nsp.truststore</td>
</tr>
<tr>
<td>truststore-pass</td>
<td>The TLS truststore password</td>
</tr>
<tr>
<td></td>
<td>Default: available from technical support</td>
</tr>
<tr>
<td>alias</td>
<td>The alias specified during keystore generation</td>
</tr>
<tr>
<td></td>
<td>You must configure the parameter. Default: —</td>
</tr>
</tbody>
</table>

5620 SAM upgrade to NFM-P
Standalone 5620 SAM system upgrade to NFM-P
To upgrade a standalone 5620 SAM system to the NFM-P

Release 18.9
September 2018
Issue 1 3HE-14075-AAAC-TQZZA 277
Table 9-2  Standalone main server parameters — tls (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pki-server</td>
<td>If you are using the automated TLS deployment method, the IP address or hostname of the PKI server. You must configure the parameter if no keystore-file value is specified. Default: —</td>
</tr>
<tr>
<td>pki-server-port</td>
<td>If you are using the automated TLS deployment method, the TCP port on which the PKI server listens for and services requests. Default: 2391</td>
</tr>
<tr>
<td>webdav</td>
<td>Whether WebDAV access to eNodeB activation data is enabled on the main server. Default: false</td>
</tr>
</tbody>
</table>

Verify the main server configuration.

1. Enter the following:
   `<main configure> show`  
   The main server configuration is displayed.

2. Review each parameter to ensure that the value is correct.

3. Configure one or more parameters, if required; see Chapter 3, “Using samconfig” for information about using the samconfig utility.

4. When you are certain that the configuration is correct, enter the following:
   `<main configure> back`  
   The prompt changes to `<main>`.

Enter the following:

   `<main> apply`  
   The configuration is applied.

Enter the following:

   `<main> exit`  
   The samconfig utility closes.
Restore standalone main server data files

Transfer the nebackup_timestamp.tar.gz file created in Step 18 of 9.3 “To perform the pre-upgrade tasks” (p. 249) to the /opt/nsp/nfmp/nebackup directory on the main server station.

Enter the following:
```
# cd /opt/nsp/nfmp/nebackup
```

Enter the following:
```
# chown nsp:nsp *.tar.gz
```

Enter the following:
```
# tar -xf nebackup_timestamp.tar.gz -C /opt/nsp/nfmp/
```

where timestamp is a backup timestamp in the format MM-DD-hh-mm

The main server nebackup data files are restored to the /opt/nsp/nfmp/nebackup directory.

After the backup file is restored, the backup file is no longer required, and may consume a large amount of disk space. To remove the backup file, enter the following:
```
# rm -f nebackup_*.*.tar.gz
```

Transfer the remaining files in the backup file set created in Step 18 of 9.3 “To perform the pre-upgrade tasks” (p. 249) to the /opt/nsp/nfmp directory on the main server station.

Enter the following:
```
# cd /opt/nsp/nfmp
```

Enter the following:
```
# chown nsp:nsp *.tar.gz
```

Enter the following commands:
```
# tar -xf lte_timestamp.tar.gz -C /opt/nsp/nfmp/
# tar -xf nelogs_timestamp.tar.gz -C /opt/nsp/nfmp/
```
# tar -xf nesoftware_timestamp.tar.gz -C /opt/nsp/nfmp/  
# tar -xf os_timestamp.tar.gz -C /opt/nsp/nfmp/  
# tar -xf savedResults_timestamp.tar.gz -C /opt/nsp/nfmp/  
where timestamp is a backup timestamp in the format MM-DD-hh-mm

The remaining main server data files are restored to the appropriate directories.

The backup files are no longer required. To remove a backup file, enter the following:

```
# rm -f filename.tar.gz
```

where filename is the name of a backup file

Enter the following:
```
# chown -R nsp:nsp lte
```

Enter the following:
```
# chown -R nsp:nsp nebackup
```

Enter the following:
```
# chown -R nsp:nsp nelogs
```

Enter the following:
```
# chown -R nsp:nsp nesoftware
```

Enter the following:
```
# chown -R nsp:nsp os
```

Enter the following:
```
# chown -R nsp:nsp server/script/savedResults
```

**Upgrade auxiliary servers**

If the system includes one or more auxiliary servers, perform 9.9 “To upgrade a 5620 SAM auxiliary server” (p. 329) on each auxiliary server station.
Notice: Do not perform the final step that describes starting the auxiliary server.

Upgrading Cflowd auxiliary servers

If the system includes one or more Cflowd auxiliary servers, perform 9.10 “To upgrade a 5620 SAM Cflowd auxiliary server” (p. 335) on each Cflowd auxiliary server station.

Upgrading auxiliary database

If the system includes an auxiliary database, perform 9.11 “To upgrade a 5620 SAM auxiliary database” (p. 340).

Starting auxiliary servers

If the system includes one or more auxiliary servers, start each auxiliary server.
1. Log in to the auxiliary server station as the sps user.
2. Open a console window.
3. Enter the following:
   ```bash
   /opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash auxstart
   ```
   The auxiliary server starts.

Starting main server

CAUTION

Service Disruption

An NFM-P system upgrade is not complete until each main server performs crucial post-upgrade tasks during initialization.

Before you attempt an operation that requires a server shutdown, you must ensure that each main server is completely initialized, or the operation fails.

Note: You cannot start a main server unless the main server configuration includes a current and valid license. You can use samconfig to specify the license file, or import a license, as described in “Software and license configuration procedures” in the NSP NFM-P System Administrator Guide.

Start the main server.
1. Enter the following to switch to the sps user:
su - nsp

2. Enter the following:
   bash$ cd /opt/nsp/nfmp/server/nms/bin

3. Enter the following:
   bash$ ./nmsserver.bash start

4. Enter the following:
   bash$ ./nmsserver.bash appserver_status

   The server status is displayed; the server is fully initialized if the status is the following:
   Application Server process is running. See nms_status for more detail.
   If the server is not fully initialized, wait five minutes and then repeat this step. Do not
   perform the next step until the server is fully initialized.

If the NFM-P is to manage wireless NEs, enter the following to update the memory
configuration accordingly for GUI clients:
   bash$ ./nmsdeploytool.bash clientmem -l

Close the console window.

Upgrade analytics servers

If the system includes one or more analytics servers, perform 9.12 “To upgrade the 5620 SAM
analytics servers” (p. 351) to upgrade each analytics server.

Install or upgrade single-user GUI clients

As required, perform the following to install or upgrade single-user GUI clients:

• 14.4 “To install a single-user GUI client” (p. 564)
• 14.5 “To upgrade an NFM-P Release 17 or 5620 SAM single-user GUI client” (p. 569)

Install or upgrade client delegate servers

As required, perform the following to install or upgrade client delegate servers:

• 15.3 “To install a client delegate server” (p. 584)
• 15.5 “To upgrade an NFM-P Release 17 or 5620 SAM client delegate server” (p. 596)
Stop PKI server

If you are deploying TLS using an NSP PKI server, stop the PKI server, as described at the end of 6.7 “To configure and enable an NSP PKI server” (p. 91).

Restore TLS version and cipher support configuration

A 5620 SAM system upgrade to the NFM-P does not preserve your changes to the system support for specific TLS versions and ciphers.

If the 5620 SAM system had customized TLS settings before the upgrade, perform “To update the supported NFM-P TLS versions and ciphers” in the NSP NFM-P System Administrator Guide to restore the settings on the NFM-P system.

Perform 9500 MPR migration post-upgrade tasks

If you are upgrading a Release 14.0 R6 or earlier 5620 SAM system that manages one or more 9500 MPR devices, perform “To perform post-upgrade tasks” in the NSP NFM-P Wavence User Guide.

Note: The 9500 MPR is renamed Wavence in Release 18.0; the device name shown in the NFM-P client GUI may vary, depending on the device release.

Configure and enable firewalls

If you intend to use any firewalls between the NFM-P components, and the firewalls are disabled, configure and enable each firewall.

Perform one of the following.

a. Configure each external firewall to allow the required traffic using the port assignments in the NSP NFM-P Planning Guide, and enable the firewall.

b. Configure and enable Firewalld on each component station, as required.
   1. Use an NFM-P template to create the Firewalld rules for the component, as described in the NSP NFM-P Planning Guide.
   2. Log in to the station as the root user.
   3. Open a console window.
   4. Enter the following:
      
      # systemctl enable firewalld

      5. Enter the following:

      # systemctl start firewalld
6. Close the console window.

END OF STEPS
Redundant 5620 SAM system upgrade to NFM-P

9.6 Component references

9.6.1 Description

CAUTION

Service Disruption

A redundant NFM-P system upgrade involves a network management outage.
Ensure that you perform the upgrade during a scheduled maintenance period of sufficient duration to accommodate the outage.

During a redundant NFM-P system upgrade, the primary and standby roles of the main servers and databases reverse, as do the Preferred and Reserved auxiliary server roles. As a result, the use of relative component identifiers such as primary and standby can cause confusion.

To clearly identify components during a redundant system upgrade, you can use the figure below. The components on the left manage the network before the upgrade, and the components on the right manage the network after the upgrade. Each component in the figure has an absolute identifier in brackets, for example, [DB1], that clearly identifies the component in the redundant system upgrade workflow and procedure steps.
9.7 Redundant 5620 SAM system upgrade workflow

9.7.1 Description

The following is the sequence of high-level actions required to upgrade a redundant NFM-P system.

9.7.2 Stages

Note: The links in the "Upgrade redundant system" (p. 287) stages lead to sections in 9.8 "To upgrade a redundant 5620 SAM system to the NFM-P" (p. 291).

Prepare system for upgrade

1

Perform 9.3 "To perform the pre-upgrade tasks" (p. 249) to prepare the NFM-P system for the upgrade.
Upgrade redundant system

2
Stop and disable the standby main server; see “Stop and disable standby main server [Main2]” (p. 292).

3
If the system includes auxiliary servers, stop the [Aux2] auxiliary servers; see “Stop auxiliary servers [Aux2]” (p. 293).

4
Disable the system redundancy functions; see “Disable database redundancy” (p. 293).

5
Upgrade the standby main database, which becomes the new primary main database; see “Upgrade standby main database [DB2]” (p. 294).
   1. Stop the main database.
   2. If required, recommission the existing main database station.
   3. Run a script on the new or recommissioned station to prepare for the Oracle software installation.
   4. Install the database packages.
   5. Restore the database.
   6. Run the database upgrade script.
   7. Verify and modify the database configuration, as required.

6
Upgrade the standby main server; see “Upgrade standby main server [Main2]” (p. 303).

7
If the NFM-P system includes one or more analytics servers or Cflowd auxiliary servers, stop each; see “Stop analytics servers, Cflowd auxiliary servers” (p. 309).

8
If the NFM-P system includes auxiliary servers, upgrade the [Aux2] auxiliary servers; see “Upgrade auxiliary servers [Aux2]” (p. 309).

9
Stop and disable the original primary main server; see “Stop and disable original primary main server [Main1]” (p. 310).

Note: This stage marks the beginning of the network management outage.
If the system includes one or more Cflowd auxiliary servers, upgrade each Cflowd auxiliary server; see “Upgrade Cflowd auxiliary servers” (p. 310).

If the NFM-P system includes auxiliary servers, stop the [Aux1] auxiliary servers; see “Stop auxiliary servers [Aux1]” (p. 310).

If the NFM-P system includes an auxiliary database, upgrade the auxiliary database; see “Upgrade auxiliary database” (p. 311).

Stop the original primary main database; see “Stop original primary main database [DB1]” (p. 311).

Restore the new primary main server data files; see “Restore main server [Main2] data files” (p. 307).

Start the new primary main server; see “Start new primary main server [Main2]” (p. 312).

If the system includes auxiliary servers, start the [Aux2] auxiliary servers; see “Start auxiliary servers [Aux2]” (p. 313).

If the system includes one or more analytics servers, upgrade each analytics server; see “Upgrade analytics servers” (p. 313).

Upgrade or install at least one NFM-P single-user client or client delegate server; see “Enable GUI client” (p. 313).

Note: This stage marks the end of the network management outage.

Perform sanity testing on the NFM-P system using a GUI client; see “Test upgraded system using GUI client” (p. 313).

Install the new standby main database; see “Install new standby main database [DB1]” (p. 314).
1. Stop the main database.
2. If required, recommission the existing main database station.
3. Run a script on the new or recommissioned station to prepare for the Oracle software installation.
4. Install the database packages.
5. Configure the standby database.
6. Verify and modify the database configuration, as required.

21
Reinstantiate the standby database; see “Reinstantiate standby database” (p. 319).

22
Upgrade the original primary main server as the new standby main server; see “Upgrade original primary main server [Main1]” (p. 319).

23
Restore the new standby main server data files; see “Restore main server [Main1] data files” (p. 323).

24
Start the new standby main server; see “Start new standby main server” (p. 325).

25
If the system includes auxiliary servers, upgrade the [Aux1] auxiliary servers; see “Upgrade auxiliary servers [Aux1]” (p. 326).

26
If the system includes auxiliary servers, start the [Aux1] auxiliary servers; see “Start auxiliary servers [Aux1]” (p. 326).

27
Install or upgrade single-user GUI clients, as required; see “Install or upgrade single-user GUI clients” (p. 326).

28
Install or upgrade client delegate servers, as required; see “Install or upgrade client delegate servers” (p. 326).

29
If you are using a PKI server to deploy TLS, stop the PKI server; see “Stop PKI server” (p. 327).
If the 5620 SAM system has customized TLS version and cipher support, restore the custom TLS support settings; see “Restore TLS version and cipher support configuration” (p. 327).

If required, perform the 9500 MPR migration post-upgrade tasks; see “Perform 9500 MPR migration post-upgrade tasks” (p. 327).

Configure and enable firewalls, if required; see “Configure and enable firewalls” (p. 327).

### 9.7.3 Concurrent task execution

Some system upgrade operations require considerable time. To reduce the duration of a redundant system upgrade, you can perform some actions concurrently.

The following table lists the redundant system upgrade workflow tasks in a format that involves two operators, A and B, who perform tasks concurrently when possible.

#### Table 9-3 Workflow for concurrent task execution during redundant upgrade

<table>
<thead>
<tr>
<th>System redundancy mode</th>
<th>Operator A actions</th>
<th>Operator B actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>DUPLEX</td>
<td>Stage 1 — Actions described in 9.3 “To perform the pre-upgrade tasks” (p. 249)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Stage 2 — “Stop and disable standby main server [Main2]” (p. 292)</td>
<td>Stage 3 — “Stop auxiliary servers [Aux2]” (p. 293)</td>
</tr>
<tr>
<td></td>
<td>Stage 5 — “Upgrade standby main database [DB2]” (p. 294)</td>
<td>Stage 6 — “Upgrade standby main server [Main2]” (p. 303)</td>
</tr>
<tr>
<td></td>
<td>Stage 7 — “Stop analytics servers, Cflowd auxiliary servers” (p. 309)</td>
<td>Stage 8 — “Upgrade auxiliary servers [Aux2]” (p. 309)</td>
</tr>
<tr>
<td>O U T A G E</td>
<td>Stage 9 — “Stop and disable original primary main server [Main1]” (p. 310)</td>
<td>Stage 10 — “Upgrade Cflowd auxiliary servers” (p. 310)</td>
</tr>
<tr>
<td></td>
<td>Stage 11 — “Stop auxiliary servers [Aux1]” (p. 310)</td>
<td>Stage 12 — “Upgrade auxiliary database” (p. 311)</td>
</tr>
<tr>
<td></td>
<td>Stage 13 — “Stop original primary main database [DB1]” (p. 311)</td>
<td>Stage 14 — “Restore main server [Main2] data files” (p. 307)</td>
</tr>
<tr>
<td></td>
<td>Stage 15 — “Start new primary main server [Main2]” (p. 312)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: The outage persists until device discovery completes.</td>
<td>Stage 16 — “Start auxiliary servers [Aux2]” (p. 313)</td>
</tr>
</tbody>
</table>
### Table 9-3  Workflow for concurrent task execution during redundant upgrade (continued)

<table>
<thead>
<tr>
<th>System redundancy mode</th>
<th>Operator A actions</th>
<th>Operator B actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIMPLEX</td>
<td>Stage 18 — “Enable GUI client” (p. 313)</td>
<td>—</td>
</tr>
<tr>
<td>SIMPLEX</td>
<td>Stage 19 — “Test upgraded system using GUI client” (p. 313)</td>
<td>—</td>
</tr>
<tr>
<td>SIMPLEX</td>
<td>Stage 20 — “Install new standby main database [DB1]” (p. 314)</td>
<td>—</td>
</tr>
<tr>
<td>SIMPLEX</td>
<td>Stage 21 — “Reinstantiate standby database” (p. 319)</td>
<td>Stage 22 — “Upgrade original primary main server [Main1]” (p. 319)</td>
</tr>
<tr>
<td>SIMPLEX</td>
<td>Stage 23 — “Restore main server [Main1] data files” (p. 323)</td>
<td>—</td>
</tr>
<tr>
<td>DULEX</td>
<td>Stage 24 — “Start new standby main server” (p. 325)</td>
<td>Stage 25 — “Upgrade auxiliary servers [Aux1]” (p. 326)</td>
</tr>
<tr>
<td>DULEX</td>
<td>Stage 26 — “Start auxiliary servers [Aux1]” (p. 326)</td>
<td>Stage 27 — “Install or upgrade single-user GUI clients” (p. 326)</td>
</tr>
<tr>
<td>DULEX</td>
<td>Stage 28 — “Install or upgrade client delegate servers” (p. 326)</td>
<td>Stage 29 — “Stop PKI server” (p. 327)</td>
</tr>
<tr>
<td>DULEX</td>
<td>Stage 30 — “Restore TLS version and cipher support configuration” (p. 327)</td>
<td>Stage 31 — “Perform 9500 MPR migration post-upgrade tasks” (p. 327)</td>
</tr>
<tr>
<td>DULEX</td>
<td>Stage 32 — “Configure and enable firewalls” (p. 327)</td>
<td>—</td>
</tr>
</tbody>
</table>

### 9.8 To upgrade a redundant 5620 SAM system to the NFM-P

#### 9.8.1 Description

The following steps describe how to upgrade a collocated or distributed main database and main server in a redundant deployment. The steps include links to procedures for installing and upgrading optional NFM-P components.

Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

> **Note:** You require the following user privileges:
> 1. on each server station in the system — root, samadmin
> 2. on each main database station — root

> **Note:** The upgrade creates the nspr user on each server station in the system.

> **Note:** The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:
> 1. # — root user
> 2. bash$ — nspr and samadmin users
9.8.2 Steps

**CAUTION**

 Deployment failure

The RHEL OS of any NFM-P component requires specific versions of some RHEL packages. If the required package versions are not installed, the component upgrade fails.

See 4.10.4 “Special RHEL OS package requirements” (p. 59) for the required package versions.

Stop and disable standby main server [Main2]

1. Open a GUI client to monitor the network during the upgrade.

2. Stop the standby main server.
   1. Log in to the standby main server station as the samadmin user.
   2. Open a console window.
   3. Enter the following:
      ```bash
      cd /opt/5620sam/server/nms/bin
      ```
   4. Enter the following:
      ```bash
      ./nmsserver.bash stop
      ```
   5. Enter the following:
      ```bash
      ./nmsserver.bash appserver_status
      ```
      The server status is displayed; the server is fully stopped if the status is the following:
      ```Application Server is stopped
      ```
      If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

3. Disable the automatic main server startup so that the main server does not start in the event of a power disruption during the upgrade.
   1. Enter the following to switch to the root user:
      ```bash
      su -
      ```
   2. Enter the following:
      ```
      cd /etc/init.d
      ```
   3. Enter the following to rename the main server startup daemon:
      ```bash
      mv 5620SAMServerWrapper inactive.5620SAMServerWrapper
      ```
Stop auxiliary servers [Aux2]

If the NFM-P system includes auxiliary servers, stop each appropriate auxiliary server [Aux2].

1. Log in to the auxiliary server station as the samadmin user.
2. Open a console window.
3. Enter the following:

   ```bash
   /opt/5620sam/auxserver/nms/bin/auxnmsserver.bash auxstop
   ```

   The auxiliary server stops.

Disable database redundancy

Disable the main database failover and switchover functions.

1. Log in to the primary main server station [Main1] as the samadmin user.
2. Open a console window.
3. Enter the following to navigate to the main server configuration directory:

   ```bash
   cd /opt/5620sam/server/nms/config
   ```

5. Open the nms-server.xml file with a plain-text editor, for example, vi.
6. Locate the section that begins with the following tag:

   ```xml
   <db
   ```

7. Locate the following line in the section:

   ```xml
   host="address"
   ```

8. Ensure that the `address` value in the line is the IP address of main database [DB1].
9. Locate the following line in the section:

   ```xml
   database="instance_name"
   ```

10. Ensure that the `instance_name` value is the instance name of main database [DB1].
11. Edit the following line in the section that reads:

    ```xml
    redundancyEnabled="true"
    ```

    to read:

    ```xml
    redundancyEnabled="false"
    ```

12. Save and close the nms-server.xml file.
13. Enter the following:

    ```bash
    /opt/5620sam/server/nms/bin/nmsserver.bash read_config
    ```

    The main server puts the change into effect, and database redundancy is disabled.
Upgrade standby main database [DB2]

6
Stop the main database and proxy services.
1. Log in to the database station as the root user.
2. Open a console window.
3. Enter the following:
   
   ```
   # cd /etc/rc3.d
   ```
4. Enter the following to stop the Oracle proxy:
   
   ```
   # ./S965620SAMOracleProxyWrapper stop
   ```
5. Enter the following to stop the database:
   
   ```
   # ./S95db5620sam stop
   ```

7
Disable the automatic database proxy startup.
1. Enter the following:
   
   ```
   # cd /etc/init.d
   ```
2. Enter the following:
   
   ```
   # mv 5620SAMOracleProxyWrapper inactive.5620SAMOracleProxyWrapper
   ```

8
If analytics aggregations are enabled, perform the following steps to disable all aggregation rules.

**Note:** Disabling analytics aggregation during a redundant system upgrade prevents the duplication of aggregation data in the NFM-P database, but does not cause the loss of any aggregation data.

Upon startup, if a primary main server detects that the most recent aggregation data is not current, the server performs the interim aggregations. If aggregation is enabled during a redundant upgrade, the original primary main server creates aggregations while the standby main server is upgraded. In such a case, after the standby main server starts as the new primary main server, the server may perform aggregations that are duplicates of the aggregations performed by the original primary main server.

The required aggregation rules are automatically enabled on the new primary main server, so the server performs the interim aggregations upon startup. If aggregation is disabled at the start of a redundant upgrade, no aggregation duplication occurs.
1. Open an NFM-P GUI client.
2. Choose Tools → Analytics → Aggregation Manager from the NFM-P main menu. The Aggregation Manager form opens.
3. Click Search. The aggregation rules are listed.
4. Click on the Enable Aggregation column to sort the rules so that the rules that have aggregation enabled are at the top of the list.
5. Select all rules that have a check mark in the Enable Aggregation column.


7. Deselect Enable Aggregation.

8. Click OK. The Aggregation Rule (multiple instances) [Edit] form closes.

9. Click OK to save your changes and close the Aggregation Manager form.

10. Close the NFM-P GUI client.

If you are re-using the standby main database [DB2] station, recommission the station according to the platform specifications in this guide and in the NSP NFM-P Planning Guide.

**Note:** After the upgrade, the station is the new primary main database station.

Log in as the root user on the station that is commissioned as the main database [DB2] station.

Transfer the following downloaded files to an empty directory on the station:

- nsp-nfmp-jre-R.r.p-rel.v.rpm
- nsp-nfmp-config-R.r.p-rel.v.rpm
- nsp-nfmp-oracle-R.r.p-rel.v.rpm
- nsp-nfmp-main-db-R.r.p-rel.v.rpm

**Note:** In subsequent steps, the directory is called the NFM-P software directory.

Transfer the following downloaded file to an empty directory on the station:

- OracleSw_PreInstall.sh

Open a console window.

You must prepare the station for the Oracle software installation. Navigate to the directory that contains the OracleSw_PreInstall.sh file.

Enter the following:

```
# chmod +x OracleSw_PreInstall.sh
```
Enter the following:

```
# ./OracleSw_PreInstall.sh
```

*Note:* A default value is displayed in brackets []. To accept the default, press `Enter`.

*Note:* If you specify a value other than the default, you must record the value for use when the `OracleSw_PreInstall.sh` script is run during a software upgrade, or when the Oracle management user information is required by technical support.

The following prompt is displayed:

This script will prepare the system for a new install/restore of an NFM-P Version Release main database.

Do you want to continue? [Yes/No]:

Enter Yes. The following prompt is displayed:

Enter the Oracle dba group name [group]:

Enter a group name.

*Note:* To reduce the complexity of subsequent software upgrades and technical support activities, it is recommended that you accept the default.

The following messages and prompt are displayed:

Creating group group if it does not exist...
done

Enter the Oracle user name:

Enter a username.

*Note:* To reduce the complexity of subsequent software upgrades and technical support activities, it is recommended that you accept the default.

The following messages and prompt are displayed:

Oracle user [username] new home directory will be
[/opt/nsp/nfmp/oracle12r1].
Checking or Creating the Oracle user home directory
/opt/nsp/nfmp/oracle12r1...,
Checking user username...
Adding username...
Changing ownership of the directory /opt/nsp/nfmp/oracle12r1 to
username:group.
About to unlock the UNIX user [username]
Unlocking password for user username.
`passwd: Success`
Unlocking the UNIX user [username] completed
Please assign a password to the UNIX user username..
New Password:

Enter a password. The following prompt is displayed:
Re-enter new Password:

Re-enter the password. The following is displayed if the password change is successful:
`passwd: password successfully changed for username`

The following message and prompt are displayed:
Specify whether an NFM-P Main Server will be installed on this workstation.
The database memory requirements will be adjusted to account for the additional load.
Will the database co-exist with an NFM-P Main Server on this workstation [Yes/No]:

Enter Yes or No, as required.
Messages like the following are displayed as the script execution completes:
`INFO: About to set kernel parameters in /etc/sysctl.conf...`
`INFO: Completed setting kernel parameters in /etc/sysctl.conf...`
`INFO: About to change the current values of the kernel parameters`
`INFO: Completed changing the current values of the kernel parameters`
`INFO: About to set ulimit parameters in /etc/security/limits.conf...`
`INFO: Completed setting ulimit parameters in /etc/security/limits.conf...`
`INFO: Completed running Oracle Pre-Install Tasks, you *MUST* reboot your box.

When the script execution is complete, enter the following to reboot the main database station:
`# systemctl reboot`
The station reboots.
When the reboot is complete, log in to the main database [DB2] station as the root user.

Open a console window.

Navigate to the NFM-P software directory.

**Note:** Ensure that the directory contains only the installation files.

Enter the following:

```
# chmod +x *
```

Enter the following:

```
# yum install *.rpm
```

The `yum` utility resolves any package dependencies, and displays the following prompt:

- Total size: nn G
- Installed size: nn G
- Is this ok [y/d/N]:

Enter `y`. The following and the installation status are displayed as each package is installed:

- Downloading packages:
- Running transaction check
- Running transaction test
- Transaction test succeeded
- Running transaction

The package installation is complete when the following is displayed:

```
Complete!
```

Transfer the database backup file set to the station.

**Note:** The path to the backup file set must be the same as the original backup path, which is named in the BACKUP_SUMMARY.INFO file from the backup file set; for example:

- **Backup Path Name:**
  - `/opt/5620sam/dbbackup/backupset_1`
Note: Ensure that the Oracle management user has full access to the directory and contents.

31

Enter the following:

```
# samrestoreDb path -migrate
```

where `path` is the absolute path of the database backup file set

The database restore begins, and messages like the following are displayed as the restore progresses.

```
Restore log is /opt/nsf/nfmp/db/install/NFM-P_Main_Database.restore. yyyy.mm.dd-hh.mm.ss.stdout.txt
```

<date time> working..

<date time> Performing Step 1 of 7 - Initializing ..

<date time> Executing StartupDB.sql ...

<date time> Performing Step 2 of 7 - Extracting backup files ..... 

<date time> Performing Step 3 of 7 - Restoring archive log files ..

<date time> Performing Step 4 of 7 - Executing restore.rcv ..........

<date time> Performing Step 5 of 7 - Restoring Accounting tablespaces ........

<date time> Performing Step 6 of 7 - Opening database ..... 

<date time> working....

<date time> Executing ConfigRestoreDB.sql ..................

<date time> working........

<date time> Performing Step 7 of 7 - Configuring NFM-P Server settings ...

The following is displayed when the restore is complete:

<date time> Database restore was successful

DONE

32

You must prepare the restored database for the upgrade.

Navigate to the directory that contains the OracleSw_PreInstall.sh file.

33

Enter the following:

```
# ./OracleSw_PreInstall.sh
```

Note: A default value is displayed in brackets []. To accept the default, press ↓.
Note: If you specify a value other than the default, you must record the value for use when the OracleSw_PreInstall.sh script is run during a software upgrade, or when the Oracle management user information is required by technical support.

The following prompt is displayed:

This script will prepare the system for an upgrade to NFM-P Version R.r Rn.

Do you want to continue? [Yes/No]:

Enter Yes. The following messages and prompt are displayed:

About to validate that the database can be upgraded to release.
Found the database installation directory /opt/5620sam/samdb/install.
Existing database version = version
Enter the password for the "SYS" Oracle user (terminal echo is off):

Enter the SYS user password.

The script begins to validate the database records, and displays the following:

Validating the database for upgrade. Please wait ...

If the validation is successful, the following messages and prompt are displayed:

INFO: Database upgrade validation passed.
Creating group group if it does not exist ...
Checking or Creating the Oracle user home directory /opt/5620sam/oracle12r1 ...
Checking user username... usermod: no changes
Changing ownership of the directory /opt/5620sam/oracle12r1 to username:group.
About to unlock the UNIX user [username]
Unlocking password for user username.
passwd: Success
Unlocking the UNIX user [username] completed
Do you want to change the password for the user username? [Yes/No]:

Go to Step 37.

If the database contains an invalid item, for example, an NE at a release that the new NFM-P software does not support, the following is displayed and the script exits:

ERROR: Unsupported records found in database. Please remove the following unsupported items first:
Please remove the following unsupported items first:
ERROR: The database cannot be upgraded. Please fix the above errors and re-run this script.

Perform the following steps.
1. Use an NFM-P GUI client to remove or update the unsupported items, as required. For example, upgrade an unsupported NE to a release that the new software supports.
2. Run the script again; go to Step 33.

Perform one of the following.

a. Enter No to retain the current password.
b. Specify a new password.
   1. Enter Yes. The following prompt is displayed:
      New Password:
   2. Enter a password. The following prompt is displayed:
      Re-enter new Password:
   3. Re-enter the password. The following is displayed if the password change is successful:
      passwd: password successfully changed for user

The following message and prompt are displayed:
Specify whether an NFM-P server will be installed on this workstation.
The database memory requirements will be adjusted to account for the additional load.
Will the database co-exist with an NFM-P server on this workstation [Yes/No]:

Enter Yes or No, as required.
Messages like the following are displayed as the script execution completes:
INFO: About to remove kernel parameters set by a previous run of this script from /etc/sysctl.conf
INFO: Completed removing kernel parameters set by a previous run of this script from /etc/sysctl.conf
INFO: About to set kernel parameters in /etc/sysctl.conf...
INFO: Completed setting kernel parameters in /etc/sysctl.conf...
INFO: About to change the current values of the kernel parameters
INFO: Completed changing the current values of the kernel parameters
INFO: About to remove ulimit parameters set by a previous run of this script from /etc/security/limits.conf
INFO: Completed removing ulimit parameters set by a previous run of this script from /etc/security/limits.conf
INFO: About to set ulimit parameters in etc/security/limits.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.conf...
INFO: Completed running Oracle Pre-Install Tasks

Enter the following to upgrade the database:

```
# samupgradeDb
```

The following prompt is displayed:

Enter the password for the "user" database user (terminal echo is off):

Enter the database user password.
The following is displayed as the database upgrade begins:

Validating...

<i>Note: A database upgrade may take considerable time.</i>

Verify the database configuration and create the database.

<i>Note: This main database [DB1] is the new primary main database.

1. Enter the following:

```
# samconfig -m db
```

The following is displayed:

Start processing command line inputs...

<db>

2. Enter the following:

```
<db> show-detail
```

The database configuration is displayed.

3. Review each parameter to ensure that the value is correct.

4. Configure one or more parameters, if required, and then enter <kbd>back</kbd>; see Chapter 3, “Using samconfig” for information about using the samconfig utility.
5. Enter the following to apply the configuration and create the database:
   
   ```
   <db> apply
   
   The configuration is applied, and the database creation begins.
   ```

6. When the database creation is complete, enter the following:
   
   ```
   <db> exit
   
   The samconfig utility closes.
   ```

### Upgrade standby main server [Main2]

42

If the main server [Main2] and database [DB2] are on separate stations, and you are re-using the main server station, recommission the station according to the platform specifications in this guide and in the *NSP NFM-P Planning Guide*.

![Note: After the upgrade, the station is the new primary main server station.](image)

43

Log in as the root user on the station that is commissioned as the main server [Main2] station.

44

Open a console window.

45

Enter the following:

```bash
# mkdir /opt/importConfigs
```

46

Transfer the mainserverBackupConfigs.tar.gz file created in 9.3 “To perform the pre-upgrade tasks” (p. 249) to the /opt/importConfigs directory.

47

Perform one of the following.

a. If the main server and database are collocated on one station, transfer the following downloaded installation files to the NFM-P software directory on the station:
   - nsp-nfmp-nspos-\*\*\*.rpm
   - nsp-nfmp-main-server-\*\*\*.rpm

b. If the main server and database are on separate stations, transfer the following downloaded installation files to an empty directory on the main server station:
   - nsp-nfmp-nspos-\*\*\*.rpm
   - nsp-nfmp-jre-\*\*\*rel\*.rpm
   - nsp-nfmp-config-\*\*\*rel\*.rpm
Navigate to the NFM-P software directory.

49

Enter the following:

```
# chmod +x *
```

Enter the following:

```
# yum install *.rpm
```

The `yum` utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

51

Enter `y`. The following and the installation status are displayed as each package is installed:

```
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
```

The package installation is complete when the following is displayed:

```
Complete!
```

52

When all packages are installed, perform one of the following.

**Note:** You cannot use a 5620 SAM TLS certificate or keystore in an NFM-P system.

a. If you are deploying TLS using an NSP PKI server, perform 6.7 “To configure and enable an NSP PKI server” (p. 91).

b. If you are using the manual TLS deployment method, generate and distribute the required TLS files for the system, as described in 6.11 “Workflow for manual TLS deployment” (p. 105).
Enter the following; see Chapter 3, "Using samconfig" for information about using samconfig:

```
Note: Regardless of whether you intend to modify the main server configuration, you must apply the main server configuration, as described in the following steps.

# samconfig -m main
```

The following is displayed:

```
Start processing command line inputs...
<main>
```

Enter the following:

```
<main> configure
```

The prompt changes to `<main configure>`.

To apply a new or updated NFM-P license, enter the following, and then enter `back`:

```
Note: You cannot start a main server unless the main server configuration includes a current and valid license. You can use samconfig to specify the license file in this step, or later import the license, as described in “Software and license configuration procedures” in the NSP NFM-P System Administrator Guide.

<main configure> license license_file
```

where `license_file` is the path and file name of the NSP license bundle

The prompt changes to `<main configure>`.

Configure the `tls` parameters in the following table, and then enter `back`:

```
Note: You cannot use a 5620 SAM TLS certificate or keystore in an NFM-P system.
```

Table 9-4  Standalone main server parameters — `tls`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keystore-file</td>
<td>The absolute path of the TLS keystore file</td>
</tr>
<tr>
<td></td>
<td>To enable automated TLS deployment, enter <code>no keystore-file</code>.</td>
</tr>
<tr>
<td></td>
<td>Default: /opt/nsp/os/tls/nsp.keystore</td>
</tr>
<tr>
<td>keystore-pass</td>
<td>The TLS keystore password</td>
</tr>
<tr>
<td></td>
<td>Default: available from technical support</td>
</tr>
</tbody>
</table>
Table 9-4  Standalone main server parameters — tls (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| truststore-file | The absolute path of the TLS truststore file  
To enable automated TLS deployment, enter no truststore-file.  
Default: /opt/nsp/os/tls/nsp.truststore |
| truststore-pass | The TLS truststore password  
Default: available from technical support |
| alias | The alias specified during keystore generation  
You must configure the parameter.  
Default: — |
| pki-server | If you are using the automated TLS deployment method, the IP address or hostname of the PKI server  
You must configure the parameter if no keystore-file value is specified.  
Default: — |
| pki-server-port | If you are using the automated TLS deployment method, the TCP port on which the PKI server listens for and services requests  
Default: 2391 |
| webdav | Whether WebDAV access to eNodeB activation data is enabled on the main server  
Default: false |

Verify the main server configuration.

1. Enter the following:
   `<main configure> show`  
The main server configuration is displayed.

2. Review each parameter to ensure that the value is correct.

3. Configure one or more parameters, if required; see Chapter 3, “Using samconfig” for information about using the samconfig utility.

4. When you are certain that the configuration is correct, enter the following:
   `<main configure> back`  
The prompt changes to `<main>`.

Enter the following:

`<main> apply`  
The configuration is applied.
Enter the following:

```
<main> exit
```

The samconfig utility closes.

**Restore main server [Main2] data files**

Transfer the nebackup_timestamp.tar.gz file created in Step 18 of 9.3 “To perform the pre-upgrade tasks” (p. 249) to the /opt/nsp/nfmp/nebackup directory on the main server station.

**Note:** Ensure that you transfer the file created for the original standby main server [Main2] station.

Enter the following:

```
# cd /opt/nsp/nfmp/nebackup
```

Enter the following:

```
# chown nsp:nsp *.tar.gz
```

Enter the following:

```
# tar -xf nebackup_timestamp.tar.gz -C /opt/nsp/nfmp/
```

where `timestamp` is a backup timestamp in the format `MM-DD-hh-mm`

The main server nebackup data files are restored to the /opt/nsp/nfmp/nebackup directory.

After the backup file is restored, the backup file is no longer required, and may consume a large amount of disk space. To remove the backup file, enter the following:

```
# rm -f nebackup_*.tar.gz
```

Transfer the remaining files in the backup file set created in Step 18 of 9.3 “To perform the pre-upgrade tasks” (p. 249) to the /opt/nsp/nfmp directory on the main server station.

**Note:** Ensure that you transfer the files created for the original standby main server [Main2] station.

Enter the following:
Enter the following:

```bash
# chown nsp:nsp *.tar.gz
```

Enter the following commands:

```bash
# tar -xf lte_timestamp.tar.gz -C /opt/nsp/nfmp/
# tar -xf nelogs_timestamp.tar.gz -C /opt/nsp/nfmp/
# tar -xf nesoftware_timestamp.tar.gz -C /opt/nsp/nfmp/
# tar -xf os_timestamp.tar.gz -C /opt/nsp/nfmp/
# tar -xf savedResults_timestamp.tar.gz -C /opt/nsp/nfmp/
```

where `timestamp` is a backup timestamp in the format `MM-DD-hh-mm`

The remaining main server data files are restored to the appropriate directories.

The backup files are no longer required. To remove a backup file, enter the following:

```bash
# rm -f filename.tar.gz
```

where `filename` is the name of a backup file

Enter the following:

```bash
# chown -R nsp:nsp lte
```

Enter the following:

```bash
# chown -R nsp:nsp nebackup
```

Enter the following:

```bash
# chown -R nsp:nsp nelogs
```

Enter the following:

```bash
# chown -R nsp:nsp nesoftware
```

Enter the following:

```bash
# chown -R nsp:nsp os
```
Enter the following:

`# chown -R nsp:nsp server/script/savedResults`

**Stop analytics servers, Cflowd auxiliary servers**

If the NFM-P system includes one or more analytics servers, stop each analytics server.

1. Log in to the analytics server station as the samadmin user.
2. Open a console window.
3. Enter the following:

   ```bash
   /opt/5620sam/analytics/bin/AnalyticsAdmin.sh stop
   ```

   The following is displayed:

   ```
   Stopping 5620 SAM Analytics Server
   ```

   When the analytics server is completely stopped, the following message is displayed:

   ```
   5620 SAM Analytics Server is not running
   ```

If the system includes one or more Cflowd auxiliary servers, stop each Cflowd auxiliary server.

1. Log in to the Cflowd auxiliary server station as the root user.
2. Open a console window.
3. Navigate to the Cflowd auxiliary server installation directory, which is one of the following:
   - Release 14.0 R5 or earlier—/opt/5620sam/dcp-R_Rn, where R_Rn is the software release identifier
   - Release 14.0 R6 or later—/opt/5620sam/dcp
4. Enter the following:

   ```bash
   ./bin/dcpctl.sh stop
   ```

   Output like the following is displayed.

   ```
   Stopping 5620 SAM Cflowd Auxiliary Server ... 5620 SAM Cflowd Auxiliary Server is stopped successfully
   ```

**Upgrade auxiliary servers [Aux2]**

If the system includes auxiliary servers, perform 9.9 "To upgrade a 5620 SAM auxiliary server" (p. 329) on each appropriate auxiliary server station [Aux2].

**Note:** Do not start any auxiliary server immediately after you upgrade the auxiliary server; the startup occurs later in the procedure.
Stop and disable original primary main server [Main1]

Stop the original primary main server.

Note: This step marks the beginning of the network management outage.

1. Log in to the original primary main server station [Main1] as the samadmin user.
2. Open a console window.
3. Enter the following:
   ```bash
   cd /opt/5620sam/server/nms/bin
   ```
4. Enter the following:
   ```bash
   ./nmsserver.bash stop
   ```
5. Enter the following:
   ```bash
   ./nmsserver.bash appserver_status
   ```
   The server status is displayed; the server is fully stopped if the status is the following:
   
   Application Server is stopped

   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

Disable the automatic main server startup so that the main server does not start in the event of a power disruption during the upgrade.

1. Enter the following to switch to the root user:
   ```bash
   su -
   ```
2. Enter the following:
   ```bash
   cd /etc/init.d
   ```
3. Enter the following to rename the main server startup daemon:
   ```bash
   mv 5620SAMServerWrapper inactive.5620SAMServerWrapper
   ```

Upgrade Cflowd auxiliary servers

If the system includes one or more Cflowd auxiliary servers, perform 9.10 “To upgrade a 5620 SAM Cflowd auxiliary server” (p. 335) on each Cflowd auxiliary server station.

Stop auxiliary servers [Aux1]

If the system includes auxiliary servers, perform the following steps on each [Aux1] auxiliary server station.
1. Log in to the auxiliary server station as the samadmin user.
2. Open a console window.
3. Enter the following:
   ```bash
   /opt/5620sam/auxserver/nms/bin/auxnmsserver.bash auxstop
   ``
   The auxiliary server stops.

Upgrade auxiliary database

If the system includes an auxiliary database, perform 9.11 “To upgrade a 5620 SAM auxiliary database” (p. 340).

Stop original primary main database [DB1]

Stop the original primary main database and proxy services.
1. Log in to the original primary main database station as the root user.
2. Open a console window.
3. Enter the following:
   ```bash
   cd /etc/rc3.d
   ``
4. Enter the following to stop the Oracle proxy:
   ```bash
   ./S965620SAMOracleProxyWrapper stop
   ``
5. Enter the following to stop the database:
   ```bash
   ./S95db5620sam stop
   ``

Disable the automatic database proxy startup.
1. Enter the following:
   ```bash
   cd /etc/init.d
   ``
2. Enter the following:
   ```bash
   mv 5620SAMOracleProxyWrapper inactive.5620SAMOracleProxyWrapper
   ```
Start new primary main server [Main2]

CAUTION

Service Disruption

The new primary database [DB2] must be upgraded and running before you start the new primary main server [Main2], or the main server initialization may fail.

If you perform the new primary main server and database upgrades concurrently, do not perform this step until the database upgrade is complete.

CAUTION

Service Disruption

An NFM-P system upgrade is not complete until each main server performs crucial post-upgrade tasks during initialization.

Before you attempt an operation that requires a server shutdown, you must ensure that each main server is completely initialized, or the operation fails.

Start the new primary main server [Main2].

Note: You cannot start a main server unless the main server configuration includes a current and valid license. You can use samconfig to specify the license file, or import a license, as described in "Software and license configuration procedures" in the NSP NFM-P System Administrator Guide.

1. Log in as the nsp user on the new primary main server station [Main2]:
2. Enter the following:
   ```bash
   cd /opt/nsp/nfmp/server/nms/bin
   ```
3. Enter the following:
   ```bash
   ./nmsserver.bash start
   ```
4. Enter the following:
   ```bash
   ./nmsserver.bash appserver_status
   ```
   The server status is displayed; the server is fully initialized if the status is the following:
   
   Application Server process is running. See nms_status for more detail.

   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

Note: This marks the end of the network management outage.
If the NFM-P is to manage wireless NEs, enter the following to update the memory configuration accordingly for GUI clients:

```
bash$ ./nmsdeploytool.bash clientmem -l
```

### Start auxiliary servers [Aux2]

If the NFM-P system includes auxiliary servers, start each appropriate auxiliary server [Aux2].

1. Log in to the auxiliary server station as the nsp user.
2. Open a console window.
3. Enter the following:
   ```bash
   bash$ cd /opt/nsp/nfmp/auxserver/nms/bin
   ```
4. Enter the following:
   ```bash
   bash$ ./auxnmsserver.bash auxstart
   ```
   The auxiliary server starts.

### Upgrade analytics servers

If the system includes one or more analytics servers, perform [9.12 “To upgrade the 5620 SAM analytics servers” (p. 351)] on each analytics server station.

### Enable GUI client

Perform one of the following to enable a GUI client for system testing:

- [14.4 “To install a single-user GUI client” (p. 564)]
- [14.5 “To upgrade an NFM-P Release 17 or 5620 SAM single-user GUI client” (p. 569)]
- [15.3 “To install a client delegate server” (p. 584)]
- [15.5 “To upgrade an NFM-P Release 17 or 5620 SAM client delegate server” (p. 596)]

### Test upgraded system using GUI client

When the new primary main server [Main2] is started, use a newly installed or upgraded GUI client to perform sanity testing of the new primary main server and database.
Note: To back out of the upgrade and return the original primary main server [Main1] and database [DB1] to service, you can do so by stopping the new primary main server [Main2] and database [DB2] and restarting the original primary main server [Main1] and database [DB1].

Install new standby main database [DB1]

92

If you are re-using the primary main database [DB1] station, recommission the station according to the platform specifications in this guide and in the NSP NFM-P Planning Guide.

Note: After the upgrade, the station is the new standby main database station.

93

Log in as the root user on the station that is commissioned as the main database [DB1] station.

94

Transfer the following downloaded files to an empty directory on the station:
- nsp-nfmp-jre-R.r.p-rel.v.rpm
- nsp-nfmp-config-R.r.p-rel.v.rpm
- nsp-nfmp-oracle-R.r.p-rel.v.rpm
- nsp-nfmp-main-db-R.r.p-rel.v.rpm

Note: In subsequent steps, the directory is called the NFM-P software directory.

95

Transfer the following downloaded file to an empty directory on the station:
- OracleSw_PreInstall.sh

96

Open a console window.

97

You must prepare the station for the Oracle software installation. Navigate to the directory that contains the OracleSw_PreInstall.sh file.

98

Enter the following:

```
# chmod +x OracleSw_PreInstall.sh
```

99

Enter the following:
Note: A default value is displayed in brackets []. To accept the default, press \.

Note: If you specify a value other than the default, you must record the value for use when the OracleSw_PreInstall.sh script is run during a software upgrade, or when the Oracle management user information is required by technical support.

The following prompt is displayed:

This script will prepare the system for a new install/restore of an NFM-P Version Release main database.

Do you want to continue? [Yes/No]:

Enter Yes. The following prompt is displayed:

Enter the Oracle dba group name [group]:

Enter a group name.

Note: To reduce the complexity of subsequent software upgrades and technical support activities, it is recommended that you accept the default.

The following messages and prompt are displayed:

Creating group group if it does not exist...
done

Enter the Oracle user name:

Enter a username.

Note: To reduce the complexity of subsequent software upgrades and technical support activities, it is recommended that you accept the default.

The following messages and prompt are displayed:

Oracle user [username] new home directory will be [/opt/nsp/nfmp/oracle12r1].
Checking or Creating the Oracle user home directory /opt/nsp/nfmp/oracle12r1...,
Checking user username...
Adding username...
Changing ownership of the directory /opt/nsp/nfmp/oracle12r1 to username:group.
About to unlock the UNIX user [username]
Unlocking password for user username.
passwd: Success
Unlocking the UNIX user [username] completed
Please assign a password to the UNIX user username..
New Password:

Enter a password. The following prompt is displayed:
Re-enter new Password:

Re-enter the password. The following is displayed if the password change is successful:
passwd: password successfully changed for username
The following message and prompt are displayed:
Specify whether an NFM-P Main Server will be installed on this workstation.
The database memory requirements will be adjusted to account for the additional load.
Will the database co-exist with an NFM-P Main Server on this workstation [Yes/No]:

Enter Yes or No, as required.
Messages like the following are displayed as the script execution completes:
INFO: About to set kernel parameters in /etc/sysctl.conf...
INFO: Completed setting kernel parameters in /etc/sysctl.conf...
INFO: About to change the current values of the kernel parameters
INFO: Completed changing the current values of the kernel parameters
INFO: About to set ulimit parameters in /etc/security/limits.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.conf...
INFO: Completed running Oracle Pre-Install Tasks, you *MUST* reboot your box.

When the script execution is complete, enter the following to reboot the station:
# systemctl reboot
The station reboots.

When the reboot is complete, log in as the root user on the main database [DB1] station.
Open a console window.

Navigate to the NFM-P software directory.

**Note:** Ensure that the directory contains only the installation files.

Enter the following:
```
# chmod +x *
```

Enter the following:
```
# yum install *.rpm
```

The `yum` utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
```

The package installation is complete when the following is displayed:

```
Complete!
```

Configure the database as a standby database.

1. Enter the following:
   ```
   # samconfig -m db
   ```

   The following is displayed:
   ```
   Start processing command line inputs...
   <db>
   ```

2. Enter the following:
   ```
   <db> configure type standby
   ```
The prompt changes to <db configure>.

3. Enter the following:
   
   `<db configure> ip address`  
   where address is the IP address of this database

4. Enter the following:
   
   `<db configure> redundant ip address`  
   where address is the IP address of the new primary database [DB2]
   
   The prompt changes to `<db configure redundant>.

5. Enter the following:
   
   `<db configure redundant> instance instance_name`  
   where instance_name is the instance name of the new primary database [DB2]

6. Enter the following:
   
   `<db configure redundant> back`  
   The prompt changes to `<db configure>.

7. Enter the following:
   
   `<db configure> passwords sys password`  
   where password is the database SYS user password
   
   The prompt changes to `<db configure passwords>.

8. Enter the following:
   
   `<db configure passwords> back`  
   The prompt changes to `<db configure>.

114

Verify the database configuration.

1. Enter the following:
   
   `<db configure> show-detail`  
   The database configuration is displayed.

2. Review each parameter to ensure that the value is correct.

3. Configure one or more parameters, if required; see Chapter 3, “Using samconfig” for information about using the samconfig utility.

4. When you are certain that the configuration is correct, enter the following:
   
   `<db configure> back`  
   The prompt changes to `<db>.

115

Enter the following to apply the configuration and begin the database creation:

   `<db> apply`  
   The database creation begins, and progress messages are displayed.
The following is displayed when the database creation is complete:

DONE
db configurations updated.

When the database creation is complete, enter the following:

<db> exit

The samconfig utility closes.

Reinstantiate standby database

Log in to an NFM-P GUI client as the admin user.

Choose Administration→System Information from the main menu. The System Information form opens.

Click Re-Instantiate Standby.

Click Yes to confirm the action. The reinstatement begins, and the GUI status bar displays reinstatement information.

Note: Database reinstatement takes considerable time if the database contains a large amount of statistics data.

You can also use the System Information form to monitor the reinstatement progress. The Last Attempted Standby Re-instantiation Time is the start time; the Standby Re-instantiation State changes from In Progress to Success when the reinstatement is complete.

When the reinstatement is complete, close the System Information form.

Upgrade original primary main server [Main1]

If the main server [Main1] and database [DB1] are on separate stations, and you are re-using the main server station, recommission the station according to the platform specifications in this guide and in the *NSP NFM-P Planning Guide*.

Note: After the upgrade, the station is the new standby main server station.
Log in as the root user on the station that is commissioned as the main server [Main1] station.

Open a console window.

Enter the following:
```
# mkdir /opt/importConfigs
```

Transfer the main server BackupConfigs.tar.gz file created in 9.3 “To perform the pre-upgrade tasks” (p. 249) to the /opt/importConfigs directory.

Perform one of the following.

a. If the main server and database are collocated on one station, transfer the following downloaded installation files to the NFM-P software directory on the station:
   - nsp-nfmp-npos-R.r.p.rpm
   - nsp-nfmp-main-server-R.r.p.rpm

b. If the main server and database are on separate stations, transfer the following downloaded installation files to an empty directory on the main server station:
   - nsp-nfmp-npos-R.r.p.rpm
   - nsp-nfmp-jre-R.r.p-rel.v.rpm
   - nsp-nfmp-config-R.r.p-rel.v.rpm
   - nsp-nfmp-main-server-R.r.p.rpm

> **Note:** In subsequent steps, the directory is called the NFM-P software directory.

Navigate to the NFM-P software directory.

> **Note:** Ensure that the directory contains only the installation files.

Enter the following:
```
# chmod +x *
```

Enter the following:
```
# yum install *.rpm
```
The yum utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

131

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
The package installation is complete when the following is displayed:
Complete!
```

132

When all packages are installed, enter the following; see Chapter 3, “Using samconfig” for information about using samconfig:

```
Note: Regardless of whether you intend to modify the main server configuration, you must apply the main server configuration, as described in the following steps.

# samconfig -m main
```

The following is displayed:

```
Start processing command line inputs...
<main>
```

133

Enter the following:

```
<main> configure
```

The prompt changes to `<main configure>`.

134

To apply a new or updated NFM-P license, enter the following, and then enter `back`:

```
Note: You cannot start a main server unless the main server configuration includes a current and valid license. You can use samconfig to specify the license file in this step, or later import the license, as described in “Software and license configuration procedures” in the NSP NFM-P System Administrator Guide.

<main configure> license license_file
```

where `license_file` is the path and file name of the NSP license bundle.
Configure the **tls** parameters in the following table, and then enter **back**.

**Note:** You cannot use a 5620 SAM TLS certificate or keystore in an NFM-P system.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keystore-file</td>
<td>The absolute path of the TLS keystore file. To enable automated TLS deployment, enter no <strong>keystore-file</strong>. Default: /opt/nsp/os/tls/nsp.keystore</td>
</tr>
<tr>
<td>keystore-pass</td>
<td>The TLS keystore password. Default: available from technical support</td>
</tr>
<tr>
<td>truststore-file</td>
<td>The absolute path of the TLS truststore file. To enable automated TLS deployment, enter no <strong>truststore-file</strong>. Default: /opt/nsp/os/tls/nsp.truststore</td>
</tr>
<tr>
<td>truststore-pass</td>
<td>The TLS truststore password. Default: available from technical support</td>
</tr>
<tr>
<td>alias</td>
<td>The alias specified during keystore generation. You must configure the parameter. Default: —</td>
</tr>
<tr>
<td>pki-server</td>
<td>If you are using the automated TLS deployment method, the IP address or hostname of the PKI server. You must configure the parameter if no keystore-file value is specified. Default: —</td>
</tr>
<tr>
<td>pki-server-port</td>
<td>If you are using the automated TLS deployment method, the TCP port on which the PKI server listens for and services requests Default: 2391</td>
</tr>
<tr>
<td>webdav</td>
<td>Whether WebDAV access to eNodeB activation data is enabled on the main server. Default: false</td>
</tr>
</tbody>
</table>

Verify the main server configuration.

1. Enter the following:
   
   `<main configure> show`  
   
   The main server configuration is displayed.

2. Review each parameter to ensure that the value is correct.
3. Configure one or more parameters, if required; see Chapter 3, “Using samconfig” for information about using the samconfig utility.

4. When you are certain that the configuration is correct, enter the following:

```bash
<main configure> back
```

The prompt changes to `<main>`.

137

Enter the following:

```bash
<main> apply
```

The configuration is applied.

138

Enter the following:

```bash
<main> exit
```

The samconfig utility closes.

**Note:** This station is the new standby main server station.

**Restore main server [Main1] data files**

139

Transfer the `nebackup_timestamp.tar.gz` file created in Step 18 of 9.3 “To perform the pre-upgrade tasks” (p. 249) to the `/opt/nsp/nfmp/nebackup` directory on the main server station.

**Note:** Ensure that you transfer the file created for the original primary main server [Main1] station.

140

Enter the following:

```bash
# cd /opt/nsp/nfmp/nebackup
```

141

Enter the following:

```bash
# chown nsp:nsp *.tar.gz
```

142

Enter the following:

```bash
# tar -xf nebackup_timestamp.tar.gz -C /opt/nsp/nfmp/ where timestamp is a backup timestamp in the format MM-DD-hh-mm
```

The main server nebackup data files are restored to the `/opt/nsp/nfmp/nebackup` directory.
After the backup file is restored, the backup file is no longer required, and may consume a large amount of disk space. To remove the backup file, enter the following:

```
# rm -f nebackup_*.tar.gz
```

Transfer the remaining files in the backup file set created in Step 18 of 9.3 “To perform the pre-upgrade tasks” (p. 249) to the /opt/nsp/nfmp directory on the main server station.

**Note:** Ensure that you transfer the files created for the original primary main server [Main1] station.

Enter the following:

```
# cd /opt/nsp/nfmp
```

Enter the following:

```
# chown nsp:nsp *.tar.gz
```

Enter the following commands:

```
# tar -xf lte_timestamp.tar.gz -C /opt/nsp/nfmp/ 
# tar -xf nelogs_timestamp.tar.gz -C /opt/nsp/nfmp/ 
# tar -xf nesoftware_timestamp.tar.gz -C /opt/nsp/nfmp/ 
# tar -xf os_timestamp.tar.gz -C /opt/nsp/nfmp/ 
# tar -xf savedResults_timestamp.tar.gz -C /opt/nsp/nfmp/ 
```

where `timestamp` is a backup timestamp in the format `MM-DD-hh-mm`

The remaining main server data files are restored to the appropriate directories.

The backup files are no longer required. To remove a backup file, enter the following:

```
# rm -f filename.tar.gz
```

where `filename` is the name of a backup file

Enter the following:

```
# chown -R nsp:nsp lte
```

Enter the following:
Start new standby main server

Start the new standby main server [Main1].

Note: You cannot start a main server unless the main server configuration includes a current and valid license. You can use samconfig to specify the license file, or import a license, as described in “Software and license configuration procedures” in the NSP NFM-P System Administrator Guide.

1. Enter the following to switch to the nsp user:
   ```bash
   # su - nsp
   ```
2. Open a console window.
3. Enter the following:
   ```bash
   bash$ cd /opt/nsp/nfmp/server/nms/bin
   ```
4. Enter the following:
   ```bash
   bash$ ./nmsserver.bash start
   ```
5. Enter the following:
   ```bash
   bash$ ./nmsserver.bash appserver_status
   ```
   The server status is displayed; the server is fully initialized if the status is the following:
   Application Server process is running. See nms_status for more detail.
   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.
If the NFM-P is to manage wireless NEs, enter the following to update the memory configuration accordingly for GUI clients:

```
bash$ ./nmsdeploytool.bash clientmem -l
```

Close the console window.

**Upgrade auxiliary servers [Aux1]**

If the system includes auxiliary servers, perform 9.9 “To upgrade a 5620 SAM auxiliary server” (p. 329) on each [Aux1] auxiliary server station.

**Start auxiliary servers [Aux1]**

If the system includes auxiliary servers, perform the following steps on each [Aux1] auxiliary server station.

1. Log in to the auxiliary server station as the nsps user.
2. Open a console window.
3. Enter the following:

```
bash$ /opt/nsps/nfmp/auxserver/nms/bin/auxnmsserver.bash auxstart
```

The auxiliary server starts.

**Install or upgrade single-user GUI clients**

As required, perform the following to install or upgrade single-user GUI clients:

- 14.4 “To install a single-user GUI client” (p. 564)
- 14.5 “To upgrade an NFM-P Release 17 or 5620 SAM single-user GUI client” (p. 569)

**Install or upgrade client delegate servers**

As required, perform the following to install or upgrade client delegate servers:

- 15.3 “To install a client delegate server” (p. 584)
- 15.5 “To upgrade an NFM-P Release 17 or 5620 SAM client delegate server” (p. 596)
Stop PKI server

If you are deploying TLS using an NSP PKI server, stop the PKI server, as described at the end of 6.7 “To configure and enable an NSP PKI server” (p. 91).

Restore TLS version and cipher support configuration

A 5620 SAM system upgrade to the NFM-P does not preserve your changes to the system support for specific TLS versions and ciphers.

If the 5620 SAM system had customized TLS settings before the upgrade, perform “To update the supported NFM-P TLS versions and ciphers” in the NSP NFM-P System Administrator Guide to restore the settings on the NFM-P system.

Perform 9500 MPR migration post-upgrade tasks

If you are upgrading a Release 14.0 R6 or earlier 5620 SAM system that manages one or more 9500 MPR devices, perform “To perform post-upgrade tasks” in the NSP NFM-P Wavence User Guide.

Note: The 9500 MPR is renamed Wavence in Release 18.0; the device name shown in the NFM-P client GUI may vary, depending on the device release.

Configure and enable firewalls

If you intend to use any firewalls between the NFM-P components, and the firewalls are disabled, configure and enable each firewall.

Perform one of the following.

a. Configure each external firewall to allow the required traffic using the port assignments in the NSP NFM-P Planning Guide, and enable the firewall.

b. Configure and enable Firewalld on each component station, as required.
   1. Use an NFM-P template to create the Firewalld rules for the component, as described in the NSP NFM-P Planning Guide.
   2. Log in to the station as the root user.
   3. Open a console window.
   4. Enter the following:
      ```
      # systemctl enable firewalld
      ```
   5. Enter the following:
      ```
      # systemctl start firewalld
      ```
6. Close the console window.
5620 SAM auxiliary server upgrade

9.9 To upgrade a 5620 SAM auxiliary server

9.9.1 Description

The following steps describe how to upgrade an auxiliary server from a 5620 SAM release to the NFM-P. Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

**Note:** An auxiliary server is dedicated to only one of the following functions:
- statistics collection
- call-trace data collection
- PCMD record collection

**Note:** You require the following user privileges on the auxiliary server station:
- root
- samadmin

**Note:** The upgrade creates the nsp user on the auxiliary server station.

**Note:** The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:
- # — root user
- bash$ — nsp and samadmin users

9.9.2 Steps

**Commission new station, if required**

1

If you are deploying the auxiliary server on a new station, commission the station according to the platform specifications in this guide and in the *NSP NFM-P Planning Guide*.

**Back up configuration**

2

Download the following NFM-P installation file to an empty local directory on the auxiliary server station:
- linuxMigration.sh

3

Navigate to the directory that contains the downloaded file.
Enter the following:

```
# chmod +x linuxMigration.sh
```

Enter the following:

```
# ./linuxMigration.sh -t aux
```

The following prompt is displayed:

Please specify a target directory for the backups (default is /opt/importConfigs):

Enter the absolute path of a target directory for the backup files, or press \( \downarrow \) to accept the default.

**Note:** The directory must exist, and the directory name must not contain a space character.

If the directory does not have sufficient capacity for the backup files, you are prompted to enter a different directory name. Otherwise, the following is displayed and the backup begins:

Backup auxiliary server config contents.

When the backup is complete, the following is displayed:

Please backup/transfer backup_dir/importConfigs/auxserverBackupConfigs.tar.gz to a secure location. You must restore this file to the /opt/importConfigs directory on the RHEL 7 station before installing the rpm(s).

The script creates the following file on the station:

- `backup_dir/importConfigs/auxserverBackupConfigs.tar.gz`

  where `backup_dir` is the specified backup directory

Transfer the auxserverBackupConfigs.tar.gz file to a secure location on a separate station for use later in the procedure.

**Note:** If the system has multiple auxiliary servers, you must ensure that you record which server the file is from.

**Decommission existing station**

Stop the auxiliary server.

1. Enter the following to switch to the samadmin user:

   ```
   # su - samadmin
   ```

2. Enter the following:
Enter the following:

```
bash$ cd /opt/5620sam/auxserver/nms/bin
```

3. Enter the following:

```
bash$ ./auxnmsserver.bash auxstop
```

4. Enter the following:

```
bash$ ./auxnmsserver.bash auxappserver_status
```

The auxiliary server is stopped when the following message is displayed:

```
Auxiliary Server is stopped
```

If the command output indicates that the server is not completely stopped, wait five minutes and then re-enter the command in this step to check the server status.

Do not proceed to the next step until the server is completely stopped.

Enter the following to switch back to the root user:

```
# exit
```

Enter the following commands in sequence to remove the NFM-P packages:

```
# yum remove nsp-nfmp-aux-server
# yum remove nsp-nfmp-config
# yum remove nsp-nfmp-jre
```

After you enter a command, the `yum` utility resolves any dependencies and displays the following prompt:

```
Installed size: nn G
Is this ok [y/N]:
```

Enter `y`. The following is displayed:

```
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Uninstalling the NFM-P package...
```

As each package removal completes, the following is displayed:

```
Complete!
```

Return to Step 10 as required to remove the next package in the sequence.
Recommission existing station, if required

13

If you are re-using the auxiliary server station, recommission the station according to the platform specifications in this guide and in the *NSP NFM-P Planning Guide*.

Install auxiliary server software

14

Log in as the root user on the station that is commissioned as the auxiliary server station.

15

Enter the following:

```
# mkdir /opt/importConfigs
```

16

Transfer the auxserverBackupConfigs.tar.gz file created in Step 6 to the /opt/importConfigs directory.

17

Download the following NFM-P installation files to an empty local directory:

- `nsp-nfmp-jre-R.r.p-rel.v.rpm`
- `nsp-nfmp-config-R.r.p-rel.v.rpm`
- `nsp-nfmp-aux-server-R.r.p-rel.v.rpm`

where

- `R.r.p` is the NSP release identifier, in the form `MAJOR.minor.patch`
- `v` is a version identifier

18

Navigate to the directory that contains the NFM-P installation files.

**Note:** Ensure that the directory contains only the installation files.

19

Enter the following:

```
# chmod +x *
```

20

Enter the following:

```
# yum install *.rpm
```

The yum utility resolves any package dependencies, and displays the following prompt:
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:

Enter y. The following and the installation status are displayed as each package is installed:
   downloading packages:
   running transaction check
   running transaction test
   transaction test succeeded
   running transaction
   the package installation is complete when the following is displayed:
   complete!

Enter the following:
   # samconfig -m aux

The following is displayed:
   start processing command line inputs...
   <aux>

Verify the auxiliary server configuration.
1. Enter the following:
   <aux> show-detail
   the auxiliary server configuration is displayed.
2. Review each parameter to ensure that the value is correct.
3. If required, modify one or more parameter values, and then enter back; see Chapter 3, “Using samconfig” for information about using the samconfig utility.
4. When you are certain that the configuration is correct, enter the following:
   <aux> apply
   the configuration is applied.
5. Enter the following:
   <aux> exit
   the samconfig utility closes.

Start the auxiliary server, unless otherwise directed in a system upgrade procedure.
1. Log in to the auxiliary server station as the nsp user.
2. Open a console window.

3. Enter the following:

   bash$ /opt/nsf/nfmp/auxserver/nms/bin/auxnmsserver.bash auxstart

   The auxiliary server starts.

END OF STEPS
5620 SAM Cflowd auxiliary server upgrade

9.10 To upgrade a 5620 SAM Cflowd auxiliary server

9.10.1 Description

The following steps describe how to upgrade a 5620 SAM Cflowd auxiliary server, which is called an NSP Flow Collector after the upgrade. Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

Note: After the upgrade, you must clear the cache of each browser that you use to configure the NSP Flow Collector, or the configuration web UI may not display correctly.

Note: You require root user privileges on the Cflowd auxiliary server station.

Note: The upgrade creates the nsp user on the NSP Flow Collector station.

Note: A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

9.10.2 Steps

Commission new station, if required

1

If you are deploying the NSP Flow Collector on a new station, commission the station according to the platform specifications in this guide and in the NSP NFM-P Planning Guide.

Stop Cflowd auxiliary server

2

Log in to the Cflowd auxiliary server station as the root user.

3

Open a console window.

4

Navigate to the 5620 SAM installation directory, which is one of the following:

- Release 14.0 R5 or earlier—/opt/5620sam/dcp-R_rRn, where R_rRn is the software release identifier
- Release 14.0 R6 or later—/opt/5620sam/dcp

5

Enter the following:
# /bin/dcpctl.sh stop

A message like the following is displayed:
Stopping 5620 SAM DCP server...
The Cflowd auxiliary server is stopped when a message like the following is displayed:
5620 SAM DCP server is stopped successfully

Back up Cflowd auxiliary server configuration

6

Download the following NFM-P installation file to an empty local directory on the Cflowd auxiliary server station:
• linuxMigration.sh

7

Navigate to the directory that contains the downloaded file.

8

Enter the following:
# chmod +x linuxMigration.sh

9

Enter the following:
# ./linuxMigration.sh -t flow

The following prompt is displayed:
Please specify a target directory for the backups (default is /opt/importConfigs):

10

Enter the absolute path of a target directory for the backup files, or press \(\downarrow\) to accept the default.

Note: The directory must exist, and the directory name must not contain a space character.
If the directory does not have sufficient capacity for the backup files, you are prompted to enter a different directory name. Otherwise, the following is displayed and the backup begins:
Backup Flow Collector config contents.

When the backup is complete, the following is displayed:
Please backup/transfer backup dir/importConfigs/flowCollectorBackupConfigs.tar.gz to a secure location.

You must restore this file to the /opt/importConfigs directory on the RHEL 7 station before installing the rpm(s).
The script creates the following file on the station:

- `backup_dir/importConfigs/flowCollectorBackupConfigs.tar.gz`

where `backup_dir` is the specified backup directory

Transfer the `flowCollectorBackupConfigs.tar.gz` file to a secure location on a separate station for use later in the procedure.

**Note:** If the system has multiple Cflowd auxiliary servers, you must ensure that you record which server the file is from.

Stop the Cflowd auxiliary server.

1. Navigate to the Cflowd auxiliary server installation directory, which is one of the following:
   - Release 14.0 R5 or earlier—`/opt/5620sam/dcp-R_rRn`, where `R_rRn` is the software release identifier
   - Release 14.0 R6 or later—`/opt/5620sam/dcp`
2. Enter the following:
   ```
   # ./dcpctl.sh stop
   ```
   A message like the following is displayed:
   ```
   Stopping 5620 SAM DCP server...
   ```
   The Cflowd auxiliary server is stopped when a message like the following is displayed:
   ```
   5620 SAM DCP server is stopped successfully
   ```

**Note:** Do not perform the next step until the Cflowd auxiliary server is stopped.

Recommission existing station, if required

If you are re-using the Cflowd auxiliary server station, recommission the station according to the platform specifications in this guide and in the *NSP NFM-P Planning Guide*.

Install NSP Flow Collector

Log in as the root user on the station that is commissioned as the NSP Flow Collector station.

Enter the following:

```
# mkdir /opt/importConfigs
```
16 Transfer the flowCollectorBackupConfigs.tar.gz file created in Step 9 to the /opt/importConfigs directory.

17 Download the following NFM-P installation files to an empty local directory:
   • nsp-nfmp-jre-R.r.p-rel.v.rpm
   • nsp-nfmp-config-R.r.p-rel.v.rpm
   • nsp-flow-collector-R.r.p-rel.v.rpm
   where
   R.r.p is the NSP release identifier, in the form MAJOR.minor.patch
   v is a version identifier

18 Navigate to the directory that contains the installation files.

   **Note:** Ensure that the directory contains only the installation files.

19 Enter the following:
   ```bash
   # chmod +x *
   ```

20 Enter the following:
   ```bash
   # yum install *.rpm
   ```
   The `yum` utility resolves any package dependencies, and displays the following prompt:
   Total size: nnn M
   Installed size: nn M
   Is this ok [y/d/N]?

21 Enter y. The following and the installation status are displayed as each package is installed:
   Downloading packages:
   Running transaction check
   Running transaction test
   Transaction test succeeded
   Running transaction
   The package installation is complete when the following is displayed:
   Complete!
Start the NSP Flow Collector; enter the following:

```bash
# /opt/nsp/flow/dcp/bin/dcpctl.sh start
dcpctl.sh start
```

The command displays a series of status messages as the NSP Flow Collector starts.

**Note:** To start the NSP Flow Collector without displaying status messages, you can use the following command:

```bash
# systemctl start nsp-flow-collector.service
dsystemctl start nsp-flow-collector.service
```

Close the console window.

**END OF STEPS**
5620 SAM auxiliary database upgrade

9.11 To upgrade a 5620 SAM auxiliary database

9.11.1 Description

The following steps describe how to upgrade a 5620 SAM auxiliary database to an NFM-P auxiliary database. Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

Note: CPU speed scaling, or CPufreq, must be set to “performance” in the BIOS of each auxiliary database station, or the auxiliary database upgrade fails. See the RHEL power management documentation for information about enabling the “performance” CPufreq governor on a station.

Setting CPufreq to “performance” effectively disables CPU speed scaling, so may result in greater energy consumption by a station.

Note: An auxiliary database upgrade from Release 14.0 R4 or earlier removes some current values, such as for performance statistics or OAM data. As a result, the periodic counter values for the first collection after an upgrade are inaccurate.

Note: You require root user privileges on each auxiliary database station.

Note: A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

9.11.2 Steps

Commission new stations, if required

1

If you are deploying the auxiliary database on one or more new stations, commission each station according to the platform specifications in this guide and in the NSP NFM-P Planning Guide.

Note: The IP address of a new auxiliary database station must match the IP address of the station that it replaces.
Back up database

2

CAUTION

Data Loss

If you specify a backup location on the database data partition, data loss or corruption may occur.

The auxiliary database backup location must be an absolute path on a partition other than the database data partition.

Back up the auxiliary database.

Note: The backup location requires 20% more space than the database data consumes.

Note: If the backup location is remote, a 10 Gb/s link to the location is required.

For auxiliary database backup information, see the NSP NFM-P System Administrator Guide for the installed release.

Obtain software, stop database

3

Transfer the backup file sets to a secure location on a station that is accessible to each auxiliary database station.

Note: Ensure that you record the following for each station:
   • backup file set directory path
   • station to which the backup file set belongs

4

Download the following NFM-P installation files to an empty local directory on a station that is reachable by each auxiliary database station:
   • nsp-nfmp-jre-R.r.p-rel.v.rpm
   • vertica-V.w.x-y.rpm
   • nsp-nfmp-aux-db-R.r.p-rel.v.rpm
   • VerticaSw_PreInstall.sh

where

R.r.p is the NSP release identifier, in the form MAJOR.minor.patch
V.w.x-y is a version number
v is a version identifier
Decommission existing stations

Perform the following steps on each auxiliary database station.

1. Log in as the root user on the auxiliary database station.
2. Open a console window.
3. Enter the following:
   ```
   # cd /etc/rc3.d
   #
   ```
4. Enter the following commands in sequence:
   ```
   # ./S90samauxdb stop
   # ./S99verticad stop
   # ./S99vertica_agent stop
   # ./S90samauxdbproxy stop
   ```
5. Enter the following commands in sequence:
   ```
   # chkconfig samauxdb off
   # chkconfig verticad off
   # chkconfig vertica_agent off
   # chkconfig samauxdbproxy off
   ```
6. Uninstall the auxiliary database software, if required.

   Note: You must use the auxiliary database uninstallation procedure in the documentation for the installed release, and not the procedure in this guide.

Recommission stations, if required

If you are re-using any auxiliary database stations, recommission each station according to the platform specifications in this guide and in the *NSP NFM-P Planning Guide*.

Note: The IP address of an auxiliary database station must not change as part of the recommissioning exercise.

Prepare all stations for upgrade

Perform Step 9 to Step 17 on each station that is commissioned as an auxiliary database station.

Go to Step 18.
Prepare individual station for upgrade

9
Log into the newly commissioned auxiliary database station as the root user.

10
Transfer the downloaded NFM-P installation files to an empty directory on the station.

Note: In subsequent steps, the directory is called the NFM-P software directory.

11
Navigate to the NFM-P software directory.

Note: Ensure that the directory contains only the installation files.

12
Enter the following:

```
# chmod +x *
```

13
Enter the following:

```
# ./VerticaSw_PreInstall.sh
```

The script displays output similar to the following:
INFO: About to set kernel parameters in /etc/sysctl.conf...
INFO: Completed setting kernel parameters in /etc/sysctl.conf...
INFO: About to change the current values of the kernel parameters...
INFO: Completed changing the current values of the kernel parameters...
INFO: About to set ulimit parameters in /etc/security/limits.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.conf...
Checking Vertica DBA group samauxdb...
Adding Vertica DBA group samauxdb...
Checking Vertica user samauxdb...
Adding Vertica user samauxdb...
Changing ownership of the directory /opt/nsp/nfmp/auxdb to samauxdb:samauxdb.
Adding samauxdb to sudoers file.
Changing ownership of /opt/nsp/nfmp/auxdb files.
INFO: About to add setting to /etc/rc.d/rc.local...
INFO: Completed adding setting to /etc/rc.d/rc.local...

14

If the script instructs you to perform a restart, perform the following steps.

1. Enter the following:
   
   ```
   # systemctl reboot
   ```
   
   The station reboots.

2. When the reboot is complete, log in to the station as the root user.

3. Open a console window.

4. Navigate to the NFM-P software directory.

15

Enter the following:

```
# yum install *.rpm
```

The `yum` utility resolves any package dependencies, and displays the following prompt:

- Total size: nn G
- Installed size: nn G

Is this ok [y/d/N]:

16

Enter **y.** The following and the installation status are displayed as each package is installed:

- Downloading packages:
- Running transaction check
- Running transaction test
- Transaction test succeeded
- Running transaction

The package installation is complete when the following is displayed:

- Complete!

17

Enter the following to reboot the auxiliary database station:

```
# systemctl reboot
```

The station reboots.

**Upgrade database**

18

When each station reboot is complete, log in to one auxiliary database station as the root user.
Note: In subsequent steps, this station is called the home station.

Open a console window.

Enter the following:

```
# cp /opt/nsp/nfmp/auxdb/install/config/install.config.default
/opt/nsp/nfmp/auxdb/install/config/install.config
```

Open the /opt/nsp/nfmp/auxdb/install/config/install.config file using a plain-text editor such as vi.

Edit the following lines in the file to read:

```
hosts=internal_IP1,internal_IP2...internal_IPn
export_hosts=internal_IP1[export_IP1],internal_IP2[export_IP2]...
            internal_IPn[export_IPn]
```

where

- `internal_IP1, internal_IP2...internal_IPn` are the IP addresses that the stations use to communicate with each other
- `export_IP1, export_IP2...export_IPn` are the IP addresses that the stations use to communicate with the NFM-P servers

Note: If the [export_IP] entry for a station is omitted, the station uses the `internal_IP` address for communication with the NFM-P servers.

The following is an export_hosts configuration example:

```
export_hosts=10.1.1.10[198.51.100.10],10.1.1.11[198.51.100.11],10.1.1.12[198.51.100.12]
```

Save and close the install.config file.

Enter the following:

```
# cd /opt/nsp/nfmp/auxdb/install/bin
```

Enter the following:

```
# ./auxdbAdmin.sh install
```

The script sequentially prompts for the root user password of each auxiliary database station.
Enter the required password at each prompt. The script installs the software on each auxiliary database station, and then starts the auxiliary database.

When the script execution is complete, enter the following to display the auxiliary database status:

```
# ./auxdbAdmin.sh status
```

The script displays the following:

```
Database status
Node    | Host     | State  | Version | DB
--------|----------|--------|---------|-------
host_IP_1 | internal_IP_1 | STATE  | version | db_name
host_IP_2 | internal_IP_2 | STATE  | version | db_name
          |           | STATE  | version | db_name
          |           | STATE  | version | db_name
```

Output captured in log_file

Repeat Step 27 periodically until each STATE entry reads UP.

Enter the following to stop the auxiliary database:

```
# ./auxdbAdmin.sh stop
```

Enter the following to display the auxiliary database status:

```
# ./auxdbAdmin.sh status
```

The script displays the following:

```
Database status
Node    | Host     | State  | Version | DB
--------|----------|--------|---------|-------
host_IP_1 | internal_IP_1 | STATE  | version | db_name
host_IP_2 | internal_IP_2 | STATE  | version | db_name
          |           | STATE  | version | db_name
          |           | STATE  | version | db_name
```
host_IP_n | internal_IP_n | STATE | version | db_name
    Output captured in log_file

31

Repeat Step 30 periodically until each STATE entry reads DOWN.

32

Perform the following steps on each auxiliary database station.
1. Transfer the backup file set for the station to the /opt/nsp/nfmp/auxdb directory.
2. Enter the following:
   ```
   # chown -R samauxdb /opt/nsp/nfmp/auxdb/backup_directory
   
   where backup_directory is the name of the directory that contains the backup file set
   ```
3. Open the following file with a plain-text editor such as vi:
   ```
   /opt/nsp/nfmp/auxdb/backup_directory/samAuxDbBackup_restore.conf
   
   where backup_directory is the name of the directory that contains the backup file set
   ```
4. Replace each instance of:
   ```
   /opt/5620sam
   
   with:
   ```
   ```
   /opt/nsp/nfmp
   ```
5. Save and close the samAuxDbBackup_restore.conf file.

33

On the home station, enter the following to switch to the samauxdb user:
```
# su - samauxdb
```

34

Enter the following:
```bash
cd /opt/nsp/nfmp/auxdb/install/bin
```

35

Enter the following to restore the database:
```bash
vbr.py --task restore --config-file /opt/nsp/nfmp/auxdb/backup_directory/samAuxDbBackup_restore.conf
```

where backup_directory is the name of the directory that contains the backup file set

The database restore begins.

36

When the database restore is complete, enter the following to switch back to the root user:
```bash
exit
```
Enter the following:

```
# ./auxdbAdmin.sh upgrade
```

The following prompt is displayed:

Updating Vertica - Please perform a backup before proceeding with this option
Do you want to proceed (YES/NO)?

Enter YES.

The following prompt is displayed:

Please enter auxiliary database dba password [if you are doing initial setup for auxiliary database, press enter]:

Enter the dba password.

The following prompt is displayed:

Please verify auxiliary database dba password:

Enter the dba password again.

The upgrade begins, and operational messages are displayed.

The upgrade is complete when the following is displayed:

```
Database database_name started successfully
Output captured in log_file
```

Enter the following to display the auxiliary database status:

```
# ./auxdbAdmin.sh status
```

The script displays the following:

```
Database status
Node | Host         | State | Version | DB
-----------------------------------------------
host_IP_1 | internal_IP_1 | STATE | version | db_name
host_IP_2 | internal_IP_2 | STATE | version | db_name
.
.
host_IP_n | internal_IP_n | STATE | version | db_name
```
Repeat Step 41 periodically until each STATE entry reads UP.

Enter the following to apply the updated database schema:

```
# ./auxdbAdmin.sh upgradeDb
```

The following prompt is displayed:

Please enter auxiliary database dba password:

Enter the dba password.

The following prompt is displayed:

Please enter auxiliary database user password:

Enter the database user password.

The following prompt is displayed:

Please enter database port [default]:

Press Enter.

The following prompt is displayed:

Do you want to proceed (YES/NO)?:

Enter YES.

Do you want to proceed (YES/NO)?:

The database schema is updated.

Enter the following to start the auxiliary database:

```
# ./auxdbAdmin.sh start
```

Enter the following to display the auxiliary database status:

```
# ./auxdbAdmin.sh status
```

The script displays the following:

Database status
<table>
<thead>
<tr>
<th>Node</th>
<th>Host</th>
<th>State</th>
<th>Version</th>
<th>DB</th>
</tr>
</thead>
<tbody>
<tr>
<td>host_IP_1</td>
<td>internal_IP_1</td>
<td>STATE</td>
<td>version</td>
<td>db_name</td>
</tr>
<tr>
<td>host_IP_2</td>
<td>internal_IP_2</td>
<td>STATE</td>
<td>version</td>
<td>db_name</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>host_IP_n</td>
<td>internal_IP_n</td>
<td>STATE</td>
<td>version</td>
<td>db_name</td>
</tr>
</tbody>
</table>

Output captured in log_file

50

Repeat Step 49 periodically until each STATE entry reads UP.

51

Close the open console windows, as required.

END OF STEPS
5620 SAM analytics server upgrade

9.12 To upgrade the 5620 SAM analytics servers

9.12.1 Description

The following steps describe how to upgrade the analytics servers in a 5620 SAM system to NSP analytics servers. Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

**Note:** You must upgrade all analytics servers in the system as one uninterrupted operation.

**Note:** You require root and nsp user privileges on each analytics server station.

**Note:** The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands

- # — root user
- bash$ — nsp user

9.12.2 Steps

**Commission new stations, if required**

1. If you are deploying the analytics servers on a new station, commission the station according to the platform specifications in this guide and in the NSP NFM-P Planning Guide.

**Stop analytics servers**

2. If all analytics servers are not stopped, perform the following steps on each analytics server station to stop the analytics server.
   1. Log in as the samadmin user on the analytics server station.
   2. Open a console window.
   3. Enter the following:
      
      ```bash
      bash$ /opt/5620sam/analytics/bin/AnalyticsAdmin.sh stop
      ```

      The following and other messages are displayed:

      Stopping 5620 SAM Analytics Application

      When the analytics server is completely stopped, the following is displayed:

      5620 SAM Analytics Server is not running
Export Analytics repository

3 You must use one existing analytics server station to export the central Analytics repository of report results.
Designate an analytics server station for the export; in subsequent steps, the station is called Server A.

4 Log in as the samadmin user on Server A.

5 Open a console window.

6 Download the following NFM-P installation file to the /opt/5620sam/analytics/bin directory on Server A:
   • analyticsDataMigration.sh

7 Navigate to the /opt/5620sam/analytics/bin directory.

8 Enter the following:
   # chmod +x analyticsDataMigration.sh

9 Enter the following:
   # ./analyticsDataMigration.sh export main_db instance port
   where
   main_db is the IP address of the standalone or primary main database
   instance is the database instance name, for example, samdb1
   port is the database listener port; the installation default is 1523
   Messages like the following are displayed as the export proceeds:
   Exporting Contents from Repository Database. This may take several minutes to complete...
   /opt/5620sam/analytics/bin/analytics.export.date-time.log can be monitored for progress
   Completed Exporting Contents from Repository Database
   Please backup/transfer /opt/5620sam/analytics/bin/analyticExport.zip to a secure location
You must restore this file to the /opt/nsp location on the RHEL 7 station after installing the new rpms.

10

Transfer the /opt/5620sam/analytics/bin/analyticExport.zip file to a secure location on another station.

Recommission Server A station, if required

11

If you are re-using the Server A station, recommission the station according to the platform specifications in this guide and in the NSP NFM-P Planning Guide.

Upgrade Server A

12

Log in to the Server A station as the root user.

13

Download the following NFM-P installation files to an empty local directory on the new or recommissioned Server A station:

• nspos-jre-\textit{R.r.p}-rel.v.rpm
• nspos-tomcat-\textit{R.r.p}-rel.v.rpm
• nspos-analytics-server-\textit{R.r.p}-rel.v.rpm

where

\textit{R.r.p} is the NSP release identifier, in the form \textit{MAJOR.minor.patch}
\textit{v} is a version identifier

\textbf{i} \textbf{Note}: In subsequent steps, the directory is called the NFM-P software directory.

14

Open a console window.

15

Navigate to the NFM-P software directory.

\textbf{i} \textbf{Note}: Ensure that the directory contains only the installation files.

16

Enter the following:

\begin{verbatim}
# chmod +x *
\end{verbatim}
Enter the following:

```
# yum install *.rpm
```

For each package, the `yum` utility resolves any package dependencies and displays the following prompt:

Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:

Enter `y`. The following and the installation status are displayed as each package is installed:

- Downloading packages:
- Running transaction check
- Running transaction test
- Transaction test succeeded
- Running transaction

The package installation is complete when the following is displayed:

```
Complete!
```

If you are manually configuring TLS, perform the following steps.

1. Transfer the required TLS keystore and truststore files from the standalone or primary main server station to the analytics server station. See Chapter 6, “TLS configuration and management” for information about configuring TLS.

   **Note:** The files must be located on a path that is owned by the nsp user.

2. Enter the following:

   ```
   # chown nsp:nsp keystore_file
   ```

   where `keystore_file` is the absolute path of the keystore file

3. Enter the following:

   ```
   # chown nsp:nsp truststore_file
   ```

   where `truststore_file` is the absolute path of the truststore file

Enter the following to switch to the nsp user:

```
# su - nsp
```

Transfer the analyticExport.zip file from Step 10 to the /opt/nsp directory.
Enter the following:

```
bash$ cd /opt/nsp/analytics/bin
```

Enter the following:

```
bash$ ./AnalyticsAdmin.sh updateConfig
```

The script displays the following prompt:

```
THIS ACTION UPDATES /opt/nsp/analytics/config/install.config
Please type 'YES' to continue
```

Enter YES. The script displays the first in a series of prompts.

At each prompt, enter a parameter value; to accept a default in brackets, press `\t`.

The following table lists and describes each parameter.

**Table 9-6  NFM-P analytics server parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary PostgreSQL Repository Database Host</td>
<td>The primary report results repository, which is the IP address or hostname of one of the following:</td>
</tr>
<tr>
<td></td>
<td>• if the NSP system includes only the NFM-P, the primary or standalone NFM-P main server</td>
</tr>
<tr>
<td></td>
<td>• if the NSP system includes the NSD and NRC, the primary or standalone NSD and NRC server</td>
</tr>
<tr>
<td>Secondary PostgreSQL Repository Database Host</td>
<td>In a redundant system, the standby report results repository, which is the IP address or hostname of one of the following:</td>
</tr>
<tr>
<td></td>
<td>• if the NSP system includes only the NFM-P, the standby NFM-P main server</td>
</tr>
<tr>
<td></td>
<td>• if the NSP system includes the NSD and NRC, the standby NSD and NRC server</td>
</tr>
<tr>
<td>Auxiliary Data Source DB Host 1</td>
<td>If the system includes an auxiliary database, the IP address of an auxiliary database station</td>
</tr>
<tr>
<td>Auxiliary Data Source DB Host 2</td>
<td>If the system includes an auxiliary database, the IP address of an auxiliary database station</td>
</tr>
<tr>
<td>Auxiliary Data Source DB Host 3</td>
<td>If the system includes an auxiliary database, the IP address of an auxiliary database station</td>
</tr>
<tr>
<td>Auxiliary Data Source DB Port [5433]</td>
<td>If the system includes an auxiliary database, the auxiliary database port</td>
</tr>
<tr>
<td>Primary Oracle Data Source DB Host</td>
<td>The primary or standalone main database IP address</td>
</tr>
<tr>
<td>Primary Oracle Data Source DB Name</td>
<td>The primary or standalone main database instance name</td>
</tr>
</tbody>
</table>
Table 9-6  NFM-P analytics server parameters  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Oracle Data Source DB Port [1523]</td>
<td>The TCP port on the primary or standalone main database station that receives database requests</td>
</tr>
<tr>
<td>Secondary Oracle Data Source DB Host</td>
<td>In a redundant system, the standby main database IP address</td>
</tr>
<tr>
<td>Secondary Oracle Data Source DB Name</td>
<td>In a redundant system, the standby main database instance name</td>
</tr>
<tr>
<td>Secondary Oracle Data Source DB Port [1523]</td>
<td>In a redundant system, the TCP port on the standby main database station that receives database requests</td>
</tr>
<tr>
<td>PKI Server IP Address</td>
<td>If the TLS configuration is automated using a PKI server, the PKI server IP address; if you have a set of signed TLS certificates, press Enter</td>
</tr>
<tr>
<td>PKI Server Port [2391]</td>
<td>If the TLS configuration is automated using a PKI server, the PKI server port</td>
</tr>
<tr>
<td>Zookeeper Connection String</td>
<td>The IP address and port of each ZooKeeper host, in the following format:</td>
</tr>
<tr>
<td></td>
<td>host1_IP:port;host2_IP:port</td>
</tr>
<tr>
<td></td>
<td>where</td>
</tr>
<tr>
<td></td>
<td>host1_IP and host2_IP are the IP addresses of the ZooKeeper hosts</td>
</tr>
<tr>
<td></td>
<td>port is the TCP port that the host uses for ZooKeeper communication</td>
</tr>
<tr>
<td></td>
<td>The ZooKeeper hosts that you specify are one of the following:</td>
</tr>
<tr>
<td></td>
<td>• if the NSP system includes only the NFM-P, the NFM-P main servers</td>
</tr>
<tr>
<td></td>
<td>• if the NSP system includes the NSD and NRC, the NSD servers</td>
</tr>
</tbody>
</table>

Perform Analytics repository migration

Enter the following:
```bash
bash$ ./AnalyticsAdmin.sh migratedb
```

Note: The analytics server starts automatically after the migration.
The following messages and prompt are displayed:
```
date time Migrating Analytics to NSPOS
Migrating Analytics Server to New Database ...
Do you have existing TLS certificates?(yes/no)
```

Perform one of the following.
a. If you have TLS keystore and truststore files, perform the following steps.
   1. Enter yes.
      The following prompt is displayed:
      Enter TLS keystore Path, including filename:
   2. Enter the absolute path of the keystore file.
      The following message and prompt are displayed:
      path/keystore_file found.
      Enter TLS truststore Path, including filename:
   3. Enter the absolute path of the truststore file.
      The following message and prompt are displayed:
      path/truststore_file found.
      Enter TLS Keystore Password:
   4. Enter the keystore password.
      The following message and prompt are displayed:
      Verifying TLS Keystore...
      Certificate loading...
      Verified TLS Certificate
      Enter TLS Truststore Password:
   5. Enter the truststore password.
      The following is displayed as the configuration is updated:
      Verifying TLS Truststore...
      Certificate loading...
      Verified TLS Certificate
      TLS Config has been updated

b. If you do not have TLS keystore and truststore files, perform the following steps.
   1. Enter no.
      The following prompt is displayed:
      Enter the Path where the TLS Certificates should be created:
   2. Enter the absolute path of a directory that is owned by the nsp user, for example, /opt/nsp.
      The following message and prompt are displayed:
      The path that will contain the keystore and the truststore is:
      path
      Set the keystore password:
   3. Enter the keystore password.
      The following prompt is displayed:
      Set the truststore password:
4. Enter the truststore password.
   The following messages are displayed:
   The files nsp.keystore and nsp.truststore have been created
   TLS Config has been updated
   
The migration proceeds, the upgrade completes, and messages like the following are displayed:
   Creating Analytics Repository Schema
   Analytics Repository Schema creation is complete
   Importing analytics server data from oracle. This may take few minutes to complete...
   /opt/nsp/analytics/log/analytics.import.date-time.log can be monitored for progress
   Finished Importing analytics server data from oracle
   date time Upgrading Analytics Server
   Updating DB TABLES After upgrade
   Updated n Tables
   date time Analytic Server upgrade is completed and starting server
   date time Starting Analytics Application
   Waiting for Analytics Server to come up
   date time Analytics Server is UP and Running
   Starting Watchdog process to check Oracle database connectivity...
   Analytics Server successfully started!
   date time Configuring Analytics Server....
   Deploying Reports After Upgrade
   Start Deploying report
   .
   .
   .
   All reports successfully tracked
   date time Analytics Server upgraded successfully

Enter the following to view the analytics server status; ensure that the server is initialized:
bash$ ./AnalyticsAdmin.sh status
The following is displayed when the analytics server is initialized:
Analytics Server Version : Release
Analytics Application is running
Active PostgreSQL Repository Database Host : n.n.n.n
Auxiliary Data source Database Host(s) : n.n.n.n,n.n.n.n, n.n.n.n ...
Active Oracle Data source Database Host : n.n.n.n
TLS KeyStore File Path : path/keystore_file
TLS trustStore File Path : path/truststore_file

Upgrade remaining analytics servers

28 If you are using new stations for the analytics servers, you must uninstall the analytics server software on each existing analytics server station.
Perform the analytics server uninstallation procedure from the documentation for the installed analytics server release on each existing analytics server.

29 Perform Step 31 to Step 46 on each remaining new or recommissioned analytics server station.

30 Go to step Step 47.

31 Log in to the analytics server station as the root user.

32 Download the following NFM-P installation files to an empty local directory:
  • nspos-jre-R.r.p-rel.v.rpm
  • nspos-tomcat-R.r.p-rel.v.rpm
  • nsp-analytics-server-R.r.p-rel.v.rpm
where
  R.r.p is the NSP release identifier, in the form MAJOR.minor.patch
  v is a version identifier

  Note: In subsequent steps, the directory is called the NFM-P software directory.

33 Open a console window.

34 Navigate to the NFM-P software directory.

  Note: Ensure that the directory contains only the installation files.
Enter the following:

```
# chmod +x *
```

Enter the following:

```
# yum install *.rpm
```

For each package, the yum utility resolves any package dependencies and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
```

The package installation is complete when the following is displayed:

```
Complete!
```

If you are manually configuring TLS, perform the following steps.

1. Transfer the required TLS keystore and truststore files from the standalone or primary main server station to the analytics server station. See Chapter 6, “TLS configuration and management” for information about configuring TLS.

   **Note:** The files must be located on a path that is owned by the nsp user.

2. Enter the following:

   ```
   # chown nsp:nsp keystore_file
   ```

   where `keystore_file` is the absolute path of the keystore file

3. Enter the following:

   ```
   # chown nsp:nsp truststore_file
   ```

   where `truststore_file` is the absolute path of the truststore file

Enter the following to switch to the nsp user:

```
# su - nsp
```
Enter the following:

```
bash$ cd /opt/nsp/analytics/bin
```

Enter the following:

```
bash$ ./AnalyticsAdmin.sh updateConfig
```

The script displays the following prompt:

```
THIS ACTION UPDATES /opt/nsp/analytics/config/install.config
Please type 'YES' to continue
```

Enter YES. The script displays the first in a series of prompts.

At each prompt, enter a parameter value; to accept a default in brackets, press `↵`.

The following table lists and describes each parameter.

**Table 9-7  NFM-P analytics server parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary PostgreSQL Repository Database Host</td>
<td>The primary report results repository, which is the IP address or hostname of one of the following:</td>
</tr>
<tr>
<td></td>
<td>• if the NSP system includes only the NFM-P, the primary or standalone NFM-P main server</td>
</tr>
<tr>
<td></td>
<td>• if the NSP system includes the NSD and NRC, the primary or standalone NSD and NRC server</td>
</tr>
<tr>
<td>Secondary PostgreSQL Repository Database Host</td>
<td>In a redundant system, the standby report results repository, which is the IP address or hostname of one of the following:</td>
</tr>
<tr>
<td></td>
<td>• if the NSP system includes only the NFM-P, the standby NFM-P main server</td>
</tr>
<tr>
<td></td>
<td>• if the NSP system includes the NSD and NRC, the standby NSD and NRC server</td>
</tr>
<tr>
<td>Auxiliary Data Source DB Host 1</td>
<td>If the system includes an auxiliary database, the IP address of an auxiliary database station</td>
</tr>
<tr>
<td>Auxiliary Data Source DB Host 2</td>
<td>If the system includes an auxiliary database, the IP address of an auxiliary database station</td>
</tr>
<tr>
<td>Auxiliary Data Source DB Host 3</td>
<td>If the system includes an auxiliary database, the IP address of an auxiliary database station</td>
</tr>
<tr>
<td>Auxiliary Data Source DB Port [5433]</td>
<td>If the system includes an auxiliary database, the auxiliary database port</td>
</tr>
<tr>
<td>Primary Oracle Data Source DB Host</td>
<td>The primary or standalone main database IP address</td>
</tr>
<tr>
<td>Primary Oracle Data Source DB Name</td>
<td>The primary or standalone main database instance name</td>
</tr>
</tbody>
</table>
### Table 9-7  NFM-P analytics server parameters  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Oracle Data Source DB Port [1523]</td>
<td>The TCP port on the primary or standalone main database station that receives database requests</td>
</tr>
<tr>
<td>Secondary Oracle Data Source DB Host</td>
<td>In a redundant system, the standby main database IP address</td>
</tr>
<tr>
<td>Secondary Oracle Data Source DB Name</td>
<td>In a redundant system, the standby main database instance name</td>
</tr>
<tr>
<td>Secondary Oracle Data Source DB Port [1523]</td>
<td>In a redundant system, the TCP port on the standby main database station that receives database requests</td>
</tr>
<tr>
<td>PKI Server IP Address</td>
<td>If the TLS configuration is automated using a PKI server, the PKI server IP address; if you have a set of signed TLS certificates, press Enter</td>
</tr>
<tr>
<td>PKI Server Port [2391]</td>
<td>If the TLS configuration is automated using a PKI server, the PKI server port</td>
</tr>
<tr>
<td>Zookeeper Connection String</td>
<td>The IP address and port of each ZooKeeper host, in the following format:</td>
</tr>
<tr>
<td></td>
<td><code>host1_IP:port;host2_IP:port</code></td>
</tr>
<tr>
<td></td>
<td>where</td>
</tr>
<tr>
<td></td>
<td><code>host1_IP</code> and <code>host2_IP</code> are the IP addresses of the ZooKeeper hosts</td>
</tr>
<tr>
<td></td>
<td><code>port</code> is the TCP port that the host uses for ZooKeeper communication</td>
</tr>
<tr>
<td></td>
<td>The ZooKeeper hosts that you specify are one of the following:</td>
</tr>
<tr>
<td></td>
<td>• if the NSP system includes only the NFM-P, the NFM-P main servers</td>
</tr>
<tr>
<td></td>
<td>• if the NSP system includes the NSD and NRC, the NSD servers</td>
</tr>
</tbody>
</table>

---

Enter the following to install the analytics server software:

```
bash$ ./AnalyticsAdmin.sh install
```

**Note:** The analytics server starts automatically after the installation.

The following message and prompt are displayed:

```text
date time Installing Analytics Server...
Do you have existing TLS certificates? (yes/no)
```

Perform one of the following.

a. If you have TLS keystore and truststore files, perform the following steps.
   1. Enter yes

---

Release 18.9
September 2018
Issue 1
The following prompt is displayed:

Enter TLS keystore Path, including filename:

2. Enter the absolute path of the TLS keystore file.
The following message and prompt are displayed:

path/keystore_file found.
Enter TLS truststore Path, including filename:

3. Enter the absolute path of the truststore file.
The following message and prompt are displayed:

path/truststore_file found.
Enter TLS Keystore Password:

4. Enter the keystore password.
The following message and prompt are displayed:

Verifying TLS Keystore...
Certificate loading...
Verified TLS Certificate
Enter TLS Truststore Password:

5. Enter the truststore password.
The following is displayed as the configuration is updated:

Verifying TLS Truststore...
Certificate loading...
Verified TLS Certificate
TLS Config has been updated

b. If you do not have TLS keystore and truststore files, perform the following steps.

1. Enter no input.
The following prompt is displayed:
Enter the Path where the TLS Certificates should be created:

2. Enter the absolute path of a directory that is owned by the nsp user, for example, /opt/nsp.
The following message and prompt are displayed:
The path that will contain the keystore and the truststore is:
path
Set the keystore password:

3. Enter the keystore password.
The following prompt is displayed:
Set the truststore password:

4. Enter the truststore password.
The following messages are displayed:
The files nsp.keystore and nsp.truststore have been created
TLS Config has been updated

The installation begins, and messages like the following are displayed:

Creating Analytics Repository Schema
Analytics Repository Schema creation is complete
Please wait while Analytics Server is being installed...This may take a few minutes
date time Deploying Analytics Server in Tomcat...
Analytics Server successfully deployed in Tomcat
date time Starting Analytics Server...
date time Starting Analytics Application
Waiting for Analytics Server to come up
date time Analytics Server is UP and Running
Starting Watchdog process to check Oracle database connectivity...
Analytics Server successfully started!
date time Configuring Analytics Server....
Deploying Reports...
Analytics Server configured successfully
date time Analytics Server successfully installed

Enter the following to view the analytics server status; ensure that the server is initialized:

bash$ ./AnalyticsAdmin.sh status

The following is displayed when the analytics server is initialized:

Analytics Server Version : Release
Analytics Application is running
Active PostgreSQL Repository Database Host : n.n.n.n
Auxiliary Data source Database Host(s) : n.n.n.n,n.n.n.n,n.n.n.n...
Active Oracle Data source Database Host : n.n.n.n
TLS KeyStore File Path : path/keystore_file
TLS trustStore File Path : path/truststore_file

Close the console window.
Finalize data migration

47
Log in to the Server A station as the nsp user.

48
Enter the following:
bash$ cd /opt/nsp/analytics/bin

49
Enter the following:
bash$ ./AnalyticsAdmin.sh droporacledb
The script displays the following prompt:
THIS ACTION WILL Delete the Oracle report repository DB. ALL REPORTS
WILL BE DELETED, regardless if there are redundant Analytics Servers
still running
Please type 'YES' to continue

50
Enter YES .
The following messages are displayed:
Dropping Oracle Analytics Schema
Dropping Existing Oracle Analytics Schema
Deleted nn Analytics Oracle Tables

51
Enter the following:
bash$ ./AnalyticsAdmin.sh stop
The Server A analytics server stops.

52
Enter the following:
bash$ ./AnalyticsAdmin.sh start
The analytics server starts.

53
Close the console window.

END OF STEPS
5620 SAM upgrade to NFM-P
5620 SAM analytics server upgrade
To upgrade the 5620 SAM analytics servers
10 NFM-P upgrade

10.1 Overview

10.1.1 Purpose
This chapter describes how to upgrade the components of a standalone or redundant NFM-P system.

10.1.2 Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1 Overview</td>
<td>367</td>
</tr>
<tr>
<td>Introduction</td>
<td>368</td>
</tr>
<tr>
<td>10.2 General information</td>
<td>368</td>
</tr>
<tr>
<td>10.3 To perform the pre-upgrade tasks</td>
<td>369</td>
</tr>
<tr>
<td>10.4 To apply an NSP RHEL qcow2 OS update</td>
<td>380</td>
</tr>
<tr>
<td>Standalone NFM-P system upgrade</td>
<td>383</td>
</tr>
<tr>
<td>10.5 Standalone system upgrade workflow</td>
<td>383</td>
</tr>
<tr>
<td>10.6 To upgrade a standalone NFM-P system</td>
<td>385</td>
</tr>
<tr>
<td>Redundant NFM-P system upgrade</td>
<td>400</td>
</tr>
<tr>
<td>10.7 Component references</td>
<td>400</td>
</tr>
<tr>
<td>10.8 Redundant system upgrade workflow</td>
<td>401</td>
</tr>
<tr>
<td>10.9 To upgrade a redundant NFM-P system</td>
<td>406</td>
</tr>
<tr>
<td>Auxiliary server upgrade</td>
<td>435</td>
</tr>
<tr>
<td>10.10 To upgrade an NFM-P auxiliary server</td>
<td>435</td>
</tr>
<tr>
<td>NSP Flow Collector upgrade</td>
<td>438</td>
</tr>
<tr>
<td>10.11 To upgrade an NSP Flow Collector</td>
<td>438</td>
</tr>
<tr>
<td>Auxiliary database upgrade</td>
<td>441</td>
</tr>
<tr>
<td>10.12 To upgrade an NFM-P auxiliary database</td>
<td>441</td>
</tr>
<tr>
<td>NFM-P analytics server upgrade</td>
<td>449</td>
</tr>
<tr>
<td>10.13 To upgrade the NFM-P analytics servers</td>
<td>449</td>
</tr>
</tbody>
</table>
Introduction

10.2 General information

10.2.1 Description

This chapter includes procedures for standalone and redundant NFM-P system upgrades, and for the upgrade of the following individual system components:

- auxiliary server
- NSP Flow Collector
- auxiliary database
- analytics server

**Note:** This chapter does not describe upgrading a 5620 SAM system to an NFM-P release. For information about such an upgrade, see Chapter 9, "5620 SAM upgrade to NFM-P".

**Note:** It is strongly recommended that you verify the checksum of each software package or file that you download from OLCS. You can compare the checksum value on the download page with, for example, the output of the RHEL md5sum or sha256sum command. See the appropriate RHEL man page for information.

**Note:** If the main servers in a redundant NFM-P system use different time zones, for example, in a geographically dispersed deployment, and the NSP Analytics application creates reports based on data aggregation, it is recommended that you upgrade the main server in the aggregation time zone first. Otherwise, during the system upgrade, aggregations may run using the previous time-zone setting and skew the aggregation report results. In such a case, after both main servers are upgraded you must use the client GUI to change the Analytics aggregation time-zone setting.

See the NSP Analytics application online help for aggregation configuration information.

Chapter 14, “Single-user client deployment” and Chapter 15, “Client delegate server deployment” describe single-user GUI client and client delegate server installation and upgrade.

The NFM-P samconfig utility is used for component configuration and deployment; see Chapter 3, "Using samconfig" for information about the samconfig utility.

**Note:** Before you begin a system upgrade, you must perform 10.3 “To perform the pre-upgrade tasks” (p. 369) to collect the required information and to ensure that the required upgrade conditions are in place.

**Note:** The Bash shell is the supported command shell for RHEL CLI operations.
10.3 To perform the pre-upgrade tasks

10.3.1 Description

CAUTION

Service Disruption

A system upgrade fails unless you strictly observe the requirements and restrictions in Chapter 2, “Before you begin” and the NSP NFM-P Planning Guide.

An NFM-P system upgrade requires a thorough understanding of the deployment restrictions and requirements.

It is essential that you plan, document, and test the upgrade procedure in advance on a lab system that is representative of the actual network. Contact technical support to assess the upgrade requirements of your system; in a large or complex network, it is strongly recommended that you engage the technical support upgrade service.

The following steps describe the actions that you must perform in advance of a standalone or redundant NFM-P system upgrade.

Note: You require the following user privileges on each server station in the system:

- root
- nsp

Note: The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:

- # —root user
- bash$ —nsp user

10.3.2 Steps

CAUTION

Deployment failure

The RHEL OS of any NFM-P component requires specific versions of some RHEL packages. If the required package versions are not installed, the component upgrade fails.

See 4.10.4 “Special RHEL OS package requirements” (p. 59) for the required package versions.

Check and configure firewalls

Before you attempt to upgrade an NFM-P system, you must ensure that each firewall between the system components allows the required traffic to pass between the components, or is disabled. You can configure and enable the firewalls after the upgrade, if required.
a. Ensure that each firewall is configured to allow the required traffic to pass. See the *NSP NFM-P Planning Guide* for a list of the ports that must be open on each component.

**i Note:** The RHEL Firewalld service must be configured using the Firewalld rules in the *NSP NFM-P Planning Guide*, which describes using NFM-P templates for rule creation.

b. Disable each firewall; see the external firewall documentation, or perform the following steps on each component station to disable Firewalld.

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following:
   ```
   # systemctl stop firewalld
   ```
4. Enter the following:
   ```
   # systemctl disable firewalld
   ```
5. Close the console window.

**Download installation files**

1. Download the following NFM-P installation files to an empty directory on a station that is not affected by the upgrade activity:

   **i Note:** The station must be reachable by each station that is to host an NFM-P main server or main database.
   - nsp-nfmp-jre-\(R.r.p\)-rel.\(v\).rpm
   - nsp-nfmp-config-\(R.r.p\)-rel.\(v\).rpm
   - nsp-nfmp-nspos-\(R.r.p\)-rel.\(v\).rpm
   - nsp-nfmp-main-server-\(R.r.p\)-rel.\(v\).rpm
   - nsp-nfmp-oracle-\(R.r.p\)-rel.\(v\).rpm
   - nsp-nfmp-main-db-\(R.r.p\)-rel.\(v\).rpm
   - OracleSw_PreInstall.sh
   where
   - \(R.r.p\) is the NSP release identifier, in the form \(MAJOR.minor.patch\)
   - \(v\) is a version identifier

2. If the NFM-P is to manage one or more LTE-N devices, download the following additional package to the directory:
   - nsp-nfmp-semvalidator-\(R.r.p\)-rel.\(v\).rpm
Validate database

4

Before you upgrade a main database, you must ensure that the main database contains only valid records, or the upgrade fails.

**Note:** In a redundant system, you must perform the validation on the primary main database station.

Login as the root user on the main database station.

5

Transfer the following downloaded file to an empty directory on the main database station:

- OracleSw_PreInstall.sh

6

Navigate to the directory that contains the OracleSw_PreInstall.sh file.

7

Enter the following:

```
# chmod +x OracleSw_PreInstall.sh
```

8

Perform the following steps.

1. Enter the following:

```
# ./OracleSw_PreInstall.sh -check
```

   The following prompt is displayed:

   Enter the password for the "SYS" Oracle user (terminal echo is off):

2. Enter the SYS user password.

   The following messages are displayed:

   Logging Oracle pre install checks to log_file

   In upgrade check mode, this script does not modify the system.

   About to validate that the database can be upgraded to release.

   Found the NFM-P main database installation directory /opt/nsp/nfmp/db/install.

   If the validation is successful, the following messages and prompt are displayed:

   INFO: Database upgrade validation passed.

3. If the validation is successful, go to **Step 9**.

4. If the script detects one or more invalid items, for example, an NE at a release that the new NFM-P software does not support, an incomplete deployment, or other upgrade restriction, one line like the following is displayed for each item:
ERROR: Error message
The following is displayed as the script exits.
ERROR: The database cannot be upgraded. Please fix the above errors and re-run this script.
Remove the upgrade restriction. For example, clear an incomplete deployment, or upgrade an unsupported NE to a release that the new software supports.
5. Run the script again; go to substep 1.

Verify database archive log synchronization

9

If the system is redundant, ensure that no archive log gap exists between the primary and standby main databases.

Note: If you attempt a database upgrade when an archive log gap exists, the upgrade fails.
1. Open an NFM-P GUI client.
2. View the Standby DB entry in the GUI status bar.
3. If the entry reads “Database archive log gap”, you must reinstantiate the standby database. Otherwise, go to Step 10.
4. Choose Administration→System Information from the main menu. The System Information form opens.
5. Click Re-Instantiate Standby.
6. Click Yes to confirm the action. The reinstatement begins, and the GUI status bar displays reinstatement information.
   Note: Database reinstatement takes considerable time if the database contains a large amount of statistics data.
   You can also use the System Information form to monitor the reinstatement progress. The Last Attempted Standby Re-instantiation Time is the start time; the Standby Re-instantiation State changes from In Progress to Success when the reinstatement is complete.
7. When the reinstatement is complete, close the System Information form.

Back up database

10

Open an NFM-P GUI client.

11

Choose Administration→Database from the main menu. The Database Manager form opens.

12

Click on the Backup tab.
CAUTION

Service Disruption

The disk partition that is to contain the database backup must have sufficient space for the database backup file set.

Ensure that the backup directory is at least five times as large as the expected database backup size. For more information, contact technical support or see the NFM-P Planning Guide.

CAUTION

Data Loss

Before the NFM-P performs a database backup, it deletes the contents of the specified backup directory.

Ensure that the backup directory that you specify does not contain files that you need to retain.

CAUTION

Data Loss

The backup directory that you specify must not include the main database installation directory, or data loss may occur.

Ensure that the directory path does not include /opt/nsp/nfmp/db.

Note: The backup directory that you specify must be a directory on a local mounted partition.

Note: The Oracle management user requires read and write permissions on the backup directory.

Note: In an NSP system that does not include the NSD and NRC module, a GUI-based main database backup operation also backs up the local Neo4j and PostgreSQL databases. The Neo4j and PostgreSQL backup files may be required in the event that the upgrade fails and is to be rolled back.

Configure the following parameters:

• Manual Backup Directory

• Enable Backup File Compression

Click Full Backup.

Click Yes. The database backup begins, and the Backup State indicator reads In Progress.
Depending on the database size, a backup may take considerable time.

Monitor the Backup State indicator, which is dynamically updated. The indicator displays Success when the backup is complete.

When the backup is complete, close the Database Manager (Edit) form.

Transfer the backup file set to a secure location on a separate station that is unaffected by the upgrade activity.

### Back up Analytics report repository

If you are upgrading from Release 18.3 or earlier and the NFM-P system includes one or more NFM-P analytics servers, preserve the saved report results, if required.

An NFM-P analytics server upgrade preserves only the most recent 5000 saved report results, which are listed in the Results folder of the NFM-P Analytics application. If you suspect that the number of saved report results exceeds 5000, and you want to preserve the results, perform the following steps.

1. Perform Step 3 to Step 14 of 10.13 “To upgrade the NFM-P analytics servers” (p. 449) on one analytics server station.

2. Enter the following:

   ```bash
   ./AnalyticsAdmin.sh checkoracledb
   ```

   The script displays the following:

   Checking number of Analytics report results in the Oracle repository

   If the number of report results in the repository is less than 5000, the following is displayed:

   Number of Reports [ nnnn ] in Oracle Database is less than 5000. All Reports will be exported/upgraded.

   If the number of report results in the repository is greater than 5000, the following is displayed:

   Number of Reports [ nnnn ] in Oracle Database is greater than 5000. If you wish to save reports older than the most recent 5000, please download them to a secure location now before proceeding with the Analytics server upgrade.

   Only the most recent 5000 report results will be exported/upgraded

3. If the number of report results is greater than 5000, and you want to preserve results that
are older than the most recent 5000, use the Export function in the NFM-P Analytics application to transfer the older results to a secure location.

**Back up custom configuration files**

---

**CAUTION**

**Service Disruption**

An NFM-P upgrade does not preserve all non-default settings in configuration files such as *nms-server.xml*.

If an NFM-P configuration file contains non-default settings that you want to retain after an upgrade, contact technical support for assistance before the upgrade.

**Note:** At the beginning of an NFM-P main or auxiliary server upgrade, specific configuration and log files are copied to a directory under the installation directory; the directory name includes a timestamp. The directories below the main server installation directory are then deleted. If you have created or customized a file below the main server installation directory, you risk losing the file unless you create a backup copy.

Make a backup copy of each file that you have created or customized in or below the */opt/nsp/nfmp/server* directory on each main server station, and store the backup files on a separate station that is not affected by the NFM-P upgrade activity.

**Back up Release 17.6 security statement**

The security statement on the NSP sign-in page is not preserved during an upgrade from Release 17.6. If you are upgrading from Release 17.6 and your NSP sign-in page has a proprietary security statement that you want to preserve, perform the following steps.

1. Open the NSP Launchpad as the admin user.
2. Click More→Settings.
3. Record the Security Statement text in a location that is not affected by the upgrade activity.
4. Close the NSP Launchpad.

**Verify compatibility with external systems**

Ensure that the new NFM-P software is compatible with the software release of each external system that connects to the NFM-P. Contact technical support for information about external system compatibility.
Close LogViewer

23

Close the LogViewer utility, if it is open.

Validate main server and GUI client firewall configuration

24

Confirm that the firewalls between the main servers and the single-user GUI clients and client delegate servers allow traffic to the HTTP or HTTPS port required for client access. Otherwise, you cannot install or upgrade a single-user client or client delegate server.

See the *NSP NFM-P Planning Guide* for NFM-P port assignment information.

Verify NFM-P policy compatibility with managed NEs

25

You must confirm that the new NFM-P release supports the software release of each managed NE and pre-provisioned NE, as stated in the *NSP NFM-P and 5620 SAM Network Element Compatibility Guide*. Perform one of the following for each NE that is at an unsupported release.

- **Note:** If the system that you are upgrading manages an NE as a GNE, and the new NFM-P release supports native management of the device type and release, you must unmanage and delete the GNE before you attempt the upgrade. After the upgrade, the NFM-P can discover and manage the device as a native NE instead of a GNE.

  a. Upgrade the device software to a release that the new NFM-P software supports; see the appropriate device documentation and the *NSP NFM-P User Guide* for information about performing NE software upgrades.

  b. Remove the NE from the NFM-P managed network; see the “Discovering devices using the NFM-P” chapter of the *NSP NFM-P User Guide* for information.

    1. Unmanage the NE.
    2. Delete the NE from the managed network.
    3. Administratively disable or remove the discovery rule element for the NE.

  c. Delete the pre-provisioned NE using the NFM-P Pre-Provisioned NE Manager; see the “Self-configuration and discovery” chapter of the *NSP NFM-P LTE RAN User Guide*.

Clear CPAM checkpoints

26

An NFM-P main server upgrade requires additional time if CPAM checkpoints are retained. The additional time varies, depending on the platform resources, managed network size, and checkpoint schedule. To reduce the upgrade time, remove the CPAM checkpoints, as described in the *NSP NFM-P Control Plane Assurance Manager User Guide*. 
Gather required information

27
Choose Administration→System Information from the main menu. The System Information form opens.

28
Record the following information:
• Domain Name
• Primary Server panel:
  − IP Address
  − Host Name
  − Status
• Primary Database Server panel:
  − Database Name
  − Instance Name
  − IP Address
  − Host Name

29
If the system is redundant, record the following additional information:
• Standby Server panel:
  − IP Address
  − Host Name
  − Status
• Standby Database Server panel:
  − Database Name
  − Instance Name
  − IP Address
  − Host Name

30
If the system includes one or more auxiliary servers, click on the Auxiliary Services tab. A list of auxiliary servers is displayed. Otherwise, go to Step 33.

31
Perform the following steps for each auxiliary server listed on the form.
1. Select the auxiliary server and click Properties. The auxiliary server properties form opens.
2. Record the following information for use during the upgrade:
   • Host Name
   • Auxiliary Server Type
   • Server Status
3. Close the auxiliary server properties form.

32

Record which auxiliary servers have a check mark in the Selected column.

Note: In 10.9 "To upgrade a redundant NFM-P system" (p. 406), the Selected auxiliary servers are collectively referred to as [Aux1]; the remaining auxiliary servers are collectively referred to as [Aux2].

33

If the system includes one or more client delegate servers, click on the Client Delegate Servers tab. Otherwise, go to Step 35.

34

Perform the following steps for each client delegate server listed on the form:

1. Select the client delegate server and click Properties. The client delegate server properties form opens.
2. Record the IP Address value for use during the upgrade.
3. Close the properties form.

35

Close the System Information form.

36

Obtain and record the following additional information for each main server:

- root user password
- nsp user password
- additional IP addresses, if NAT or multiple interfaces are used:
  - IP address that each main database must use to reach the main server
  - IP address that the GUI and XML API clients must use to reach the main server; the public IP address, if NAT is used
  - IP address that the auxiliary servers must use to reach the main server
  - private IP address, if NAT is used

37

Obtain and record the following additional main database information:

- root user password
- Oracle management user information:
  - username; installation default is oracle
  - password
• group name; installation default is dba
• Oracle database user information:
  − username; installation default is samuser
  − password
• Oracle SYS user password
• additional database IP addresses, if NAT or multiple interfaces are used:
  − IP address that each main server must use to reach the database
  − IP address that each auxiliary server must use to reach the database

Close client sessions

38

Close the open GUI and XML API client sessions, as required.
1. Open a GUI client using an account with security management privileges, such as admin.
3. Click on the Sessions tab.
4. Click Search. The form lists the open GUI and XML API client sessions.
5. Identify the GUI session that you are using based on the value in the Client IP column.
6. Select all sessions except for the following:
  • the session that you are using
  • the sessions required to monitor the network during a redundant system upgrade
7. Click Close Session.
8. Click Yes to confirm the action.
9. Click Search to refresh the list and verify that only the required sessions are open.

Uninstall Mac OS X clients

39

A Mac OS X single-user client upgrade from NFM-P Release 17 is not supported.

Uninstall each NFM-P Release 17 single-user client installed on Mac OS X.

Note: You are directed to install the new Mac OS X client software at the end of the system upgrade procedure.
Close GUI client

If the GUI client that you are using is not required for network monitoring during the upgrade, close the client.

END OF STEPS

10.4 To apply an NSP RHEL qcow2 OS update

10.4.1 Description

If you are upgrading an NFM-P component in a VM created using the NSP RHEL OS qcow2 image described in 4.8 “To deploy the RHEL OS for NFM-P using a qcow2 image” (p. 47), you must apply a RHEL update to the OS before you can upgrade the component.

Note: The procedure applies only to a VM OS deployed using the NSP RHEL OS qcow2 image.

Note: If required, you can roll back an applied update by using the ‘yum history’ command to do the following.

1. Obtain the yum transaction ID.
2. Undo the transaction.
   See the RHEL OS documentation for more information.

10.4.2 Steps

1
Stop the NFM-P component on the station, if it is running. See the appropriate NSP NFM-P System Administrator Guide procedure, as required.

2
Log in to the component station as the root user.

3
Open a console window.

4
Enter the following:

   # mkdir -p /opt/OSUpdate

5
Download the following compressed file for the new NFM-P release to the /opt/OSUpdate directory:
To apply an NSP RHEL qcow2 OS update

NSP_RHEL\textsubscript{n} QCOW2_UPDATE\_yy\_mm.tar.gz

where
\textit{n} is the major RHEL version, for example, 7
\textit{yy.mm} is the issue date of the OS update

6  Enter the following:
   \texttt{\# cd /opt/OSUpdate}

7  Enter the following to expand the downloaded file:
   \texttt{\# tar -zxvf NSP_RHEL\textsubscript{n} QCOW2_UPDATE\_yy\_mm.tar.gz}
   The update files are extracted to the following directory:
   /opt/OSUpdate/rhelversion-\textit{yy.mm.dd}
   where
   \textit{version} is the RHEL version, for example, 7.5
   \textit{yy.mm.dd} is the issue date of the OS update

8  Enter the following:
   \texttt{\# cd rhelversion-\textit{yy.mm.dd}}

9  Enter the following to install the update:
   \texttt{\# yum install *}

10 Enter the following:
    \texttt{\# systemctl reboot}
    The station reboots.

11 After the reboot, remove the /opt/OSUpdate directory to conserve disk space.

12 Applying the update may leave outdated and inactive OS kernel instances on the station.
   To remove any previous kernel instances, enter the following as the root user:
   \texttt{\# package-cleanup --oldkernels --count=1}
Close any open console windows.

END OF STEPS
Standalone NFM-P system upgrade

10.5 Standalone system upgrade workflow

10.5.1 Description
The following is the sequence of high-level actions required to upgrade a standalone NFM-P system.

10.5.2 Stages

Note: The links in the “Upgrade standalone system” (p. 383) stages lead to sections in 10.6 “To upgrade a standalone NFM-P system” (p. 385).

Prepare system for upgrade

1. Perform 10.3 “To perform the pre-upgrade tasks” (p. 369) to prepare for the upgrade.

Upgrade standalone system

2. If the system includes one or more NSP Flow Collectors or analytics servers, stop each; see “Stop analytics servers, NSP Flow Collectors” (p. 385).

3. Prepare the main server for the upgrade; see “Stop and disable standalone main server” (p. 386).
   1. Stop the main server.
   2. Disable automatic main server startup.

4. Upgrade the main database; see “Upgrade standalone main database” (p. 387).
   1. Stop the main database.
   2. Run a script on the database station to prepare for the Oracle software installation.
   3. Install the required packages.
   4. Run the database upgrade script.
   5. Verify and modify the database configuration, as required.

5. If the system includes one or more auxiliary servers, stop the auxiliary servers; see “Stop auxiliary servers” (p. 393).
6 Upgrade the main server; see “Upgrade standalone main server” (p. 393).

7 If the system includes one or more auxiliary servers, upgrade each auxiliary server; see “Upgrade auxiliary servers” (p. 396).

8 If the system includes one or more NSP Flow Collectors, upgrade each NSP Flow Collector; see “Upgrade NSP Flow Collectors” (p. 396).

9 If the system includes an auxiliary database, upgrade the auxiliary database; see “Upgrade auxiliary database” (p. 396).

10 If the system includes one or more auxiliary servers, start each auxiliary server; see “Start auxiliary servers” (p. 396).

11 Start the main server; see “Start main server” (p. 396).

12 If the system includes one or more analytics servers, upgrade each analytics server; see “Upgrade analytics servers” (p. 397).

13 Install or upgrade single-user GUI clients, as required; see “Install or upgrade single-user GUI clients” (p. 397).

14 Install or upgrade client delegate servers, as required; see “Install or upgrade client delegate servers” (p. 398).

15 If required, restore the Release 17.6 NSP sign-in page security statement; see “Restore Release 17.6 security statement” (p. 398).

16 If you are using a PKI server to deploy TLS, stop the PKI server; see “Stop PKI server” (p. 398).
If the NFM-P system has customized TLS version and cipher support, restore the custom TLS support settings; see “Restore TLS version and cipher support configuration” (p. 398).

Configure and enable firewalls, if required; see “Configure and enable firewalls” (p. 398).

10.6 To upgrade a standalone NFM-P system

10.6.1 Description

The following steps describe how to upgrade a collocated or distributed main database and main server in a standalone deployment. The steps include links to procedures for installing and upgrading optional NFM-P components.

Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

Note: You require the following user privileges:
  • on each server station in the system — root, nsp
  • on the main database station — root, database_user

Note: The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:
  • # — root user
  • bash$ — nsp user

10.6.2 Steps

1. Open at least one GUI client to monitor the network before the upgrade.

Stop analytics servers, NSP Flow Collectors

2. If the system includes one or more analytics servers, stop each analytics server.
   1. Log in to the analytics server station as the nsp user.
   2. Open a console window.
   3. Enter the following:
      
      ```bash
      bash$ /opt/nsp/nfmp/analytics/bin/AnalyticsAdmin.sh stop
      ```

      The following is displayed:
      
      Stopping Analytics Server

      When the analytics server is completely stopped, the following message is displayed:
Analytics Server is not running

If the system includes one or more NSP Flow Collectors, stop each NSP Flow Collector.
1. Log in to the NSP Flow Collector station as the root user.
2. Open a console window.
3. Enter the following:
   
   ```bash
   # /opt/nsp/flow/dcp/bin/dcpctl.sh stop
   ```

   The command displays a series of status messages as the NSP Flow Collector stops.

   **Note:** To stop the NSP Flow Collector without displaying status messages, you can use the following command:

   ```bash
   # systemctl stop nsp-flow-collector.service
   ```

Stop and disable standalone main server

Stop the main server.
1. Log in to the main server station as the nsp user.
2. Open a console window.
3. Enter the following:
   
   ```bash
   cd /opt/nsp/nfmp/server/nms/bin
   ```

4. Enter the following:

   ```bash
   ./nmsserver.bash stop
   ```

5. Enter the following:

   ```bash
   ./nmsserver.bash appserver_status
   ```

   The server status is displayed; the server is fully stopped if the status is the following:

   **Application Server is stopped**

   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

Disable the automatic main server startup so that the main server does not start in the event of a power disruption during the upgrade.

1. Enter the following to switch to the root user:

   ```bash
   su -
   ```

2. Enter the following:

   ```bash
   # systemctl disable nfmp-main-config.service
   ```

3. Enter the following:

   ```bash
   # systemctl disable nfmp-main.service
   ```
Upgrade standalone main database

6

Log in to the database station as the root user.

7

Open a console window.

8

Stop and disable the Oracle proxy and main database services.
1. Enter the following to stop the Oracle proxy:
   # systemctl stop nfmp-oracle-proxy.service
2. Enter the following to disable the automatic Oracle proxy startup:
   # systemctl disable nfmp-oracle-proxy.service
3. Enter the following to stop the main database:
   # systemctl stop nfmp-main-db.service
4. Enter the following to disable the automatic database startup:
   # systemctl disable nfmp-main-db.service

9

If the main database is deployed in a VM created using the NSP RHEL qcow2 image, perform the following steps.
1. Perform 10.4 "To apply an NSP RHEL.qcow2 OS update" (p. 380) on the main database station.
2. Open the /etc/fstab file using a plain-text editor such as vi.
3. Locate the tmpfs file system entry.
4. Remove the noexec option so that the entry reads as follows:
   tmpfs /dev/shm tmpfs nodev,nosuid 0 0
5. Save and close the /etc/fstab file.
6. Enter the following to remount the /dev/shm partition:
   # mount -o remount /dev/shm

10

Perform one of the following.

a. If the main server and database are collocated on one station, perform the following steps.
   1. Transfer the following downloaded installation files to an empty directory on the main database station:
      • nsp-nfmp-oracle-R.r.p-rel.v.rpm
      • nsp-nfmp-main-db-R.r.p-rel.v.rpm
      • nsp-nfmp-nspos-R.r.p.rpm
1. In subsequent steps, the directory is called the NFM-P software directory.

2. If the NFM-P is to manage one or more LTE-N devices, transfer the following additional package to the directory:
   - nsp-nfmp-semvalidator-R.r.p-rel.v.rpm

b. If the main server and database are on separate stations, transfer the following downloaded installation files to an empty directory on the main database station:
   - nsp-nfmp-jre-R.r.p-rel.v.rpm
   - nsp-nfmp-config-R.r.p-rel.v.rpm
   - nsp-nfmp-oracle-R.r.p-rel.v.rpm
   - nsp-nfmp-main-db-R.r.p-rel.v.rpm

   **Note:** In subsequent steps, the directory is called the NFM-P software directory.

11. Transfer the following downloaded file to an empty directory on the main database station:
   - OracleSw_PreInstall.sh

12. Navigate to the directory that contains the OracleSw_PreInstall.sh file.

13. Enter the following:
   ```
   # chmod +x OracleSw_PreInstall.sh
   ```

14. Enter the following:
   ```
   # ./OracleSw_PreInstall.sh
   ```

   **Note:** A default value is displayed in brackets []. To accept the default, press ↵.

   **Note:** If you specify a value other than the default, you must record the value for use when the OracleSw_PreInstall.sh script is run during a software upgrade, or when the Oracle management user information is required by technical support.

   The following prompt is displayed:
   
   This script will prepare the system for an upgrade to NFM-P Version R.r Rn database.

   Do you want to continue? [Yes/No]:

   ```
Enter Yes. The following messages and prompt are displayed:

About to validate that the database can be upgraded to release.

Found the database installation directory /opt/nsp/nfmp/db/install.

Existing database version = version

Enter the password for the "SYS" Oracle user (terminal echo is off):

Enter the SYS user password.

The script begins to validate the database records, and displays the following:

Validating the database for upgrade. Please wait ...

If the validation is successful, the following messages and prompt are displayed:

INFO: Database upgrade validation passed.

Creating group group if it does not exist ...

Checking or Creating the Oracle user home directory /opt/nsp/nfmp/oracle12r1...

Checking user username...

usermod: no changes

Changing ownership of the directory /opt/nsp/nfmp/oracle12r1 to username:group.

About to unlock the UNIX user [username]

Unlocking password for user username.

passwd: Success

Unlocking the UNIX user [username] completed

Do you want to change the password for the UNIX user username? [Yes/No]:

Go to Step 18.

If the database contains an invalid item, for example, an NE at a release that the new NFM-P software does not support, the following is displayed and the script exits:

ERROR: Unsupported records found in database. Please remove the following unsupported items first:

Please remove the following unsupported items first:

item_1

item_2

.. 

item_n
ERROR: The database cannot be upgraded. Please fix the above errors and re-run this script.

Perform the following steps.
1. Use an NFM-P GUI client to remove or update the unsupported items, as required. For example, upgrade an unsupported NE to a release that the new software supports.
2. Run the script again; go to Step 14.

Perform one of the following.

a. Enter No to retain the current password.
b. Specify a new password.
   1. Enter Yes. The following prompt is displayed:
      New Password:
   2. Enter a password. The following prompt is displayed:
      Re-enter new Password:
   3. Re-enter the password. The following is displayed if the password change is successful:
      passwd: password successfully changed for username

The following message and prompt are displayed:
Specify whether an NFM-P server will be installed on this workstation.
The database memory requirements will be adjusted to account for the additional load.
Will the database co-exist with an NFM-P server on this workstation [Yes/No]:

Enter Yes or No, as required.
Messages like the following are displayed as the script execution completes:
INFO: About to remove kernel parameters set by a previous run of this script from /etc/sysctl.conf
INFO: Completed removing kernel parameters set by a previous run of this script from /etc/sysctl.conf
INFO: About to set kernel parameters in /etc/sysctl.conf...
INFO: Completed setting kernel parameters in /etc/sysctl.conf...
INFO: About to change the current values of the kernel parameters
INFO: Completed changing the current values of the kernel parameters
INFO: About to remove ulimit parameters set by a previous run of this script from /etc/security/limits.conf
INFO: Completed removing ulimit parameters set by a previous run of this script from /etc/security/limits.conf
INFO: About to set ulimit parameters in etc/security/limits.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.conf...
INFO: Completed running Oracle Pre-Install Tasks

20
When the script execution is complete, enter the following to reboot the station:

```
# systemctl reboot
```

The station reboots.

21
When the reboot is complete, log in as the root user on the main database station.

22
Open a console window.

23
Navigate to the NFM-P software directory.

Note: Ensure that the directory contains only the installation files.

24
Enter the following:

```
# chmod +x *
```

25
Enter the following:

```
# yum install *.rpm
```

The yum utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

26
Enter y. The following and the installation status are displayed as each package is installed:

Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
The package installation is complete when the following is displayed:

Complete!

27

Enter the following to upgrade the database:

# samupgradeDb

The following prompt is displayed:

Enter the password for the "user" database user (terminal echo is off):

28

Enter the database user password.

The following is displayed as the database upgrade begins:

Validating...

Note: A database upgrade may take considerable time.

29

When the upgrade is complete, verify the database configuration.

1. Enter the following:

   # samconfig -m db

   The following is displayed:

   Start processing command line inputs...

   <db>

2. Enter the following:

   <db> show-detail

   The database configuration is displayed.

3. Review each parameter to ensure that the value is correct.

4. Configure one or more parameters, if required, and then enter back; see Chapter 3, “Using samconfig” for information about using the samconfig utility.

5. If you change one or more parameters, enter the following:

   <db> apply

   The configuration is applied.

6. Enter the following:

   <db> exit

   The samconfig utility closes.
It is recommended that as a security measure, you limit the number of database user login failures that the NFM-P allows before the database user account is locked; see “NFM-P database management procedures” in the NSP NFM-P System Administrator Guide.

Note: You do not need to perform the step if the database has been configured before the upgrade to limit the user login failures.

Stop auxiliary servers

If the system includes one or more auxiliary servers, stop each auxiliary server.
1. Log in to the auxiliary server station as the nsr user.
2. Open a console window.
3. Enter the following:
   ```bash
   /opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash auxstop
   ```
   The auxiliary server stops.

Upgrade standalone main server

Log in as the root user on the main server station.

Open a console window.

If the main server and database are on separate stations and deployed in VMs created using the NSP RHEL OS qcow2 image, perform 10.4 “To apply an NSP RHEL qcow2 OS update” (p. 380) on the main server station.

Perform one of the following.
a. If the main server and database are collocated on one station, go to step Step 41.
b. If the main server and database are on separate stations, transfer the following downloaded installation files to an empty directory on the main server station:
   - nsp-nfmp-nspos-R.rr.p.rpm
   - nsp-nfmp-jre-R.rr.p-rel.v.rpm
   - nsp-nfmp-config-R.rr.p-rel.v.rpm
   - nsp-nfmp-main-server-R.rr.p.rpm

Note: In subsequent steps, the directory is called the NFM-P software directory.
If the NFM-P is to manage one or more LTE-N devices, transfer the following additional package to the directory:

- nsp-nfmp-semvalidator-\(R_r.p\)-rel.v.rpm

Navigate to the NFM-P software directory.

**Note:** Ensure that the directory contains only the installation files.

Enter the following:

```bash
# chmod +x *
```

Enter the following:

```bash
# yum install *.rpm
```

The `yum` utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

Enter y. The following and the installation status are displayed as each package is installed:

- Downloading packages:
- Running transaction check
- Running transaction test
- Transaction test succeeded
- Running transaction

The package installation is complete when the following is displayed:

```
Complete!
```

Enter the following; see Chapter 3, “Using samconfig” for information about using `samconfig`:

**Note:** Regardless of whether you intend to modify the main server configuration, you must apply the main server configuration, as described in the following steps.

```bash
# samconfig -m main
```

The following is displayed:

```
Start processing command line inputs...
```
Enter the following:
<main> configure <br /></main>
The prompt changes to <main configure>.

To apply an NFM-P license, enter the following, and then enter back <br />:

Note: You cannot start a main server unless the main server configuration includes a current and valid license. You can use samconfig to specify the license file, or import the license, as described in “Software and license configuration procedures” in the NSP NFM-P System Administrator Guide.

<main configure> license license_file <br /></main>
where license_file is the absolute path and file name of the NSP license bundle

Verify the main server configuration.
1. Enter the following:
<main configure> show <br /></main>
The main server configuration is displayed.
2. Review each parameter to ensure that the value is correct.
3. Configure one or more parameters, if required; see Chapter 3, “Using samconfig” for information about using the samconfig utility.
4. When you are certain that the configuration is correct, enter the following:
<main configure> back <br /></main>
The prompt changes to <main>.

Enter the following:
<main> apply <br /></main>
The configuration is applied.

Enter the following:
<main> exit <br /></main>
The samconfig utility closes.
Upgrade auxiliary servers

47

If the system includes one or more auxiliary servers, perform 10.10 “To upgrade an NFM-P auxiliary server” (p. 435) on each auxiliary server station.

Note: Do not perform the final step that describes starting the auxiliary server.

Upgrade NSP Flow Collectors

48

If the system includes one or more NSP Flow Collectors, perform 10.11 “To upgrade an NSP Flow Collector” (p. 438) on each NSP Flow Collector station.

Upgrade auxiliary database

49

If the system includes an auxiliary database, perform 10.12 “To upgrade an NFM-P auxiliary database” (p. 441).

Start auxiliary servers

50

If the system includes one or more auxiliary servers, start each auxiliary server.

1. Log in to the auxiliary server station as the nsp user.
2. Open a console window.
3. Enter the following:

   bash$ /opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash auxstart

The auxiliary server starts.

Start main server

51

CAUTION

Service Disruption

An NFM-P system upgrade is not complete until each main server performs crucial post-upgrade tasks during initialization.

Before you attempt an operation that requires a server shutdown, you must ensure that each main server is completely initialized, or the operation fails.
Note: You cannot start a main server unless the main server configuration includes a current and valid license. You can use samconfig to specify the license file, or import a license, as described in “Software and license configuration procedures” in the NSP NFM-P System Administrator Guide.

Start the main server.
1. Enter the following to switch to the nsp user:
   
   `# su - nsp`

2. Enter the following:
   
   `bash$ cd /opt/nsp/nfmp/server/nms/bin`

3. Enter the following:
   
   `bash$ ./nmsserver.bash start`

4. Enter the following:
   
   `bash$ ./nmsserver.bash appserver_status`

   The server status is displayed; the server is fully initialized if the status is the following:

   Application Server process is running. See nms_status for more detail.

   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

If the NFM-P is to manage wireless NEs, enter the following to update the memory configuration accordingly for GUI clients:

`bash$ ./nmsdeploytool.bash clientmem -l`

Close the console window.

Upgrade analytics servers

If the system includes one or more analytics servers, perform 10.13 “To upgrade the NFM-P analytics servers” (p. 449) to upgrade each analytics server.

Install or upgrade single-user GUI clients

As required, perform the following to install or upgrade single-user GUI clients:

- 14.4 “To install a single-user GUI client” (p. 564)
- 14.5 “To upgrade an NFM-P Release 17 or 5620 SAM single-user GUI client” (p. 569)
Install or upgrade client delegate servers

As required, perform the following to install or upgrade client delegate servers:

- 15.3 “To install a client delegate server” (p. 584)
- 15.5 “To upgrade an NFM-P Release 17 or 5620 SAM client delegate server” (p. 596)

Restore Release 17.6 security statement

If you are upgrading from Release 17.6 and recorded the NSP sign-in page security statement in Step 21 of 10.3 “To perform the pre-upgrade tasks” (p. 369), perform the following steps.

1. Open the NSP Launchpad as the admin user.
2. Click More → Settings.
3. Enter the security statement text in the Security Statement field.
4. Close the NSP Launchpad.

Stop PKI server

If you are deploying TLS using an NSP PKI server, stop the PKI server, as described at the end of 6.7 “To configure and enable an NSP PKI server” (p. 91).

Restore TLS version and cipher support configuration

An NFM-P system upgrade does not preserve your changes to the system support for specific TLS versions and ciphers.

If the system had customized TLS settings before the upgrade, perform “To update the supported NFM-P TLS versions and ciphers” in the NSP NFM-P System Administrator Guide to restore the TLS version and cipher support settings.

Configure and enable firewalls

If you intend to use any firewalls between the NFM-P components, and the firewalls are disabled, configure and enable each firewall.

Perform one of the following.

a. Configure each external firewall to allow the required traffic using the port assignments in the NSP NFM-P Planning Guide, and enable the firewall.

b. Configure and enable Firewalld on each component station, as required.
1. Use an NFM-P template to create the Firewalld rules for the component, as described in the NSP NFM-P Planning Guide.
2. Log in to the station as the root user.
3. Open a console window.
4. Enter the following:
   ```
   # systemctl enable firewalld
   ```
5. Enter the following:
   ```
   # systemctl start firewalld
   ```
6. Close the console window.
Redundant NFM-P system upgrade

10.7 Component references

10.7.1 Description

CAUTION

Service Disruption

A redundant NFM-P system upgrade involves a network management outage.

Ensure that you perform the upgrade during a scheduled maintenance period of sufficient duration to accommodate the outage.

During a redundant NFM-P system upgrade, the primary and standby roles of the main servers and databases reverse, as do the Preferred and Reserved auxiliary server roles. As a result, the use of relative component identifiers such as primary and standby can cause confusion.

To clearly identify components during a redundant system upgrade, you can use the figure below. The components on the left manage the network before the upgrade, and the components on the right manage the network after the upgrade. Each component in the figure has an absolute identifier in brackets, for example, [DB1], that clearly identifies the component in the redundant system upgrade workflow and procedure steps.
10.8 Redundant system upgrade workflow

10.8.1 Description

The following is the sequence of high-level actions required to upgrade a redundant NFM-P system.

10.8.2 Stages

**Note:** The links in the “Upgrade redundant system” (p. 402) stages lead to sections in 10.9 “To upgrade a redundant NFM-P system” (p. 406).

Prepare system for upgrade

1. Perform 10.3 “To perform the pre-upgrade tasks” (p. 369) to prepare the NFM-P system for the upgrade.
Upgrade redundant system

2
Stop and disable the standby main server; see "Stop and disable standby main server [Main2]" (p. 406).

3
If the system includes auxiliary servers, stop the [Aux2] auxiliary servers; see "Stop auxiliary servers [Aux2]" (p. 407).

4
Disable the system redundancy functions; see "Disable database redundancy" (p. 407).

5
Upgrade the standby main database, which becomes the new primary main database; see "Upgrade standby main database [DB2]" (p. 408).
1. Stop the main database.
2. Run a script on the database station to prepare for the Oracle software installation.
3. Install the database packages.
4. Run the database upgrade script.
5. Verify and modify the database configuration, as required.

6
Upgrade the standby main server; see "Upgrade standby main server [Main2]" (p. 415).

7
If the NFM-P system includes one or more fNSP Flow Collectors or analytics servers, stop each; see "Stop analytics servers, NSP Flow Collectors" (p. 417).

8
If the NFM-P system includes auxiliary servers, upgrade the [Aux2] auxiliary servers; see "Upgrade auxiliary servers [Aux2]" (p. 418).

9
Stop and disable the original primary main server; see "Stop and disable original primary main server [Main1]" (p. 418).

Note: This stage marks the beginning of the network management outage.

10
If the system includes one or more NSP Flow Collectors, upgrade each NSP Flow Collector; see "Upgrade NSP Flow Collectors" (p. 419).
If the NFM-P system includes auxiliary servers, stop the [Aux1] auxiliary servers; see “Stop auxiliary servers [Aux1]” (p. 419).

If the NFM-P system includes an auxiliary database, upgrade the auxiliary database; see “Upgrade auxiliary database” (p. 419).

Stop the original primary main database; see “Stop original primary main database [DB1]” (p. 419).

Start the new primary main server; see “Start new primary main server [Main2]” (p. 420).

If the system includes auxiliary servers, start the [Aux2] auxiliary servers; see “Start auxiliary servers [Aux2]” (p. 421).

If the system includes one or more analytics servers, upgrade each analytics server; see “Upgrade analytics servers” (p. 421).

Upgrade or install at least one NFM-P single-user client or client delegate server; see “Enable GUI client” (p. 422).

Note: This stage marks the end of the network management outage.

Perform sanity testing on the NFM-P system using a GUI client; see “Test upgraded system using GUI client” (p. 422).

If required, restore the Release 17.6 NSP sign-in page security statement; see “Restore Release 17.6 security statement” (p. 422).

Uninstall the original primary main database; see “Uninstall original primary database [DB1]” (p. 422).

Install the new standby main database; see “Install new standby main database [DB1]” (p. 422).
1. Stop the main database.
2. Run a script to prepare for the Oracle software installation.
3. Install the database packages.
4. Configure the standby database.
5. Verify and modify the database configuration, as required.

22
Reinstantiate the standby database; see "Reinstantiate standby database" (p. 428).

23
Upgrade the original primary main server as the new standby main server; see "Upgrade original primary main server [Main1]" (p. 429).

24
Start the new standby main server; see "Start new standby main server [Main1]" (p. 431).

25
If the system includes auxiliary servers, upgrade the [Aux1] auxiliary servers; see "Upgrade auxiliary servers [Aux1]" (p. 432).

26
If the system includes auxiliary servers, start the [Aux1] auxiliary servers; see "Start auxiliary servers [Aux1]" (p. 432).

27
Install or upgrade single-user GUI clients, as required; see "Install or upgrade single-user GUI clients" (p. 432).

28
Install or upgrade client delegate servers, as required; see "Install or upgrade client delegate servers" (p. 433).

29
If you are using a PKI server to deploy TLS, stop the PKI server; see "Stop PKI server" (p. 433).

30
If the 5620 SAM system has customized TLS version and cipher support, restore the custom TLS support settings; see "Restore TLS version and cipher support configuration" (p. 433).

31
Configure and enable firewalls, if required; see "Configure and enable firewalls" (p. 433).
10.8.3 Concurrent task execution

Some system upgrade operations require considerable time. To reduce the duration of a redundant system upgrade, you can perform some actions concurrently.

The following table lists the redundant system upgrade workflow tasks in a format that involves two operators, A and B, who perform tasks concurrently when possible.

Table 10-1 Workflow for concurrent task execution during redundant upgrade

<table>
<thead>
<tr>
<th>System redundancy mode</th>
<th>Operator A actions</th>
<th>Operator B actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>DUPLEX</td>
<td>Stage 1 — Actions described in 10.3 “To perform the pre-upgrade tasks” (p. 369)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Stage 2 — “Stop and disable standby main server [Main2]” (p. 406)</td>
<td>Stage 3 — “Stop auxiliary servers [Aux2]” (p. 407)</td>
</tr>
<tr>
<td></td>
<td>Stage 4 — “Disable database redundancy” (p. 407)</td>
<td></td>
</tr>
<tr>
<td>SIMPLEX</td>
<td>Stage 5 — “Upgrade standby main database [DB2]” (p. 408)</td>
<td>Stage 6 — “Upgrade standby main server [Main2]” (p. 415)</td>
</tr>
<tr>
<td></td>
<td>Stage 7 — “Stop analytics servers, NSP Flow Collectors” (p. 417)</td>
<td>Stage 8 — “Upgrade auxiliary servers [Aux2]” (p. 418)</td>
</tr>
<tr>
<td>OUTAGE</td>
<td>Stage 9 — “Stop and disable original primary main server [Main1]” (p. 418)</td>
<td>Stage 10 — “Upgrade NSP Flow Collectors” (p. 419)</td>
</tr>
<tr>
<td></td>
<td>Stage 11 — “Stop auxiliary servers [Aux1]” (p. 419)</td>
<td>Stage 12 — “Upgrade auxiliary database” (p. 419)</td>
</tr>
<tr>
<td></td>
<td>Stage 13 — “Stop original primary main database [DB1]” (p. 419)</td>
<td>Stage 15 — “Start auxiliary servers [Aux2]” (p. 421)</td>
</tr>
<tr>
<td></td>
<td>Stage 14 — “Start new primary main server [Main2]” (p. 420)</td>
<td>Stage 16 — “Upgrade analytics servers” (p. 421)</td>
</tr>
<tr>
<td></td>
<td>Note: The outage persists until device discovery completes.</td>
<td></td>
</tr>
<tr>
<td>SIMPLEX</td>
<td>Stage 17 — “Enable GUI client” (p. 422)</td>
<td>Stage 20 — “Uninstall original primary database [DB1]” (p. 422)</td>
</tr>
<tr>
<td></td>
<td>Stage 18 — “Test upgraded system using GUI client” (p. 422)</td>
<td>Stage 21 — “Install new standby main database [DB1]” (p. 422)</td>
</tr>
<tr>
<td></td>
<td>Stage 19 — “Restore Release 17.6 security statement” (p. 422)</td>
<td>Stage 22 — “Reinstantiate standby database” (p. 428)</td>
</tr>
<tr>
<td></td>
<td>Stage 20 — “Uninstall original primary database [DB1]” (p. 422)</td>
<td>Stage 23 — “Upgrade original primary main server [Main1]” (p. 429)</td>
</tr>
</tbody>
</table>

Note: The outage persists until device discovery completes.
Table 10-1  Workflow for concurrent task execution during redundant upgrade  (continued)

<table>
<thead>
<tr>
<th>System redundancy mode</th>
<th>Operator A actions</th>
<th>Operator B actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>DUPLICLEX</td>
<td>Stage 24 — “Start new standby main server [Main1]” (p. 431)</td>
<td>Stage 25 — “Upgrade auxiliary servers [Aux1]” (p. 432)</td>
</tr>
<tr>
<td>DUPLICLEX</td>
<td>Stage 26 — “Start auxiliary servers [Aux1]” (p. 432)</td>
<td>Stage 28 — “Install or upgrade client delegate servers” (p. 433)</td>
</tr>
<tr>
<td>DUPLICLEX</td>
<td>Stage 27 — “Install or upgrade single-user GUI clients” (p. 432)</td>
<td>Stage 29 — “Stop PKI server” (p. 433)</td>
</tr>
<tr>
<td>DUPLICLEX</td>
<td>Stage 31 — “Configure and enable firewalls” (p. 433)</td>
<td>Stage 30 — “Restore TLS version and cipher support configuration” (p. 433)</td>
</tr>
</tbody>
</table>

10.9  To upgrade a redundant NFM-P system

10.9.1 Description

The following steps describe how to upgrade a collocated or distributed main database and main server in a redundant deployment. The steps include links to procedures for installing and upgrading optional NFM-P components.

Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

$i$ Note: You require the following user privileges:
- on each server station in the system — root, nsp
- on each main database station — root

$i$ Note: The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:
- # — root user
- bash$ — nsp user

10.9.2 Steps

Stop and disable standby main server [Main2]

1. Open a GUI client to monitor the network during the upgrade.

2. Stop the standby main server.
   1. Log in to the standby main server station as the nsp user.
   2. Open a console window.
3. Enter the following:
   
   bash$ cd /opt/nsp/nfmp/server/nms/bin

4. Enter the following:
   
   bash$ ./nmsserver.bash stop

5. Enter the following:
   
   bash$ ./nmsserver.bash appserver_status

   The server status is displayed; the server is fully stopped if the status is the following:
   
   Application Server is stopped

   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform
   the next step until the server is fully stopped.

3

Disable the automatic main server startup so that the main server does not start in the event of
a power disruption during the upgrade.

1. Enter the following to switch to the root user:
   
   bash$ su -

2. Enter the following:
   
   # systemctl disable nfmp-main-config.service

3. Enter the following:
   
   # systemctl disable nfmp-main.service

Stop auxiliary servers [Aux2]

4

If the NFM-P system includes auxiliary servers, stop each appropriate auxiliary server [Aux2].

1. Log in to the auxiliary server station as the nsp user.
2. Open a console window.
3. Enter the following:
   
   bash$ /opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash auxstop

   The auxiliary server stops.

Disable database redundancy

5

Disable the main database failover and switchover functions.

1. Log in to the primary main server station [Main1] as the nsp user.
2. Open a console window.
3. Enter the following to navigate to the main server configuration directory:
   
   bash$ cd /opt/nsp/nfmp/server/nms/config
5. Open the nms-server.xml file with a plain-text editor, for example, vi.
6. Locate the section that begins with the following tag:
   ```xml
   <db
   ```
7. Locate the following line in the section:
   ```xml
   host="address"
   ```
8. Ensure that the `address` value in the line is the IP address of main database [DB1].
9. Locate the following line in the section:
   ```xml
   database="instance_name"
   ```
10. Ensure that the `instance_name` value is the instance name of main database [DB1].
11. Edit the following line in the section that reads:
    ```bash
    redundancyEnabled="true"
    ```
    to read:
    ```bash
    redundancyEnabled="false"
    ```
12. Save and close the nms-server.xml file.
13. Enter the following:
    ```bash
    bash$ /opt/nsP/server/nms/bin/nmsserver.bash read_config
    ```
    The main server puts the change into effect, and database redundancy is disabled.

### Upgrade standby main database [DB2]

6. Log in to the standby main database [DB2] station as the root user.

   **Note:** After the upgrade, the station is the new primary main database station.

7. Open a console window.

8. Stop and disable the Oracle proxy and main database services.
   1. Enter the following to stop the Oracle proxy:
      ```bash
      # systemctl stop nfmp-oracle-proxy.service
      ```
   2. Enter the following to disable the automatic Oracle proxy startup:
      ```bash
      # systemctl disable nfmp-oracle-proxy.service
      ```
   3. Enter the following to stop the main database:
      ```bash
      # systemctl stop nfmp-main-db.service
      ```
   4. Enter the following to disable the automatic database startup:
      ```bash
      # systemctl disable nfmp-main-db.service
      ```
If analytics aggregations are enabled, perform the following steps to disable all aggregation rules.

**Note:** Disabling analytics aggregation during a redundant system upgrade prevents the duplication of aggregation data in the NFM-P database, but does not cause the loss of any aggregation data.

Upon startup, if a primary main server detects that the most recent aggregation data is not current, the server performs the interim aggregations. If aggregation is enabled during a redundant upgrade, the original primary main server creates aggregations while the standby main server is upgraded. In such a case, after the standby main server starts as the new primary main server, the server may perform aggregations that are duplicates of the aggregations performed by the original primary main server.

The required aggregation rules are automatically enabled on the new primary main server, so the server performs the interim aggregations upon startup. If aggregation is disabled at the start of a redundant upgrade, no aggregation duplication occurs.

1. Open an NFM-P GUI client.
2. Choose Tools→Analytics→Aggregation Manager from the NFM-P main menu. The Aggregation Manager form opens.
3. Click Search. The aggregation rules are listed.
4. Click on the Enable Aggregation column to sort the rules so that the rules that have aggregation enabled are at the top of the list.
5. Select all rules that have a check mark in the Enable Aggregation column.
7. Deselect Enable Aggregation.
8. Click OK. The Aggregation Rule (multiple instances) [Edit] form closes.
9. Click OK to save your changes and close the Aggregation Manager form.
10. Close the NFM-P GUI client.

If the standby main database is deployed in a VM created using the NSP RHEL OS qcow2 image, perform the following steps on the standby main database [DB2] station.

1. Perform 10.4 "To apply an NSP RHEL qcow2 OS update" (p. 380).
2. Open the /etc/fstab file using a plain-text editor such as vi.
3. Locate the tmpfs file system entry.
4. Remove the noexec option so that the entry reads as follows:
   
   ```
   tmpfs /dev/shm tmpfs nodev,nosuid 0 0
   ```
5. Save and close the /etc/fstab file.
6. Enter the following to remount the /dev/shm partition:
   
   ```
   # mount -o remount /dev/shm
   ```
Perform one of the following.

a. If the main server and database are collocated on one station, perform the following steps.
   1. Transfer the following downloaded installation files to an empty directory on the main database station:
      • nsp-nfmp-oracle-R.r.p-rel.v.rpm
      • nsp-nfmp-main-db-R.r.p-rel.v.rpm
      • nsp-nfmp-nspos-R.r.p.rpm
      • nsp-nfmp-jre-R.r.p-rel.v.rpm
      • nsp-nfmp-config-R.r.p-rel.v.rpm
      • nsp-nfmp-main-server-R.r.p.rpm

      Note: In subsequent steps, the directory is called the NFM-P software directory.
   2. If the NFM-P is to manage one or more LTE-N devices, transfer the following additional package to the directory:
      • nsp-nfmp-semvalidator-R.r.p-rel.v.rpm

b. If the main server and database are on separate stations, transfer the following downloaded installation files to an empty directory on the main database station:
   • nsp-nfmp-jre-R.r.p-rel.v.rpm
   • nsp-nfmp-config-R.r.p-rel.v.rpm
   • nsp-nfmp-oracle-R.r.p-rel.v.rpm
   • nsp-nfmp-main-db-R.r.p-rel.v.rpm

   Note: In subsequent steps, the directory is called the NFM-P software directory.

Transfer the following downloaded file to an empty directory on the main database station:
• OracleSw_PreInstall.sh

Navigate to the directory that contains the OracleSw_PreInstall.sh file.

Enter the following:
```
# chmod +x OracleSw_PreInstall.sh
d
```

Enter the following:
```
# ./OracleSw_PreInstall.sh
d
```

Note: A default value is displayed in brackets []. To accept the default, press <Enter>. 
Note: If you specify a value other than the default, you must record the value for use when the OracleSw_PreInstall.sh script is run during a software upgrade, or when the Oracle management user information is required by technical support.

The following prompt is displayed:

This script will prepare the system for an upgrade to NFM-P Version R.r Rn.
Do you want to continue? [Yes/No]:

16

Enter Yes. The following messages and prompt are displayed:

About to validate that the database can be upgraded to release.
Found the database installation directory /opt/nsp/nfmp/db/install.
Existing database version = version
Enter the password for the "SYS" Oracle user (terminal echo is off):

17

Enter the SYS user password.
The script begins to validate the database records, and displays the following:
Validating the database for upgrade. Please wait ...

If the validation is successful, the following messages and prompt are displayed:
INFO: Database upgrade validation passed.
Creating group group if it does not exist ...
Checking or Creating the Oracle user home directory
/opt/nsp/nfmp/oracle12r1...
Checking user username... usermod: no changes
Changing ownership of the directory /opt/nsp/nfmp/oracle12r1 to username:group.
About to unlock the UNIX user [username]
Unlocking password for user username.
passwd: Success
Unlocking the UNIX user [username] completed
Do you want to change the password for the user username? [Yes/No]:

Goto Step 19.

18

If the database contains an invalid item, for example, an NE at a release that the new NFM-P software does not support, the following is displayed and the script exits:

ERROR: Unsupported records found in database. Please remove the following unsupported items first:
Please remove the following unsupported items first:
ERROR: The database cannot be upgraded. Please fix the above errors and re-run this script.

Perform the following steps.
1. Use an NFM-P GUI client to remove or update the unsupported items, as required. For example, upgrade an unsupported NE to a release that the new software supports.
2. Run the script again; go to Step 15.

Perform one of the following.

a. Enter No to retain the current password.
b. Specify a new password.
   1. Enter Yes. The following prompt is displayed:
      
      New Password:
   2. Enter a password. The following prompt is displayed:
      
      Re-enter new Password:
   3. Re-enter the password. The following is displayed if the password change is successful:
      
      passwd: password successfully changed for user

The following message and prompt are displayed:
Specify whether an NFM-P server will be installed on this workstation.
The database memory requirements will be adjusted to account for the additional load.
Will the database co-exist with an NFM-P server on this workstation [Yes/No]:

Enter Yes or No, as required.
Messages like the following are displayed as the script execution completes:
INFO: About to remove kernel parameters set by a previous run of this script from /etc/sysctl.conf
INFO: Completed removing kernel parameters set by a previous run of this script from /etc/sysctl.conf
INFO: About to set kernel parameters in /etc/sysctl.conf...
INFO: Completed setting kernel parameters in /etc/sysctl.conf...
INFO: About to change the current values of the kernel parameters
INFO: Completed changing the current values of the kernel parameters
INFO: About to remove ulimit parameters set by a previous run of this script from /etc/security/limits.conf
INFO: Completed removing ulimit parameters set by a previous run of this script from /etc/security/limits.conf
INFO: About to set ulimit parameters in etc/security/limits.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.conf...
INFO: Completed running Oracle Pre-Install Tasks

When the script execution is complete, enter the following to reboot the main database station:
#
# systemctl reboot  

The station reboots.

When the reboot is complete, log in to the main database [DB2] station as the root user.

Open a console window.

Navigate to the NFM-P software directory.

Note: Ensure that the directory contains only the installation files.

Enter the following:
#
# chmod +x *  

Enter the following:
#
# yum install *.rpm  

The yum utility resolves any package dependencies, and displays the following prompt:
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:

Enter y. The following and the installation status are displayed as each package is installed:
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction

The package installation is complete when the following is displayed:
Complete!

Enter the following to upgrade the database:

```bash
# samupgradeDb
```

The following prompt is displayed:

Enter the password for the "user" database user (terminal echo is off):

Enter the database user password.
The following is displayed as the database upgrade begins:
Validating...

**Note:** A database upgrade may take considerable time.

Verify the database configuration and create the database.

**Note:** This main database [DB1] is the new primary main database.

1. Enter the following:
   ```bash
   # samconfig -m db
   ```
   The following is displayed:
   Start processing command line inputs...
   `<db>`

2. Enter the following:
   ```bash
   <db> show-detail
   ```
   The database configuration is displayed.

3. Review each parameter to ensure that the value is correct.

4. Configure one or more parameters, if required, and then enter `back`;
   see Chapter 3, "Using samconfig" for information about using the samconfig utility.

5. Enter the following to apply the configuration and create the database:
   ```bash
   <db> apply
   ```
   The configuration is applied, and the database creation begins.
6. When the database creation is complete, enter the following:

```
<db> exit
```

The samconfig utility closes.

**Upgrade standby main server [Main2]**

31

Log in as the root user on the main server [Main2] station.

ℹ️ **Note:** After the upgrade, the station is the new primary main server station.

32

If the standby main server and database are on separate stations, and the standby main server is deployed in a VM created using the NSP RHEL OS qcow2 image, perform 10.4 “To apply an NSP RHEL qcow2 OS update” (p. 380) on the standby main server [Main2] station.

33

Open a console window.

34

Perform one of the following.

a. If the main server and database are collocated on one station, go to Step 39.

b. If the main server and database are on separate stations, transfer the following downloaded installation files to an empty directory on the main server station:
   - nsp-nfmp-nspos-R.r.p.rpm
   - nsp-nfmp-jre-R.r.p-rel.v.rpm
   - nsp-nfmp-config-R.r.p-rel.v.rpm
   - nsp-nfmp-main-server-R.r.p.rpm

ℹ️ **Note:** In subsequent steps, the directory is called the NFM-P software directory.

35

If the NFM-P is to manage one or more LTE-N devices, transfer the following additional package to the directory:

- nsp-nfmp-semvalidator-R.r.p-rel.v.rpm

36

Enter the following:

```
# chmod +x *
```

37

Enter the following:
# yum install *.rpm

The `yum` utility resolves any package dependencies, and displays the following prompt:

Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:

Enter y. The following and the installation status are displayed as each package is installed:

Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction

The package installation is complete when the following is displayed:

Complete!

Enter the following; see Chapter 3, “Using samconfig” for information about using samconfig:

Note: Regardless of whether you intend to modify the main server configuration, you must apply the main server configuration, as described in the following steps.

# samconfig -m main

The following is displayed:

Start processing command line inputs...
<main>

Enter the following:
<main> configure

The prompt changes to <main configure>.

To apply a new or updated NFM-P license, enter the following, and then enter back:

Note: You cannot start a main server unless the main server configuration includes a current and valid license. You can use samconfig to specify the license file in this step, or later import the license, as described in “Software and license configuration procedures” in the NSP NFM-P System Administrator Guide.

<main configure> license license_file

where `license_file` is the path and file name of the NSP license bundle.
The prompt changes to <main configure>.

42

Verify the main server configuration.
1. Enter the following:
   
   <main configure> show
   
   The main server configuration is displayed.
2. Review each parameter to ensure that the value is correct.
3. Configure one or more parameters, if required; see Chapter 3, "Using samconfig" for information about using the samconfig utility.
4. When you are certain that the configuration is correct, enter the following:
   
   <main configure> back
   
   The prompt changes to <main>.

43

Enter the following:

<main> apply

The configuration is applied.

44

Enter the following:

<main> exit

The samconfig utility closes.

Stop analytics servers, NSP Flow Collectors

45

If the system includes one or more analytics servers, stop each analytics server.
1. Log in to the analytics server station as the nsp user.
2. Open a console window.
3. Enter the following:
   
   bash$ /opt/nsp/nfmp/analytics/bin/AnalyticsAdmin.sh stop
   
   The following is displayed:
   
   Stopping Analytics Server
   
   When the analytics server is completely stopped, the following message is displayed:
   
   Analytics Server is not running

46

If the system includes one or more NSP Flow Collectors, stop each NSP Flow Collector.
1. Log in to the NSP Flow Collector station as the root user.
2. Open a console window.
3. Enter the following:
   
   ```bash
define NSPFlowCollector stop
   sh /opt/nsp/flow/dcp/bin/dcpctl.sh stop
define NSPFlowCollector stop
   The command displays a series of status messages as the NSP Flow Collector stops.
```

**Note:** To stop the NSP Flow Collector without displaying status messages, you can use the following command:

```bash
sh systemctl stop nsp-flow-collector.service
```

**Upgrade auxiliary servers [Aux2]**

47

If the system includes auxiliary servers, perform **10.10 “To upgrade an NFM-P auxiliary server”** (p. 435) on each appropriate auxiliary server station [Aux2].

**Note:** Do not start any auxiliary server immediately after you upgrade the auxiliary server; the startup occurs later in the procedure.

**Stop and disable original primary main server [Main1]**

48

Stop the original primary main server.

**Note:** This step marks the beginning of the network management outage.

1. Log in to the original primary main server station [Main1] as the nsp user.
2. Open a console window.
3. Enter the following:

   ```bash
   sh cd /opt/nsp/nfmp/server/nms/bin
   sh ./nmsserver.bash stop
   sh ./nmsserver.bash appserver_status
   The server status is displayed; the server is fully stopped if the status is the following:
   Application Server is stopped
   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform
   the next step until the server is fully stopped.
   ```

49

Disable the automatic main server startup so that the main server does not start in the event of a power disruption during the upgrade.

1. Enter the following to switch to the root user:
Upgrade NSP Flow Collectors

50

If the system includes one or more NSP Flow Collectors, perform 10.11 “To upgrade an NSP Flow Collector” (p. 438) on each NSP Flow Collector station.

Stop auxiliary servers [Aux1]

51

If the system includes auxiliary servers, perform the following steps on each [Aux1] auxiliary server station.
1. Log in to the auxiliary server station as the nsps user.
2. Open a console window.
3. Enter the following:
   
   `bash$ /opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash auxstop`

   The auxiliary server stops.

Upgrade auxiliary database

52

If the system includes an auxiliary database, perform 10.12 “To upgrade an NFM-P auxiliary database” (p. 441).

Stop original primary main database [DB1]

53

Log in to the original primary main database [DB1] station as the root user.

54

Open a console window.

55

Stop and disable the Oracle proxy and main database services.
1. Enter the following to stop the Oracle proxy:
   
   `# systemctl stop nfmp-oracle-proxy.service`
2. Enter the following to disable the automatic Oracle proxy startup:
   
   `# systemctl disable nfmp-oracle-proxy.service`

3. Enter the following to stop the main database:
   
   `# systemctl stop nfmp-main-db.service`

4. Enter the following to disable the automatic database startup:
   
   `# systemctl disable nfmp-main-db.service`

If the original primary main database is deployed in a VM created using the NSP RHEL OS qcow2 image, perform the following steps on the original primary main database [DB1] station.

1. Perform 10.4 “To apply an NSP RHEL qcow2 OS update” (p. 380).
2. Open the `/etc/fstab` file using a plain-text editor such as `vi`.
3. Locate the tmpfs file system entry.
4. Remove the noexec option so that the entry reads as follows:
   
   `tmpfs /dev/shm tmpfs nodev,nosuid 0 0`

5. Save and close the `/etc/fstab` file.
6. Enter the following to remount the `/dev/shm` partition:
   
   `# mount -o remount /dev/shm`

Start new primary main server [Main2]

CAUTION

Service Disruption

The new primary database [DB2] must be upgraded and running before you start the new primary main server [Main2], or the main server initialization may fail.

If you perform the new primary main server and database upgrades concurrently, do not perform this step until the database upgrade is complete.

CAUTION

Service Disruption

An NFM-P system upgrade is not complete until each main server performs crucial post-upgrade tasks during initialization.

Before you attempt an operation that requires a server shutdown, you must ensure that each main server is completely initialized, or the operation fails.

Start the new primary main server [Main2].

Note: You cannot start a main server unless the main server configuration includes a
current and valid license. You can use samconfig to specify the license file, or import a license, as described in “Software and license configuration procedures” in the NSP NFM-P System Administrator Guide.

1. Log in as the nsp user on the new primary main server station [Main2].
2. Enter the following:
   bash$ cd /opt/nsp/nfmp/server/nms/bin
3. Enter the following:
   bash$ ./nmsserver.bash start
4. Enter the following:
   bash$ ./nmsserver.bash appserver_status
   The server status is displayed; the server is fully initialized if the status is the following:
   Application Server process is running. See nms_status for more detail.
   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

Note: This marks the end of the network management outage.

58

If the NFM-P is to manage wireless NEs, enter the following to update the memory configuration accordingly for GUI clients:

bash$ ./nmsdeploytool.bash clientmem -l

Start auxiliary servers [Aux2]

59

If the NFM-P system includes auxiliary servers, start each appropriate auxiliary server [Aux2].
1. Log in to the auxiliary server station as the nsp user.
2. Open a console window.
3. Enter the following:
   bash$ cd /opt/nsp/nfmp/auxserver/nms/bin
4. Enter the following:
   bash$ ./auxnmsserver.bash auxstart
   The auxiliary server starts.

Upgrade analytics servers

60

If the system includes one or more analytics servers, perform 10.13 “To upgrade the NFM-P analytics servers” (p. 449) on each analytics server station.
Enable GUI client

Perform one of the following to enable a GUI client for system testing:

- 14.4 “To install a single-user GUI client” (p. 564)
- 14.5 “To upgrade an NFM-P Release 17 or 5620 SAM single-user GUI client” (p. 569)
- 15.3 “To install a client delegate server” (p. 584)
- 15.5 “To upgrade an NFM-P Release 17 or 5620 SAM client delegate server” (p. 596)

Test upgraded system using GUI client

When the new primary main server [Main2] is started, use a newly installed or upgraded GUI client to perform sanity testing of the new primary main server and database.

**Note:** To back out of the upgrade and return the original primary main server [Main1] and database [DB1] to service, you can do so by stopping the new primary main server [Main2] and database [DB2] and restarting the original primary main server [Main1] and database [DB1].

Restore Release 17.6 security statement

If you are upgrading from Release 17.6 and recorded the NSP sign-in page security statement in Step 21 of 10.3 “To perform the pre-upgrade tasks” (p. 369), perform the following steps.

1. Open the NSP Launchpad as the admin user.
2. Click More→Settings.
3. Enter the security statement text in the Security Statement field.
4. Close the NSP Launchpad.

Uninstall original primary database [DB1]

Perform 13.8 “To uninstall a main database” (p. 554) to uninstall the original primary database [DB1].

Install new standby main database [DB1]

Log in as the root user on the original primary main database [DB1] station.

**Note:** After the upgrade, the station is the new standby main database station.
Perform one of the following.

a. If the main server and database are collocated on one station, perform the following steps.
   1. Transfer the following downloaded installation files to an empty directory on the main database station:
      • nsp-nfmp-oracle-R.r.p-rel.v.rpm
      • nsp-nfmp-main-db-R.r.p-rel.v.rpm
      • nsp-nfmp-nspos-R.r.p.rpm
      • nsp-nfmp-jre-R.r.p-rel.v.rpm
      • nsp-nfmp-config-R.r.p-rel.v.rpm
      • nsp-nfmp-main-server-R.r.p.rpm
      **Note:** In subsequent steps, the directory is called the NFM-P software directory.
   2. If the NFM-P is to manage one or more LTE-N devices, transfer the following additional package to the directory:
      • nsp-nfmp-semvalidator-R.r.p-rel.v.rpm

b. If the main server and database are on separate stations, transfer the following downloaded installation files to an empty directory on the main database station:
   • nsp-nfmp-jre-R.r.p-rel.v.rpm
   • nsp-nfmp-config-R.r.p-rel.v.rpm
   • nsp-nfmp-oracle-R.r.p-rel.v.rpm
   • nsp-nfmp-main-db-R.r.p-rel.v.rpm

   **Note:** In subsequent steps, the directory is called the NFM-P software directory.

Transfer the following downloaded file to an empty directory on the main database station:
• OracleSw_PreInstall.sh

Open a console window.

Navigate to the directory that contains the OracleSw_PreInstall.sh file.

Enter the following:
# chmod +x OracleSw_PreInstall.sh  

Enter the following:
# ./OracleSw_PreInstall.sh  

NFM-P upgrade
Redundant NFM-P system upgrade
To upgrade a redundant NFM-P system
Note: A default value is displayed in brackets []. To accept the default, press ↵.

Note: If you specify a value other than the default, you must record the value for use when the OracleSw_PreInstall.sh script is run during a software upgrade, or when the Oracle management user information is required by technical support.

The following prompt is displayed:

This script will prepare the system for a new install/restore of an NFM-P Version R.r Rn database.

Do you want to continue? [Yes/No]:

Enter Yes. The following prompt is displayed:

Enter the Oracle dba group name [group]:

Press ↵ to accept the default.

The following messages and prompt are displayed:

Creating group group if it does not exist...
WARNING: Group group already exists locally.
Do you want to use the existing group? [Yes/No]:

Enter Yes.

The following message and prompt are displayed:

The user [username] for the group [group] already exists locally.
Do you want to use the existing user? [Yes/No]:

Enter Yes.

The following messages and prompt are displayed:

Checking or Creating the Oracle user home directory /opt/nsp/nfmp/oracle12r1...
Checking user username...
WARNING: Oracle user with the specified name already exists locally.
Redefining the primary group and home directory of user username ... usermod: no changes
Changing ownership of the directory /opt/nsp/nfmp/oracle12r1 to username:group.
About to unlock the UNIX user [username]
Unlocking password for user username.
passwd: Success
Unlocking the UNIX user [username] completed
Do you want to change the password for the user username? [Yes/No]:

Perform one of the following.
a. If you did not change the password during the upgrade of the original standby database, enter No.
b. If you changed the password during the upgrade of the original standby database, perform the following steps.
   1. Enter Yes. The following prompt is displayed:
      New Password:
   2. Enter a password. The following prompt is displayed:
      Re-enter new Password:
   3. Re-enter the password. The following is displayed if the password change is successful:
      passwd: password successfully changed for user

The following message and prompt are displayed:
Specify whether an NFM-P nserver will be installed on this workstation.
The database memory requirements will be adjusted to account for the additional load.
Will the database co-exist with an NFM-P server on this workstation [Yes/No]:

Enter Yes or No, as required.
Messages like the following are displayed as the script execution completes:
INFO: About to remove kernel parameters set by a previous run of this script from /etc/sysctl.conf
INFO: Completed removing kernel parameters set by a previous run of this script from /etc/sysctl.conf
INFO: About to set kernel parameters in /etc/sysctl.conf...
INFO: Completed setting kernel parameters in /etc/sysctl.conf...
INFO: About to change the current values of the kernel parameters
INFO: Completed changing the current values of the kernel parameters
INFO: About to remove ulimit parameters set by a previous run of this script from /etc/security/limits.conf
INFO: Completed removing ulimit parameters set by a previous run of this script from /etc/security/limits.conf
INFO: About to set ulimit parameters in etc/security/limits.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.conf...
INFO: Completed running Oracle Pre-Install Tasks

78

When the script execution is complete, enter the following to reboot the station:

```
# systemctl reboot
```

The station reboots.

79

When the reboot is complete, log in as the root user on the original primary main database [DB1] station.

⚠️ Note: After the upgrade, this database is the new standby main database.

80

Open a console window.

81

Navigate to the NFM-P software directory.

⚠️ Note: Ensure that the directory contains only the installation files.

82

Enter the following:

```
# chmod +x *
```

83

Enter the following:

```
# yum install *.rpm
```

The yum utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

84

Enter y. The following and the installation status are displayed as each package is installed:

- Downloading packages:
- Running transaction check
- Running transaction test
- Transaction test succeeded
Running transaction
The package installation is complete when the following is displayed:
Complete!

Configure the database as a standby database.
1. Enter the following:
   ```
   # samconfig -m db
   The following is displayed:
   Start processing command line inputs...
   <db>
   ```
2. Enter the following:
   ```
   <db> configure type standby
   The prompt changes to <db configure>.
   ```
3. Enter the following:
   ```
   <db configure> ip address
   where address is the IP address of this database
   ```
4. Enter the following:
   ```
   <db configure> redundant ip address
   where address is the IP address of the new primary database [DB2]
   The prompt changes to <db configure redundant>.
   ```
5. Enter the following:
   ```
   <db configure redundant> instance instance_name
   where instance_name is the instance name of the new primary database [DB2]
   ```
6. Enter the following:
   ```
   <db configure redundant> back
   The prompt changes to <db configure>.
   ```
7. Enter the following:
   ```
   <db configure> passwords sys password
   where password is the database SYS user password]
   The prompt changes to <db configure passwords>.
   ```
8. Enter the following:
   ```
   <db configure passwords> back
   The prompt changes to <db configure>.
   ```

Verify the database configuration.
1. Enter the following:
Enter the following to apply the configuration and begin the database creation:

```
<db> apply
```

The database creation begins, and progress messages are displayed.
The following is displayed when the database creation is complete:

```
DONE
db configurations updated.
```

When the database creation is complete, enter the following:

```
<db> exit
```

The samconfig utility closes.

**Reinstantiate standby database**

Log in to an NFM-P GUI client as the admin user.

Choose Administration→System Information from the main menu. The System Information form opens.

Click Re-Instantiate Standby.

Click Yes to confirm the action. The reinstatement begins, and the GUI status bar displays reinstatement information.

**Note:** Database reinstatement takes considerable time if the database contains a large amount of statistics data.
You can also use the System Information form to monitor the reinstantiation progress. The Last Attempted Standby Re-instantiation Time is the start time; the Standby Re-instantiation State changes from In Progress to Success when the reinstantiation is complete.

When the reinstantiation is complete, close the System Information form.

Upgrade original primary main server [Main1]

Log in as the root user on the original primary main server [Main1] station.

**Note:** After the upgrade, the station is the new standby main server station.

If the original primary main server and database are on separate stations, and the original primary main server is deployed in a VM created using the NSP RHEL OS qcow2 image, perform 10.4 “To apply an NSP RHEL qcow2 OS update” (p. 380) on the original primary main server [Main1] station.

Open a console window.

Perform one of the following.

a. If the main server and database are collocated on one station, go to **Step 102**.

b. If the main server and database are on separate stations, transfer the following downloaded installation files to an empty directory on the main server station:
   - nsp-nfmp-nspos-R.r.p.rpm
   - nsp-nfmp-jre-R.r.p-rel.v.rpm
   - nsp-nfmp-config-R.r.p-rel.v.rpm
   - nsp-nfmp-main-server-R.r.p.rpm

**Note:** In subsequent steps, the directory is called the NFM-P software directory.

If the NFM-P is to manage one or more LTE-N devices, transfer the following additional package to the directory:

- nsp-nfmp-semvalidator-R.r.p-rel.v.rpm

Enter the following:
Enter the following:
```
# chmod +x *
```

The yum utility resolves any package dependencies, and displays the following prompt:
```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

Enter y. The following and the installation status are displayed as each package is installed:
```
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
The package installation is complete when the following is displayed:
Complete!
```

Enter the following; see Chapter 3, "Using samconfig" for information about using samconfig:

Note: Regardless of whether you intend to modify the main server configuration, you must apply the main server configuration, as described in the following steps.
```
# samconfig -m main
```

The following is displayed:
```
Start processing command line inputs...
</main>
```

Enter the following:
```
</main> configure
```

The prompt changes to <main configure>.

To apply a new or updated NFM-P license, enter the following, and then enter back:

Note: You cannot start a main server unless the main server configuration includes a current and valid license. You can use samconfig to specify the license file in this step, or
later import the license, as described in “Software and license configuration procedures” in the *NSP NFM-P System Administrator Guide*.

```
<main configure> license license_file
```

where *license_file* is the path and file name of the NSP license bundle.

---

105

Verify the main server configuration.
1. Enter the following:
   
   ```
   <main configure> show
   ```

   The main server configuration is displayed.
2. Review each parameter to ensure that the value is correct.
3. Configure one or more parameters, if required; see Chapter 3, “Using samconfig” for information about using the samconfig utility.
4. When you are certain that the configuration is correct, enter the following:
   
   ```
   <main configure> back
   ```

   The prompt changes to `<main>`.

---

106

Enter the following:

```
<main> apply
```

The configuration is applied.

---

107

Enter the following:

```
<main> exit
```

The samconfig utility closes.

**Note:** This station is the new standby main server station.

**Start new standby main server [Main1]**

---

108

Start the new standby main server [Main1].

**Note:** You cannot start a main server unless the main server configuration includes a current and valid license. You can use samconfig to specify the license file, or import a license, as described in “Software and license configuration procedures” in the *NSP NFM-P System Administrator Guide*.

1. Enter the following to switch to the nsp user:

   ```
   # su - nsp
   ```
2. Open a console window.
3. Enter the following:
   bash$ cd /opt/nsp/nfmp/server/nms/bin

4. Enter the following:
   bash$ ./nmsserver.bash start

5. Enter the following:
   bash$ ./nmsserver.bash appserver_status

   The server status is displayed; the server is fully initialized if the status is the following:
   Application Server process is running. See nms_status for more detail.
   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

If the NFM-P is to manage wireless NEs, enter the following to update the memory configuration accordingly for GUI clients:

bash$ ./nmsdeploytool.bash clientmem -l

Close the console window.

Upgrade auxiliary servers [Aux1]

If the system includes auxiliary servers, perform 10.10 “To upgrade an NFM-P auxiliary server” (p. 435) on each [Aux1] auxiliary server station.

Start auxiliary servers [Aux1]

If the system includes auxiliary servers, perform the following steps on each [Aux1] auxiliary server station.
1. Log in to the auxiliary server station as the nsp user.
2. Open a console window.
3. Enter the following:
   bash$ /opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash auxstart
   The auxiliary server starts.

Install or upgrade single-user GUI clients

As required, perform the following to install or upgrade single-user GUI clients:
Install or upgrade client delegate servers

As required, perform the following to install or upgrade client delegate servers:

- 15.3 “To install a client delegate server” (p. 584)
- 15.5 “To upgrade an NFM-P Release 17 or 5620 SAM client delegate server” (p. 596)

Stop PKI server

If you are deploying TLS using an NSP PKI server, stop the PKI server, as described at the end of 6.7 “To configure and enable an NSP PKI server” (p. 91).

Restore TLS version and cipher support configuration

An NFM-P system upgrade does not preserve your changes to the system support for specific TLS versions and ciphers.

If the system had customized TLS settings before the upgrade, perform “To update the supported NFM-P TLS versions and ciphers” in the NSP NFM-P System Administrator Guide to restore the TLS version and cipher support settings.

Configure and enable firewalls

If you intend to use any firewalls between the NFM-P components, and the firewalls are disabled, configure and enable each firewall.

Perform one of the following.

a. Configure each external firewall to allow the required traffic using the port assignments in the NSP NFM-P Planning Guide, and enable the firewall.

b. Configure and enable Firewalld on each component station, as required.

1. Use an NFM-P template to create the Firewalld rules for the component, as described in the NSP NFM-P Planning Guide.

2. Log in to the station as the root user.

3. Open a console window.

4. Enter the following:

   # systemctl enable firewalld

5. Enter the following:
# systemctl start firewalld

6. Close the console window.

END OF STEPS
Auxiliary server upgrade

10.10 To upgrade an NFM-P auxiliary server

10.10.1 Description

The following steps describe how to upgrade the NFM-P auxiliary server software on a station. Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

**Note:** An auxiliary server is dedicated to only one of the following functions:
- statistics collection
- call-trace data collection
- PCMD record collection

**Note:** You require the following user privileges on the auxiliary server station:
- root
- nsp

**Note:** The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:
- # — root user
- bash$ — nsp user

10.10.2 Steps

**Install auxiliary server software**

1. Log in as the root user on the auxiliary server station.

2. If the auxiliary server is deployed in a VM created using the NSP RHEL OS qcow2 image, perform 10.4 “To apply an NSP RHEL qcow2 OS update” (p. 380) on the auxiliary server station.

3. Download the following NFM-P installation files to an empty local directory:
   - nsp-nfmp-jre-R.r.p-rel.v.rpm
   - nsp-nfmp-config-R.r.p-rel.v.rpm
   - nsp-nfmp-aux-server-R.r.p-rel.v.rpm

   where
R.r.p is the NSP release identifier, in the form MAJOR.minor.patch
v is a version identifier

4
Navigate to the directory that contains the NFM-P installation files.

Note: Ensure that the directory contains only the installation files.

5
Enter the following:

```
# chmod +x *
```

6
Enter the following:

```
# yum install *.rpm
```
The yum utility resolves any package dependencies, and displays the following prompt:

Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:

7
Enter y. The following and the installation status are displayed as each package is installed:

Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
The package installation is complete when the following is displayed:
Complete!

8
Enter the following:

```
# samconfig -m aux
```
The following is displayed:

Start processing command line inputs...
<aux>

9
Verify the auxiliary server configuration.

1. Enter the following:
<aux> show-detail
The auxiliary server configuration is displayed.

2. Review each parameter to ensure that the value is correct.

3. If required, modify one or more parameter values, and then enter back; see Chapter 3, "Using samconfig" for information about using the samconfig utility.

4. When you are certain that the configuration is correct, enter the following:

   <aux> apply
   The configuration is applied.

5. Enter the following:

   <aux> exit
   The samconfig utility closes.

Start the auxiliary server, unless otherwise directed in a system upgrade procedure.

1. Log in to the auxiliary server station as the nsp user.

2. Open a console window.

3. Enter the following:

   bash$ /opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash auxstart
   The auxiliary server starts.

END OF STEPS
NSP Flow Collector upgrade

10.11 To upgrade an NSP Flow Collector

10.11.1 Description

The following steps describe how to upgrade the NSP Flow Collector software on a station. Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

Note: After the upgrade, you must clear the cache of each browser that you use to configure the NSP Flow Collector, or the configuration web UI may not display correctly.

Note: You require root user privileges on the NSP Flow Collector station.

Note: A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

10.11.2 Steps

Stop NSP Flow Collector

1. Log in to the NSP Flow Collector station as the root user.

2. Open a console window.

3. Stop the NSP Flow Collector; enter the following:

   # /opt/nsp/flow/dcp/bin/dcpctl.sh stop

   The command displays a series of status messages as the NSP Flow Collector stops.

   Note: To stop the NSP Flow Collector without displaying status messages, you can use the following command:

   # systemctl stop nsp-flow-collector.service

4. If the NSP Flow Collector is deployed in a VM created using the NSP RHEL OS qcow2 image, perform 10.4 “To apply an NSP RHEL qcow2 OS update” (p. 380) on the NSP Flow Collector station.
Install NSP Flow Collector

Download the following NFM-P installation files to an empty local directory:

- nsp-nfmp-jre-\textit{R.r.p-rel.v}.rpm
- nsp-nfmp-config-\textit{R.r.p-rel.v}.rpm
- nsp-flow-collector-\textit{R.r.p-rel.v}.rpm

where

\textit{R.r.p} is the NSP release identifier, in the form \textit{MAJOR.minor.patch}
\textit{v} is a version identifier

Navigate to the directory that contains the installation files.

\textit{Note:} Ensure that the directory contains only the installation files.

Enter the following:

```
# chmod +x *
```

Enter the following:

```
# yum install *.rpm
```

The \textit{yum} utility resolves any package dependencies, and displays the following prompt:

\textit{Total size}: \textit{nnn M}
\textit{Installed size}: \textit{nn M}
\textit{Is this ok \{y/d/N\}}:

Enter \textit{y}. The following and the installation status are displayed as each package is installed:

\textbf{Downloading packages:}
\textbf{Running transaction check}
\textbf{Running transaction test}
\textbf{Transaction test succeeded}
\textbf{Running transaction}

\textit{The package installation is complete} when the following is displayed:

\textit{Complete!}

Start the NSP Flow Collector; enter the following:
# /opt/nsp/flow/dcp/bin/dcpctl.sh start

The command displays a series of status messages as the NSP Flow Collector starts.

**Note:** To start the NSP Flow Collector without displaying status messages, you can use the following command:

# systemctl start nsp-flow-collector.service

Close the console window.

**END OF STEPS**
Auxiliary database upgrade

10.12 To upgrade an NFM-P auxiliary database

10.12.1 Description

The following steps describe how to upgrade the NFM-P auxiliary database software on one or more stations. Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

**Note:** CPU speed scaling, or CPUfreq, must be set to “performance” in the BIOS of each auxiliary database station, or the auxiliary database upgrade fails. See the RHEL power management documentation for information about enabling the “performance” CPUfreq governor on a station.

Setting CPUfreq to “performance” effectively disables CPU speed scaling, so may result in greater energy consumption by a station.

**Note:** You require the following user privileges on each auxiliary database station:

- root
- samauxdb

**Note:** The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands

- # — root user
- bash$ — samauxdb user

10.12.2 Steps

Back up database

1

**CAUTION**

**Data Loss**

*If you specify a backup location on the database data partition, data loss or corruption may occur.*

The auxiliary database backup location must be an absolute path on a partition other than the database data partition.

Back up the auxiliary database.

**Note:** The backup location requires 20% more space than the database data consumes.

**Note:** If the backup location is remote, a 10 Gb/s link to the location is required.
For auxiliary database backup information, see the *NSP NFM-P System Administrator Guide* for the installed release.

**Obtain software**

2

Download the following NFM-P installation files to an empty local directory on a station that is reachable by each auxiliary database station:

- nsp-nfmp-jre-\(R.r.p\)-rel.v.rpm
- vertica-V.w.x-y.rpm
- nsp-nfmp-aux-db-\(R.r.p\)-rel.v.rpm
- VerticaSw_PreInstall.sh

where

\(R.r.p\) is the NSP release identifier, in the form *MAJOR*.*minor*.*patch*

V.w.x-y is a version number

v is a version identifier

**Stop database**

3

Log into one auxiliary database station as the root user.

4

Open a console window.

5

Enter the following:

```
# cd /opt/nsp/nfmp/auxdb/install/bin
```

6

Enter the following to stop the auxiliary database:

```
# ./auxdbAdmin.sh stop
```

7

Enter the following to display the auxiliary database status:

```
# ./auxdbAdmin.sh status
```

The script displays the following:

```
Database status
Node | Host | State | Version | DB
---------------------------------------------
```

Repeat **Step 7** periodically until each **STATE** entry reads **DOWN**.

**Prepare all stations for upgrade**

**Perform Step 11 to Step 21 on each auxiliary database station.**

**Go to Step 22.**

**Prepare individual station for upgrade**

**Log into the auxiliary database station as the root user.**

**Open a console window.**

**Enter the following commands in sequence to stop the auxiliary database services:**

```
# systemctl stop nfmp-auxdb.service
# systemctl stop nfmp-auxdbproxy.service
# /etc/rc3.d/S99verticad stop
# /etc/rc3.d/S99vertica_agent stop
```

**Enter the following commands in sequence to disable the database services:**

```
# systemctl disable nfmp-auxdb.service
# systemctl disable nfmp-auxdbproxy.service
# chkconfig verticad off
# chkconfig vertica_agent off
```
Transfer the downloaded NFM-P installation files to an empty directory on the station.

**Note:** In subsequent steps, the directory is called the NFM-P software directory.

Navigate to the NFM-P software directory.

**Note:** Ensure that the directory contains only the installation files.

Enter the following:

```
# chmod +x *
```

Enter the following:

```
# ./VerticaSw_PreInstall.sh
```

The script displays output like the following:

```
Logging Vertica pre install checks to log_file
INFO: About to remove proxy parameters set by a previous run of this script from /etc/profile.d/proxy.sh
INFO: Completed removing proxy parameters set by a previous run of this script from /etc/profile.d/proxy.sh
INFO: About to set proxy parameters in /etc/profile.d/proxy.sh...
INFO: Completed setting proxy parameters in /etc/profile.d/proxy.sh...
INFO: About to remove kernel parameters set by a previous run of this script from /etc/sysctl.conf
INFO: Completed removing kernel parameters set by a previous run of this script from /etc/sysctl.conf
INFO: About to set kernel parameters in /etc/sysctl.conf...
INFO: Completed setting kernel parameters in /etc/sysctl.conf...
INFO: About to change the current values of the kernel parameters
INFO: Completed changing the current values of the kernel parameters
INFO: About to remove ulimit parameters set by a previous run of this script from /etc/security/limits.conf
INFO: Completed removing ulimit parameters set by a previous run of this script from /etc/security/limits.conf
INFO: About to set ulimit parameters in /etc/security/limits.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.conf...
Checking Vertica DBA group samauxdb...
```
WARNING: Vertica DBA group with the specified name already exists locally.
Checking Vertica user samauxdb...
WARNING: Vertica user with the specified name already exists locally.
Changing ownership of the directory /opt/nsp/nfmp/auxdb/install to samauxdb:samauxdb.
Adding samauxdb to sudoers file.
Changing ownership of /opt/nsp/nfmp/auxdb files.
INFO: About to remove commands set by a previous run of this script from /etc/rc.d/rc.local
INFO: Completed removing commands set by a previous run of this script from /etc/rc.d/rc.local
INFO: About to add setting to /etc/rc.d/rc.local...
INFO: Completed adding setting to /etc/rc.d/rc.local...

If the script instructs you to perform a restart, perform the following steps.

1. Enter the following:
   
   # systemctl reboot  
   
   The station reboots.

2. When the reboot is complete, log in to the station as the root user.

3. Open a console window.

4. Navigate to the NFM-P software directory.

Enter the following:

# yum install *.rpm  

The yum utility resolves any package dependencies, and displays the following prompt:

Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:

Enter y. The following and the installation status are displayed as each package is installed:

Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
The package installation is complete when the following is displayed:
Complete!

Upgrade database

22
Log in to one auxiliary database station as the root user.

23
Open a console window.

24
Enter the following:
```
# cd /opt/nsp/nfmp/auxdb/install/bin
```

25
Enter the following:
```
#/auxdbAdmin.sh upgrade
```
The following prompt is displayed:
Updating Vertica - Please perform a backup before proceeding with this option
Do you want to proceed (YES/NO)?

26
Enter YES.

27
Enter the auxiliary database dba password [if you are doing initial setup for auxiliary database, press enter]:

28
Enter the dba password again.

The upgrade begins, and operational messages are displayed.
The upgrade is complete when the following is displayed:
Database database_name started successfully
Enter the following to display the auxiliary database status:

```
# ./auxdbAdmin.sh status
```

The script displays the following:

Database status

<table>
<thead>
<tr>
<th>Node</th>
<th>Host</th>
<th>State</th>
<th>Version</th>
<th>DB</th>
</tr>
</thead>
<tbody>
<tr>
<td>host_IP_1</td>
<td>internal_IP_1</td>
<td>STATE</td>
<td>version</td>
<td>db_name</td>
</tr>
<tr>
<td>host_IP_2</td>
<td>internal_IP_2</td>
<td>STATE</td>
<td>version</td>
<td>db_name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Output captured in log_file

**30**

Repeat **Step 29** periodically until each STATE entry reads UP.

**31**

Enter the following to apply the updated database schema:

```
# ./auxdbAdmin.sh upgradeDb
```

⚠️ **Note:** The operation may take considerable time.

The following prompt is displayed:

Please enter auxiliary database dba password:

**32**

Enter the dba password.

The following prompt is displayed:

Please enter auxiliary database user password:

**33**

Enter the database user password.

The following prompt is displayed:

Please enter database port[default]:

**34**

Press \( \downarrow \).
The following message and prompt are displayed:
INFO: Please perform a database backup before proceeding with this option.
Do you want to proceed (YES/NO)?:

Enter YES ↵.

The following and operational messages are displayed as the database schema is updated.
INFO: Database upgrade can take a very long time on large databases.
INFO: Please don’t reboot any database nodes until upgrade is completed.
INFO: logs are stored under /opt/nsp/nftp/auxdb/install. Check the logs for progress.
INFO: Please wait ......

The schema update is complete when the following is displayed:
Output captured in log_file

Perform the following steps on each auxiliary database station.
1. Log in as the root user.
2. Open a console window.
3. Enter the following commands in sequence to enable the database services:
   # systemctl enable nfmp-auxdb.service
   # systemctl enable nfmp-auxdbproxy.service
   # chkconfig verticad on
   # chkconfig vertica_agent on
4. Enter the following commands in sequence to start the auxiliary database services:
   # systemctl start nfmp-auxdb.service
   # systemctl start nfmp-auxdbproxy.service

Close the open console windows, as required.

END OF STEPS
NFM-P analytics server upgrade

10.13 To upgrade the NFM-P analytics servers

10.13.1 Description

The following steps describe how to upgrade the analytics servers in an NFM-P system at Release 18.3 or earlier to NSP analytics servers. Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

To upgrade one or more Release 18.6 NSP analytics servers, see the required upgrade procedure in the NSP Deployment and Installation Guide.

Note: You must upgrade all analytics servers in the system as one uninterrupted operation.

Note: You require root and nsp user privileges on each analytics server station.

Note: The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands

- # — root user
- bash$ — nsp user

10.13.2 Steps

Stop analytics servers

1

If any analytics server is running, perform the following steps on the analytics server station to stop the server.

Note: You must ensure that no analytics server is running.

1. Log in as the nsp user on the station.
2. Open a console window.
3. Enter the following:

   bash$ /opt/nsp/nfmp/analytics/bin/AnalyticsAdmin.sh stop

The following and other messages are displayed:

Stopping Analytics Application

When the analytics server is completely stopped, the following is displayed:

Analytics Application is not running
Enable NSP compatibility

2

If the NSP system includes the NSD and NRC module, and the NSD-NRC is at Release 18.6 or later, you must configure compatibility with the NSD-NRC.

To apply the compatibility configuration, perform the following steps on each NSP server station.

**Note:** The following conditions must be met before you apply the configuration.

- No NSP application sessions are open, and no NSP application user is logged in to the NSP.
- Each NSP server is at Release 18.6 or later, and is operational.

1. Log in to the NSP server station as the nsp user.
2. Open a console window.
3. Enter the following to restore the backed-up Analytics application war file for the current release:
   ```bash
   mv /opt/nsp/patches/backup/wars/R.r/Analytics.war /opt/nsp/os/appl-tomcat/webapps/
   ```
   where `R.r` is the current NSP release
4. Switch to the root user.
5. Enter the following to restart the NSP application server:
   ```bash
   # systemctl restart nspos-app1-tomcat
   ```
6. Close the console window.

Prepare for Analytics repository migration

3

You must use one existing analytics server station to export the central Analytics repository of report results.

Designate an analytics server station for the export; in subsequent steps, the station is called Server A.

4

Log in to the Server A station as the root user.

5

If the analytics server is deployed in a VM created using the NSP RHEL OS qcow2 image, perform 10.4 "To apply an NSP RHEL qcow2 OS update" (p. 380) on the analytics server station.

6

Download the following NSP installation files to an empty local directory:
• npos-jre-R.r.p-rel.v.rpm
• npos-tomcat-R.r.p-rel.v.rpm
• nsp-analytics-server-R.r.p-rel.v.rpm

where

R.r.p is the NSP release identifier, in the form MAJOR.minor.patch
v is a version identifier

Note: In subsequent steps, the directory is called the NSP software directory.

7

Navigate to the NSP software directory.

Note: Ensure that the directory contains only the installation files.

8

Enter the following:

```
# chmod +x *
```

9

Enter the following:

```
# yum install *.rpm
```

For each package, the yum utility resolves any package dependencies and displays the following prompt:

- Total size: nn G
- Installed size: nn G

Is this ok [y/d/N]:

10

Enter y. The following and the installation status are displayed as each package is installed:

- Downloading packages:
- Running transaction check
- Running transaction test
- Transaction test succeeded
- Running transaction

The package installation is complete when the following is displayed:

Complete!

11

Enter the following to switch back to the nsp user:

```
# exit
```
To upgrade the NFM-P analytics servers

Enter the following:

```
bash$ cd /opt/nsp/analytics/bin
```

Enter the following:

```
bash$ ./AnalyticsAdmin.sh updateConfig
```

The script displays the following prompt:

```
THIS ACTION UPDATES /opt/nsp/analytics/config/install.config
Please type 'YES' to continue
```

Enter YES. The script displays the first in a series of prompts.
At each prompt, enter a parameter value; to accept a default in brackets, press <
cr>.

The following table lists and describes each parameter.

**Table 10-2  Analytics server parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary PostgreSQL Repository Database Host</td>
<td>The primary report results repository, which is the IP address or hostname of one of the following:</td>
</tr>
<tr>
<td></td>
<td>• if the NSP system includes only the NFM-P, the primary or standalone NFM-P main server</td>
</tr>
<tr>
<td></td>
<td>• if the NSP system includes the NSD and NRC, the primary or standalone NSD and NRC server</td>
</tr>
<tr>
<td>Secondary PostgreSQL Repository Database Host</td>
<td>In a redundant system, the standby report results repository, which is the IP address or hostname of one of the following:</td>
</tr>
<tr>
<td></td>
<td>• if the NSP system includes only the NFM-P, the standby NFM-P main server</td>
</tr>
<tr>
<td></td>
<td>• if the NSP system includes the NSD and NRC, the standby NSD and NRC server</td>
</tr>
<tr>
<td>Auxiliary Data Source DB Host 1</td>
<td>If the system includes an auxiliary database, the IP address of an auxiliary database station</td>
</tr>
<tr>
<td>Auxiliary Data Source DB Host 2</td>
<td>If the system includes an auxiliary database, the IP address of an auxiliary database station</td>
</tr>
<tr>
<td>Auxiliary Data Source DB Host 3</td>
<td>If the system includes an auxiliary database, the IP address of an auxiliary database station</td>
</tr>
<tr>
<td>Auxiliary Data Source DB Port [5433]</td>
<td>If the system includes an auxiliary database, the auxiliary database port</td>
</tr>
<tr>
<td>Primary Oracle Data Source DB Host</td>
<td>The primary or standalone main database IP address</td>
</tr>
<tr>
<td>Primary Oracle Data Source DB Name</td>
<td>The primary or standalone main database instance name</td>
</tr>
</tbody>
</table>
Table 10-2  Analytics server parameters  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Oracle Data Source DB Port [1523]</td>
<td>The TCP port on the primary or standalone main database station that receives database requests</td>
</tr>
<tr>
<td>Secondary Oracle Data Source DB Host</td>
<td>In a redundant system, the standby main database IP address</td>
</tr>
<tr>
<td>Secondary Oracle Data Source DB Name</td>
<td>In a redundant system, the standby main database instance name</td>
</tr>
<tr>
<td>Secondary Oracle Data Source DB Port [1523]</td>
<td>In a redundant system, the TCP port on the standby main database station that receives database requests</td>
</tr>
<tr>
<td>PKI Server IP Address or Hostname</td>
<td>If the TLS configuration is automated using a PKI server, the PKI server IP address; if you have a set of signed TLS certificates, press Enter</td>
</tr>
<tr>
<td>PKI Server Port [2391]</td>
<td>If the TLS configuration is automated using a PKI server, the PKI server port</td>
</tr>
</tbody>
</table>
| Zookeeper Connection String                   | The IP address and port of each ZooKeeper host, in the following format: host1_IP:port;host2_IP:port  
where host1_IP and host2_IP are the IP addresses of the ZooKeeper hosts
port is the TCP port that the host uses for ZooKeeper communication
The ZooKeeper hosts that you specify are one of the following:
• if the NSP system includes only the NFM-P, the NFM-P main servers
• if the NSP system includes the NSD and NRC, the NSD servers |

Export Analytics database

Enter the following:

bash$ ./AnalyticsAdmin.sh exportdb  

Note: The analytics server starts automatically after the export.
The following message is displayed:

Checking the number of reports before exporting data from Oracle
If the repository contains more than 5000 saved report results, the following messages are displayed, and the extra reports are purged:
Number of Reports [ nnnn ] in Oracle Database is greater than 5000.
Older reports will be purged before export
nnn Analytic Reports are purged
The following messages are displayed as the export proceeds:

Starting to export data from Oracle Repository. This may take few minutes to complete...

/opt/nsp/analytics/log/analytics.export.date-time.log can be monitored for progress

Finished data export from Oracle Repository

**Perform Analytics database migration**

16

If you are manually configuring TLS, perform the following steps.

1. Transfer the required TLS keystore and truststore files from the standalone or primary main server station to the analytics server station. See [Chapter 6, “TLS configuration and management”](#) for information about configuring TLS.

   **Note:** The files must be located on a path that is owned by the nsp user.

2. Enter the following:

   ```bash
   # chown nsp:nsp keystore_file
   where keystore_file is the absolute path of the keystore file
   ```

3. Enter the following:

   ```bash
   # chown nsp:nsp truststore_file
   where truststore_file is the absolute path of the truststore file
   ```

17

Enter the following:

```
bash$ ./AnalyticsAdmin.sh migratedb
```

**Note:** The analytics server starts automatically after the database migration.

The following messages and prompt are displayed:

```
date time Migrating Analytics to NSPOS
Migrating Analytics Server to New Database ...
Do you have existing TLS certificates? (yes/no)
```

18

Perform one of the following.

a. If you have TLS keystore and truststore files, perform the following steps.

   1. Enter yes `yes`

      The following prompt is displayed:

      ```bash
      Enter TLS keystore Path, including filename:
      ```

   2. Enter the absolute path of the keystore file.

      The following message and prompt are displayed:
path/keystore_file found.  
Enter TLS truststore Path, including filename:

3. Enter the absolute path of the truststore file.  
The following message and prompt are displayed:  
   path/truststore_file found.  
Enter TLS Keystore Password:

4. Enter the keystore password.  
The following message and prompt are displayed:  
   Verifying TLS Keystore...  
   Certificate loading...  
   Verified TLS Certificate  
Enter TLS Truststore Password:

5. Enter the truststore password.  
The following is displayed as the configuration is updated:  
   Verifying TLS Truststore...  
   Certificate loading...  
   Verified TLS Certificate  
   TLS Config has been updated

b. If you do not have TLS keystore and truststore files, perform the following steps.

1. Enter no .  
The following prompt is displayed:  
   Enter the Path where the TLS Certificates should be created:

2. Enter the absolute path of a directory that is owned by the nsp user, for example, /opt/nsp.  
The following message and prompt are displayed:  
   The path that will contain the keystore and the truststore is:  
   path  
   Set the keystore password:

3. Enter the keystore password.  
The following prompt is displayed:  
   Set the truststore password:

4. Enter the truststore password.  
The following messages are displayed:  
   The files nsp.keystore and nsp.truststore have been created 
   TLS Config has been updated

The migration proceeds, the upgrade completes, and messages like the following are displayed:
Creating Analytics Repository Schema
Analytics Repository Schema creation is complete
Importing analytics server data from oracle. This may take few minutes to complete...
/opt/nsp/analytics/log/analytics.import.date-time.log can be monitored for progress
Finished Importing analytics server data from oracle
date time Upgrading Analytics Server
Updating DB TABLES After upgrade
Updated n Tables
date time Analytic Server upgrade is completed and starting server
date time Starting Analytics Application
Waiting for Analytics Server to come up
date time Analytics Server is UP and Running
Starting Watchdog process to check Oracle database connectivity...
Analytics Server successfully started!
date time Configuring Analytics Server....
Deploying Reports After Upgrade
Start Deploying report
.
.
.
All reports successfully tracked
date time Analytics Server upgraded successfully

Enter the following to view the analytics server status; ensure that the server is initialized:
bash$ ./AnalyticsAdmin.sh status

The following is displayed when the analytics server is initialized:
Analytics Server Version : Release
Analytics Application is running
Active PostgreSQL Repository Database Host : n.n.n.n
Auxiliary Data source Database Host(s) : n.n.n.n,n.n.n.n, n.n.n.n ...
Active Oracle Data source Database Host : n.n.n.n
TLS KeyStore File Path : path/keystore_file
TLS trustStore File Path : path/truststore_file
Upgrade remaining analytics servers

20 Perform Step 22 to Step 36 on each remaining analytics server station.

21 Go to step Step 37.

22 Log in to the analytics server station as the root user.

23 If the analytics server is deployed in a VM created using the NSP RHEL OS qcow2 image, perform 10.4 “To apply an NSP RHEL qcow2 OS update” (p. 380) on the analytics server station.

24 Download the following NSP installation files to an empty local directory:
   • nspos-jre-R.r.p-rel.v.rpm
   • nspos-tomcat-R.r.p-rel.v.rpm
   • nsp-analytics-server-R.r.p-rel.v.rpm
   where
   R.r.p is the NSP release identifier, in the form MAJOR.minor.patch
   v is a version identifier

   Note: In subsequent steps, the directory is called the NSP software directory.

25 Open a console window.

26 Navigate to the NSP software directory.

   Note: Ensure that the directory contains only the installation files.

27 Enter the following:
   # chmod +x *

28 Enter the following:
   # yum install *.rpm
For each package, the yum utility resolves any package dependencies and displays the following prompt:

Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:

29

Enter y. The following and the installation status are displayed as each package is installed:

Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction

The package installation is complete when the following is displayed:
Complete!

30

If you are manually configuring TLS, perform the following steps.

1. Transfer the required TLS keystore and truststore files from the standalone or primary main server station to the analytics server station. See Chapter 6, “TLS configuration and management” for information about configuring TLS.

  Note: The files must be located on a path that is owned by the nsp user.

2. Enter the following:

   # chown nsp:nsp keystore_file

   where keystore_file is the absolute path of the keystore file

3. Enter the following:

   # chown nsp:nsp truststore_file

   where truststore_file is the absolute path of the truststore file

31

Enter the following to switch to the nsp user:

   # su - nsp

32

Enter the following:

bash$ cd /opt/nsp/analytics/bin

33

Enter the following:

bash$ ./AnalyticsAdmin.sh updateConfig
The script displays the following prompt:

THIS ACTION UPDATES /opt/nsp/analytics/config/install.config

Please type 'YES' to continue

Enter YES. The script displays the first in a series of prompts.
At each prompt, enter a parameter value; to accept a default in brackets, press ↵.

The following table lists and describes each parameter.

### Table 10-3  Analytics server parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Primary PostgreSQL Repository Database Host | The primary report results repository, which is the IP address or hostname of one of the following:  
  - if the NSP system includes only the NFM-P, the primary or standalone NFM-P main server  
  - if the NSP system includes the NSD and NRC, the primary or standalone NSD and NRC server |
| Secondary PostgreSQL Repository Database Host | In a redundant system, the standby report results repository, which is the IP address or hostname of one of the following:  
  - if the NSP system includes only the NFM-P, the standby NFM-P main server  
  - if the NSP system includes the NSD and NRC, the standby NSD and NRC server |
| Auxiliary Data Source DB Host 1           | If the system includes an auxiliary database, the IP address of an auxiliary database station |
| Auxiliary Data Source DB Host 2           | If the system includes an auxiliary database, the IP address of an auxiliary database station |
| Auxiliary Data Source DB Host 3           | If the system includes an auxiliary database, the IP address of an auxiliary database station |
| Auxiliary Data Source DB Port [5433]      | If the system includes an auxiliary database, the auxiliary database port |
| Primary Oracle Data Source DB Host        | The primary or standalone main database IP address |
| Primary Oracle Data Source DB Name        | The primary or standalone main database instance name |
| Primary Oracle Data Source DB Port [1523] | The TCP port on the primary or standalone main database station that receives database requests |
| Secondary Oracle Data Source DB Host      | In a redundant system, the standby main database IP address |
| Secondary Oracle Data Source DB Name      | In a redundant system, the standby main database instance name |
| Secondary Oracle Data Source DB Port [1523] | In a redundant system, the TCP port on the standby main database station that receives database requests |
Table 10-3  Analytics server parameters  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKI Server IP Address or Hostname</td>
<td>If the TLS configuration is automated using a PKI server, the PKI server IP address; if you have a set of signed TLS certificates, press Enter</td>
</tr>
<tr>
<td>PKI Server Port [2391]</td>
<td>If the TLS configuration is automated using a PKI server, the PKI server port</td>
</tr>
</tbody>
</table>
| Zookeeper Connection String            | The IP address and port of each ZooKeeper host, in the following format:  
                                          | \textit{host1\_IP:port;host2\_IP:port}  
                                          | where  
                                          | \textit{host1\_IP} and \textit{host2\_IP} are the IP addresses of the ZooKeeper hosts  
                                          | \textit{port} is the TCP port that the host uses for ZooKeeper communication  
                                          | The ZooKeeper hosts that you specify are one of the following:  
                                          | • if the NSP system includes only the NFM-P, the NFM-P main servers  
                                          | • if the NSP system includes the NSD and NRC, the NSD servers |

Enter the following to install the analytics server software:

bash$ ./AnalyticsAdmin.sh install

Note: The analytics server starts automatically after the installation.

The following message and prompt are displayed:

date time Installing Analytics Server...
Do you have existing TLS certificates? (yes/no)

Perform one of the following.

a. If you have TLS keystore and truststore files, perform the following steps.
   1. Enter yes $\checkmark$.
      
      The following prompt is displayed:
      
      Enter TLS keystore Path, including filename:

      Enter TLS keystore Path, including filename:

   2. Enter the absolute path of the TLS keystore file.
      
      The following message and prompt are displayed:

      Enter TLS truststore Path, including filename:

   3. Enter the absolute path of the TLS truststore file.
The following message and prompt are displayed:
path/truststore_file found.
Enter TLS Keystore Password:

4. Enter the keystore password.
The following message and prompt are displayed:
Verifying TLS Certificate...
Certificate loading...
Verified TLS Certificate
Enter TLS Truststore Password:

5. Enter the truststore password.
The following message and prompt are displayed:
Verifying TLS Truststore...
Certificate loading...
Verified TLS Certificate
TLS Config has been updated

b. If you do not have TLS keystore and truststore files, perform the following steps.
1. Enter no.
The following prompt is displayed:
Enter the Path where the TLS Certificates should be created:

2. Enter the absolute path of a directory that is owned by the nspl user, for example, /opt/nspl.
The following message and prompt are displayed:
The path that will contain the keystore and the truststore is:
path
Set the keystore password:

3. Enter the keystore password.
The following prompt is displayed:
Set the truststore password:

4. Enter the truststore password.
The following messages are displayed:
The files nspl.keystore and nspl.truststore have been created
TLS Config has been updated

The installation begins, and messages like the following are displayed:
Creating Analytics Repository Schema
Analytics Repository Schema creation is complete
Please wait while Analytics Server is being installed...This may take a few minutes
date time Deploying Analytics Server in Tomcat...
Analytics Server successfully deployed in Tomcat
date time Starting Analytics Server...
date time Starting Analytics Application
Waiting for Analytics Server to come up
date time Analytics Server is UP and Running
Starting Watchdog process to check Oracle database connectivity...
Analytics Server successfully started!
date time Configuring Analytics Server....
Deploying Reports...
Analytics Server configured successfully
date time Analytics Server successfully installed

Uninstall NFM-P analytics software

When the NSP Analytics application is operational and each NSP analytics server is running, perform the following steps on each analytics server station to uninstall the NFM-P analytics server software, which is no longer of use.

1. Log in to the analytics server station as the nsf user.
2. Open a console window.
3. Enter the following:
   ```bash
   cd /opt/nsp/nfmp/analytics/bin
   ```
4. Enter the following:
   ```bash
   ./AnalyticsAdmin.sh uninstall
   ```
   The NFM-P analytics software is uninstalled.

Enter the following to switch to the root user:
```bash
su -
```

Enter the following:
```
# yum erase nsp-nfmp-analytics nsp-nfmp-tomcat nsp-nfmp-jre
```
The yum utility resolves any package dependencies, and displays the following prompt:
Remove 3 Packages
Installed size: n.n G
Is this ok [y/N]:

NFM-P upgrade
NFM-P analytics server upgrade
To upgrade the NFM-P analytics servers
Enter `y`.
The following and other progress messages are displayed:
- Downloading packages:
- Running transaction check
- Running transaction test
- Transaction test succeeded
- Running transaction

When the removal of all packages is complete, the following is displayed:
Complete!

Remove the `/opt/nsp/nfmp/analytics` directory and contents.

Close the console window.

Finalize data migration

Log in to the Server A station as the nsp user.

Enter the following:
```
bash$ cd /opt/nsp/analytics/bin
```

Enter the following:
```
bash$ ./AnalyticsAdmin.sh droporacledb
```
The script displays the following prompt:

THIS ACTION WILL Delete the Oracle report repository DB. ALL REPORTS WILL BE DELETED, regardless if there are redundant Analytics Servers still running
Please type 'YES' to continue

Enter YES.
The following messages are displayed:
- Dropping Oracle Analytics Schema
- Dropping Existing Oracle Analytics Schema
- Deleted nn Analytics Oracle Tables
Enter the following:
bash$ ./AnalyticsAdmin.sh stop
The Server A analytics server stops.

Enter the following:
bash$ ./AnalyticsAdmin.sh start
The analytics server starts.

Close the console window.

END OF STEPS
11 NFM-P conversion to redundancy

11.1 Overview

11.1.1 Purpose
This chapter describes the conversion of a standalone NFM-P system to a redundant NFM-P system.

11.1.2 Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1 Overview</td>
<td>465</td>
</tr>
<tr>
<td>Introduction</td>
<td>466</td>
</tr>
<tr>
<td>11.2 General information</td>
<td>466</td>
</tr>
<tr>
<td>11.3 System conversion to redundancy workflow</td>
<td>467</td>
</tr>
<tr>
<td>NFM-P system conversion to redundancy</td>
<td>469</td>
</tr>
<tr>
<td>11.4 To convert a standalone NFM-P system to a redundant system</td>
<td>469</td>
</tr>
</tbody>
</table>
11.2 General information

11.2.1 Description

CAUTION

Service Disruption

Failure to follow the requirements and restrictions that apply to NFM-P system deployment has serious consequences. It is strongly recommended that you engage the upgrade service for a system conversion to redundancy in a large or complex network.

Converting an NFM-P system to redundancy requires a thorough understanding of the applicable restrictions and requirements. It is essential that you plan, document, and test the conversion in advance in a lab deployment that is representative of the target live network. Contact technical support to assess the conversion requirements of your NFM-P system.

CAUTION

Service Disruption

An NFM-P system conversion to redundancy fails unless the requirements and restrictions described in Chapter 2, “Before you begin” and the NSP NFM-P Planning Guide are observed, and specific conditions are in place.

Before you attempt to perform a conversion to redundancy, the following must be true.

• The NFM-P system is at the release described in this guide; you cannot combine an upgrade and a conversion to redundancy in one operation.

• If the system to be converted is a newly upgraded system, the system is fully initialized. An upgraded main server performs crucial post-upgrade tasks during initialization.

• Each NFM-P component is running and operational.

CAUTION

Service Disruption

An NFM-P system conversion to redundancy involves a network management outage.

You must perform a conversion only during a maintenance period of sufficient duration for the outage.

Note: It is strongly recommended that you verify the checksum of each software package or file that you download from OLCS. You can compare the checksum value on the download page with, for example, the output of the RHEL md5sum or sha256sum command. See the appropriate RHEL man page for information.
**11.3 System conversion to redundancy workflow**

**11.3.1 Description**

The following is the sequence of high-level actions required to convert a standalone NFM-P system to a redundant system. Each link is a reference to a section in 11.4 “To convert a standalone NFM-P system to a redundant system” (p. 469).

**11.3.2 Stages**

1. Configure TLS and firewalls, as required; see “Perform security preconfiguration” (p. 469).
2. Back up the NFM-P configuration files; see “Back up configuration files” (p. 470).
3. Gather the system information required for the conversion; see “Gather required information” (p. 470).
4. Close the unrequired NFM-P client sessions; see “Close client sessions” (p. 472).
5. Close the LogViewer utility, if it is open; see “Close LogViewer utility” (p. 472).
6. Back up the main database; see “Back up database” (p. 473).
7. Stop the main server; see “Stop main server” (p. 473).
8. Convert the standalone database to a primary database; see “Convert standalone database to primary database” (p. 474).
9. Convert the standalone server to a primary main server; see “Convert standalone main server to primary main server” (p. 476).

10. Create an Oracle management user account and configure the associated system parameters on the standby main database station; see “Prepare new station for standby database installation” (p. 480).

11. Install the standby database; see “Install standby database” (p. 483).

12. Install the standby main server; see “Install standby main server” (p. 487).

13. Reinstall the standby database; see “Reinstall standby database” (p. 498).

14. Use an NFM-P GUI client to perform sanity testing on the newly redundant NFM-P system.

15. Configure and enable firewalls, if required; see “Configure and enable firewalls” (p. 498).
**NFM-P system conversion to redundancy**

### 11.4 To convert a standalone NFM-P system to a redundant system

#### 11.4.1 Description

The following steps describe how to convert an NFM-P system in a standalone deployment to a redundant system. This requires the following:

- Converting the standalone main server and database to a primary main server and database
- Installing the standby main server and database software
- Reinstantiating the database on the new standby main database station

Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

**Note:** Command-line examples use the following to represent the RHEL CLI prompts:

- `#`—represents the prompt for the root user
- `bash$`—represents the prompt for the nspr user

Do not type the leading # symbol or `bash$` when you enter a command.

**Note:** You require the following user privileges:

- on the standalone main server station—root, nspr
- on the standby main server station—root
- on the standalone main database station—root. *Oracle management*
- on the standby main database station—root

**Note:** The nspr user account is created on the standby main server station during this procedure.

**Note:** The Oracle management user account is created on the standby main database station during this procedure.

#### 11.4.2 Steps

**Perform security preconfiguration**

1. Perform one of the following.

   a. If you are deploying TLS using an NSP PKI server, perform 6.7 "To configure and enable an NSP PKI server" (p. 91).

   b. If you are using the manual TLS deployment method, generate and distribute the required TLS files for the redundant system, as described in 6.11 "Workflow for manual TLS deployment" (p. 105).
Before you attempt an NFM-P system conversion to redundancy, you must ensure that each firewall between NFM-P components allows the required traffic to pass between the components, or is disabled. You can configure and enable the firewall after the installation, if required.

**Note:** The RHEL Firewalld service is typically enabled by default in a new RHEL OS installation.

Perform one of the following.

a. Configure each firewall to allow the required traffic to pass. See the *NSP NFM-P Planning Guide* for a list of the ports that must be open on each component.

   **Note:** The RHEL Firewalld service must be configured using the Firewalld rules in the *NSP NFM-P Planning Guide*, which describes using NFM-P templates for rule creation.

b. Disable each firewall; see the external firewall documentation, or perform the following steps on each component station to disable Firewalld.

   1. Log in to the station as the root user.
   2. Open a console window.
   3. Enter the following:
      ```
      # systemctl stop firewalld
      ```
   4. Enter the following:
      ```
      # systemctl disable firewalld
      ```
   5. Close the console window.

### Back up configuration files

Make a backup copy of each file that you have created or customized in or under the /opt/nsp/nfmp/server/nms and /opt/nsp/nfmp/server/jre directories on each server station.

**Note:** At the beginning of an NFM-P server conversion, the NFM-P installation utility backs up specific configuration and log files to a timestamped directory under the installation directory. The utility then deletes directories under the main server installation directory. If you have created or customized a file under the installation directory, you risk losing the file unless you back up the file before the conversion to a storage location that is unaffected by the conversion.

Store the files in a secure location that is unaffected by the conversion activity.

### Gather required information

Obtain the following information from the main server station and record it for use during the conversion:
Obtain the following information from the main database station and record it for use during the conversion:

- **hostname**
- **IP addresses**
  - IP addresses that the current and new main servers use to reach the database
  - IP address that the auxiliary servers use to reach the database
- **root user password**
- **Oracle database user password**
- **Oracle SYS password**

If the NFM-P system includes one or more auxiliary servers, perform the following steps.
Otherwise, go to Step 8.

1. Open an NFM-P GUI client.
2. Choose Administration → System Information from the main menu. The System Information form is displayed.
3. Click on the Auxiliary Services tab.

Perform the following steps for each auxiliary server listed on the form:

1. Select an auxiliary server in the list and click Properties. The properties form for the auxiliary server opens.
2. Record the following information for use during the conversion:
   - Host Name
   - Auxiliary Server Type
   - Server Status
   - Public IP address
   - Private IP address, if displayed
3. Close the auxiliary server properties form.

8

If the NFM-P system includes one or more client delegate servers, perform the following steps. Otherwise, go to Step 10.

1. Open an NFM-P GUI client.
2. Choose Administration → System Information from the main menu. The System Information form is displayed.
3. Click on the Client Delegate Servers tab.

9

Perform the following steps for each client delegate server listed on the form:

1. Select a client delegate server in the list and click Properties. The properties form for the client delegate server opens.
2. Record the IP Address value for use during the conversion.
3. Close the client delegate server properties form.

10

Close the System Information form, if it is open.

Close LogViewer utility

11

CAUTION

Service Disruption

*If the LogViewer utility is running during an NFM-P conversion to redundancy, the conversion fails.*

You must ensure that the LogViewer is closed.

Close the LogViewer utility, if it is open.

Close client sessions

12

Close the open NFM-P GUI and XML API client sessions.

1. Open an NFM-P GUI client using an account with security management privileges, such as admin.
3. Click on the Sessions tab.
4. Click Search. The form lists the open GUI and XML API client sessions.
5. Identify the GUI session that you are using based on the value in the Client IP column.
6. Select all sessions except your current session and click Close Session.
7. Click Yes to confirm the action.
8. Click Search to refresh the list and verify that only the current session is open.

**Back up database**

13

**CAUTION**

Data Loss

*The path of the main database backup directory must not include the main database installation directory, or data loss may occur.*

Ensure that the backup directory path that you specify does not include `/opt/nsp/nfmp/db`.

**Note:** Before the NFM-P performs a database backup, it deletes the contents of the specified backup directory. Ensure that the backup directory that you specify does not contain files that you want to retain.

You must perform a database backup before you convert an NFM-P system to redundancy. Perform one of the following *NSP NFM-P System Administrator Guide* procedures to back up the main database:

- "To back up the main database from the client GUI"
- "To back up the main database from a CLI"

**Stop main server**

14

Stop the main server.
1. Log in to the main server station as the nsp user.
2. Open a console window.
3. Enter the following:
   ```bash
   cd /opt/nsp/nfmp/server/nms/bin
   ```
4. Enter the following:
   ```bash
   ./nmsserver.bash stop
   ```
5. Enter the following:
   ```bash
   ./nmsserver.bash appserver_status
   ```
   The server status is displayed; the server is fully stopped if the status is the following:
Application Server is stopped
If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

15

Disable the automatic main server startup so that the main server does not start in the event of a power disruption during the conversion.

1. Enter the following to switch to the root user:
   
bash$ su -

2. Enter the following:
   
   # systemctl disable nfmp-main-config.service

3. Enter the following:
   
   # systemctl disable nfmp-main.service

Convert standalone database to primary database

16

Log in to the standalone main database station as the root user.

17

Open a console window.

18

Enter the following:

   # samconfig -m db

The following is displayed:

Start processing command line inputs...
<db>

19

Enter the following, and then enter back.

   <db> configure redundant ip address

where address is the IP address of the new standby database

The prompt changes to <db configure redundant>.

20

If required, configure the ip-validation parameters in the following table, and then enter back.
Note: When you enable IP validation on an NFM-P system that includes auxiliary servers, NSP Flow Collectors, or analytics servers, you must configure the remote-servers parameter; otherwise, the servers cannot reach the database.

Table 11-1  Primary database parameters — ip-validation

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>main-one</td>
<td>IP address of primary main server</td>
</tr>
<tr>
<td></td>
<td>Configuring the parameter enables IP validation.</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>main-two</td>
<td>IP address of standby main server</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>remote-servers</td>
<td>Comma-separated list of the IP addresses of each of the following components</td>
</tr>
<tr>
<td></td>
<td>that must connect to the database:</td>
</tr>
<tr>
<td></td>
<td>• auxiliary servers</td>
</tr>
<tr>
<td></td>
<td>• NSP Flow Collectors</td>
</tr>
<tr>
<td></td>
<td>• NSP analytics servers</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
</tbody>
</table>

Verify the database configuration.

1. Enter the following:
   
   `<db configure> show-detail`  
   
   The database configuration is displayed.

2. Review each parameter to ensure that the value is correct.

3. Configure one or more parameters, if required; see Chapter 3, “Using samconfig” for information about using the samconfig utility.

4. When you are certain that the configuration is correct, enter the following:
   
   `<db configure> back`  
   
   The prompt changes to `<db>`.

Enter the following to begin the database conversion:

```
<db> apply
```

The database conversion begins, and messages are displayed as the operation progresses.

The following is displayed when the database conversion is complete:

```
DONE  

db configurations updated.
```
When the database conversion is complete, enter the following:
```
<db> exit
```

The samconfig utility closes.

**Convert standalone main server to primary main server**

Log in to the standalone main server station as the root user.

Open a console window.

Ensure that no-one is logged in to the station as the nsp user.
1. Enter the following:
   ```
   # who
   ```
   The active user sessions are listed.
2. If the nsp user is listed, close each nsp user session; see the RHEL documentation for more information.

Enter the following:
```
# samconfig -m main
```

The following is displayed:
```
Start processing command line inputs...
<main>
```

Enter the following:
```
<main> configure redundancy enabled
```

The prompt changes to `<main configure redundancy>`.

Configure the general redundancy parameters in the following table.
### Table 11-2  Primary main server parameters — redundancy

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-to-peer</td>
<td>The primary main server IP address that the standby main server must use for general communication.</td>
</tr>
<tr>
<td></td>
<td>Default: IP address of primary network interface</td>
</tr>
<tr>
<td>rsync-ip</td>
<td>The primary main server IP address that the standby main server must use for data synchronization.</td>
</tr>
<tr>
<td></td>
<td>Default: IP address of primary network interface</td>
</tr>
</tbody>
</table>

Configure the **database** redundancy parameters in the following table, and then enter **back**.

### Table 11-3  Primary main server parameters — redundancy, database

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>The IP address that the primary main server must use to reach the standby database.</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>instance</td>
<td>Standby database instance name</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>backup-sync</td>
<td>Whether database backup file synchronization is enabled</td>
</tr>
<tr>
<td></td>
<td>When the parameter is enabled, each database backup file set is copied to the peer main database station after the backup completes.</td>
</tr>
<tr>
<td></td>
<td>You must ensure that there is sufficient network bandwidth between the main database stations before you enable this parameter. See the <em>NSP NFM-P Planning Guide</em> for information about the bandwidth requirements of database backup file synchronization.</td>
</tr>
<tr>
<td></td>
<td>You must set the parameter to the same value on each main server. Default: false</td>
</tr>
<tr>
<td>alignment</td>
<td>Whether automatic database alignment is enabled</td>
</tr>
<tr>
<td></td>
<td>If automatic database alignment is enabled, a main server and database attempt to assume a common role, primary or standby, after an event such as a server activity switch or database failover. In a geographically dispersed system, the function helps to ensure that a main server communicates with the local database in order to reduce the network latency between the components.</td>
</tr>
<tr>
<td></td>
<td>For more information about database alignment, see the <em>NFM-P system Administrator Guide</em>. Default: false</td>
</tr>
</tbody>
</table>
### Table 11-3  Primary main server parameters — redundancy, database  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| prefer-instance   | The name of the database instance with which the primary main server is to align.  
                        The parameter is configurable when the alignment parameter is enabled.  
                        Default: —  |
| reinstatiation-delay | The delay, in minutes, between the completion of a database failover and the automatic reinstatiation of the standby database  
                        A value of 0 disables automatic database reinstatiation.  
                        Default: 60 |

Configure the peer-server redundancy parameters in the following table, and then enter back ↵.

### Table 11-4  Primary main server parameters — redundancy, peer-server

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| ip        | The standby main server IP address that the primary main server uses for general communication  
                        Default: —  |
| hostname  | The standby main server hostname that the primary main server uses for general communication  
                        If the TLS certificate contains the FQDN, you must specify the FQDN as the parameter value.  
                        The parameter is configurable and mandatory when the hostname parameter in the client level is configured.  
                        Default: —  |
| rsync-ip  | The standby main server IP address that the primary main server uses for data synchronization  
                        Default: —  |
| public-ip | The IP address that the GUI and XML API clients must use to reach the standby main server  
                        Default: —  |
| jndi-port | The TCP port on the standby main server station used for EJB JNDI messaging to GUI clients  
                        It is recommended that you accept the default unless another application uses the port, or there is a firewall between the GUI clients and the standby main server.  
                        Default: 1099 |
Table 11-4  Primary main server parameters — redundancy, peer-server  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-to-auxes</td>
<td>The standby main server IP address that the auxiliary servers must use to reach the standby main server. You must configure the parameter if the NFM-P system includes one or more auxiliary servers. Default: —</td>
</tr>
<tr>
<td>snmp-ipv4</td>
<td>The IPv4 address that the managed NEs must use to reach the standby main server.</td>
</tr>
<tr>
<td>snmp-ipv6</td>
<td>The IPv6 address that the managed NEs must use to reach the standby main server.</td>
</tr>
<tr>
<td>snmp-port</td>
<td>The TCP port on the standby main server station used for SNMP communication with the managed NEs. Default: 162</td>
</tr>
<tr>
<td>traplog-id</td>
<td>The SNMP trap log ID associated with the standby main server. Default: 98</td>
</tr>
</tbody>
</table>

32

Enter the following:

```
<main configure redundancy> back
```

The prompt changes to `<main configure>`.

33

Verify the main server configuration.

1. Enter the following:

```
<main configure> show-detail
```

The main server configuration is displayed.

2. Review each parameter to ensure that the value is correct.

3. Configure one or more parameters, if required; see Chapter 3, “Using samconfig” for information about using the samconfig utility.

4. When you are certain that the configuration is correct, enter the following:

```
<main configure> back
```

The prompt changes to `<main>`.

34

Enter the following:

```
<main> apply
```

The configuration is applied.
Enter the following:

<main> exit ↵

The samconfig utility closes.

Start the primary main server.

1. Enter the following to switch to the nsp user:
   
   # su - nsp ↵

2. Enter the following:

   bash$ cd /opt/nsp/nfmp/server/nms/bin ↵

3. Enter the following:

   bash$ ./nmsserver.bash start ↵

4. Enter the following:

   bash$ ./nmsserver.bash appserver_status ↵

   The server status is displayed; the server is fully initialized if the status is the following:

   Application Server process is running. See nms_status for more detail.

   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

Close the console window.

Enable primary main server automatic startup

Enable automatic startup on the primary main server.

1. Enter the following to switch back to the root user:

   bash$ exit ↵

2. Enter the following to disable the main server startup:

   # systemctl enable nfmp-main.service

Prepare new station for standby database installation

Log in as the root user on the standby main database station.
40 Download the following NFM-P installation files for the existing release to an empty directory on the station:
- nsp-nfmp-jre-$R.r.p-rel.v.rpm
- nsp-nfmp-config-$R.r.p-rel.v.rpm
- nsp-nfmp-oracle-$R.r.p-rel.v.rpm
- nsp-nfmp-main-db-$R.r.p-rel.v.rpm

where

$R.r.p$ is the NSP release identifier, in the form $MAJOR.minor.patch$

$v$ is a version identifier

**Note:** In subsequent steps, the directory is called the NFM-P software directory.

41 Transfer the following downloaded file to an empty directory on the main database station:
- OracleSw_PreInstall.sh

42 Open a console window.

43 Navigate to the directory that contains the OracleSw_PreInstall.sh file.

44 Enter the following:
```
# chmod +x OracleSw_PreInstall.sh
```

**CAUTION**

**Misconfiguration Risk**

The NFM-P software includes a script that configures the Oracle environment. The script is specific to an NFM-P release; using a different version may cause the database creation to fail.

You must run only the script that is included with the current NFM-P software.

Enter the following:
```
#/OracleSw_PreInstall.sh
```

**Note:** A default value is displayed in brackets []. To accept the default, press ↓. The following prompt is displayed:
This script will prepare the system for a new install/restore of an NFM-P Version Release main database.

Do you want to continue? [Yes/No]:

Enter Yes. The following prompt is displayed:

Enter the Oracle dba group name [group]:

Enter a group name.

Note: The group name must match the group name specified during the primary database conversion.

The following messages and prompt are displayed:

Creating group group if it does not exist...
done

Enter the Oracle user name:

Enter a username.

Note: The username must match the username specified during the primary database conversion.

The following messages and prompt are displayed:

Oracle user [username] new home directory will be [/opt/nsf/nfmp/oracle12r1].
Checking or Creating the Oracle user home directory /opt/nsf/nfmp/oracle12r1..,
Checking user username...
Adding username...
Changing ownership of the directory /opt/nsf/nfmp/oracle12r1 to username:group.
About to unlock the UNIX user [username]
Unlocking password for user username.
passwd: Success
Unlocking the UNIX user [username] completed
Please assign a password to the UNIX user username..
New Password:

Enter a password.
**Note:** The password must match the password specified during the primary database conversion.

The following prompt is displayed:

Re-enter new Password:

---

50

Re-enter the password. The following is displayed if the password change is successful:

```
passwd: password successfully changed for username
```

The following message and prompt are displayed:

Specify whether an NFM-P Main Server will be installed on this workstation.

The database memory requirements will be adjusted to account for the additional load.

Will the database co-exist with an NFM-P Main Server on this workstation [Yes/No]:

---

51

Enter Yes or No, as required.

Messages like the following are displayed as the script execution completes:

```
INFO: About to set kernel parameters in /etc/sysctl.conf...
INFO: Completed setting kernel parameters in /etc/sysctl.conf...
INFO: About to change the current values of the kernel parameters
INFO: Completed changing the current values of the kernel parameters
INFO: About to set ulimit parameters in /etc/security/limits.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.conf...
INFO: Completed running Oracle Pre-Install Tasks
```

---

52

When the script execution is complete, enter the following to reboot the station:

```
# systemctl reboot
```

The station reboots.

**Install standby database**

---

53

When the reboot is complete, log in as the root user on the standby main database station.

---

54

Open a console window.
Navigate to the NFM-P software directory.

ℹ️ Note: Ensure that the directory contains only the installation files.

Enter the following:

```
# chmod +x *
```

Enter the following:

```
# yum install *.rpm
```

The `yum` utility resolves any package dependencies, and displays the following prompt:

Total size: nn G

Installed size: nn G

Is this ok [y/N]:

Enter y. The following and the installation status are displayed as each package is installed:

- Downloading packages:
- Running transaction check
- Running transaction test
- Transaction test succeeded
- Running transaction

The package installation is complete when the following is displayed:

Complete!

Enter the following:

```
# samconfig -m db
```

The following is displayed:

Start processing command line inputs...

<db>

Enter the following:

```
<db> configure type standby
```

The prompt changes to `<db configure>`. 
If required, configure the `ip` parameter; enter the following:

Note: The default is the IP address of the primary network interface on the station.

```
<db configure> ip address
```

where *address* is the IP address of this database

Enter the following:

```
<db configure> redundant ip address
```

where *address* is the IP address of the primary database

The prompt changes to `<db configure redundant>`.

Enter the following, and then enter `back`:

```
<db configure redundant> instance instance_name
```

where *instance_name* is the primary database instance name

Configure the `passwords` parameters in the following table, and then enter `back`.

Note: The values must match the primary database values.

Note: After you save the configuration, you cannot use samconfig to change a database password; you must use the method described in the *NSP NFM-P System Administrator Guide*.

**Table 11-5  Standby database parameters — passwords**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>Database user password; the password must match the password specified during the primary database installation</td>
</tr>
<tr>
<td></td>
<td>Default: available from technical support</td>
</tr>
<tr>
<td>sys</td>
<td>Oracle SYS user password; the password must match the password specified during the primary database installation</td>
</tr>
<tr>
<td></td>
<td>Default: available from technical support</td>
</tr>
</tbody>
</table>

If required, configure the `ip-validation` parameters in the following table to enable IP validation, which restricts database access to only the specified main and auxiliary servers, and then enter `back`.
Note: When you enable IP validation on an NFM-P system that includes auxiliary servers, NSP Flow Collectors, or analytics servers, you must configure the `remote-servers` parameter; otherwise, the servers cannot reach the database.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| main-one    | IP address of primary main server  
              | Configuring the parameter enables IP validation.  
              | Default: —                                |
| main-two    | IP address of standby main server  
              | Default: —                                |
| remote-servers | Comma-separated list of the IP addresses of each of the following  
                  | components that must connect to the database:  
                  | • auxiliary servers  
                  | • NSP Flow Collectors  
                  | • NSP analytics servers  
              | Default: —                                |

Verify the database configuration.

1. Enter the following:
   `<db configure> show-detail`
   The database configuration is displayed.
2. Review each parameter to ensure that the value is correct.
3. Configure one or more parameters, if required; see Chapter 3, “Using samconfig” for information about using the samconfig utility.
4. When you are certain that the configuration is correct, enter the following:
   `<db configure> back`
   The prompt changes to `<db>`.

Enter the following to begin the database creation:

`<db> apply`

The database creation begins, and progress messages are displayed.

The following is displayed when the database creation is complete:

```
DONE
db configurations updated.
```
When the database creation is complete, enter the following:

```
<db> exit
```

The samconfig utility closes.

---

Enter the following to reboot the standby main database station:

```
# systemctl reboot
```

The station reboots.

---

**Install standby main server**

---

Log in as the root user on the standby main server station.

---

Perform one of the following.

a. If the standby main server and database are to be collocated on one station, download the following installation files to the NFM-P software directory on the station:

- `nsp-nfmp-nspos-R.r.p-rel.v.rpm`
- `nsp-nfmp-main-server-R.r.p-rel.v.rpm`

where

R.r.p is the NSP release identifier, in the form `MAJOR.minor.patch`

v is a version identifier

b. If the standby main server and database are to be on separate stations, copy the following files to an empty directory on the main server station:

- `nsp-nfmp-nspos-R.r.p-rel.v.rpm`
- `nsp-nfmp-jre-R.r.p-rel.v.rpm`
- `nsp-nfmp-config-R.r.p-rel.v.rpm`
- `nsp-nfmp-main-server-R.r.p-rel.v.rpm`

where

R.r.p is the NSP release identifier, in the form `MAJOR.minor.patch`

v is a version identifier

**Note:** In subsequent steps, the directory is called the NFM-P software directory.

---

Open a console window.
Ensure that no-one is logged in to the station as the nsp user.

1. Enter the following:
   # who -d
   The active user sessions are listed.
2. If the nsp user is listed, close each nsp user session; see the OS documentation for information about closing user sessions.

Navigate to the NFM-P software directory.

**Note:** Ensure that the directory contains only the installation files.

Enter the following:

# chmod +x *

Enter the following:

# yum install *.rpm

The yum utility resolves any package dependencies, and displays the following prompt:

Total size: nn G
Installed size: nn G
Is this ok [y/N]:

Enter y. The following and the installation status are displayed as each package is installed:

Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction

The package installation is complete when the following is displayed:

Complete!

The initial NFM-P server installation on a station creates the nsp user account and assigns a randomly generated password.

If this is the first installation of a main server, auxiliary server, NSP Flow Collector, or analytics server on the station, change the nsp password.
Note: The nsp password must not contain the @ symbol, or eNodeB device management may be compromised.

1. Enter the following:
   
   `# passwd nsp`  

   The following prompt is displayed:
   
   `New Password:`

2. Enter a password.
   
   The following prompt is displayed:
   
   `Confirm Password:`

3. Re-enter the password.

4. Record the password and store it in a secure location.

Enter the following:

`# samconfig -m main`  

The following is displayed:

Start processing command line inputs...  

`<main>`

Enter the following:

`<main> configure`  

The prompt changes to `<main configure>`.

Enter the following:

Note: You cannot start a main server unless the main server configuration includes a current and valid license. You can use samconfig to specify the license file in this step, or later import the license, as described in “Software and license configuration procedures” in the NSP NFM-P System Administrator Guide.

`<main configure> license license_file`  

where `license_file` is the path and file name of the NSP license bundle

Enter the following:

`<main configure> redundancy enabled`  

The prompt changes to `<main configure redundancy>`.  

To convert a standalone NFM-P system to a redundant system
Configure the general redundancy parameters in the following table.

Table 11-7  Standby main server parameters — redundancy

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-to-peer</td>
<td>The standby main server IP address that the primary main server must use for general communication Default: IP address of primary network interface</td>
</tr>
<tr>
<td>rsync-ip</td>
<td>The standby main server IP address that the primary main server must use for data synchronization Default: IP address of primary network interface</td>
</tr>
</tbody>
</table>

Configure the database redundancy parameters in the following table, and then enter `back`.

Table 11-8  Standby main server parameters — redundancy, database

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>The IP address that the standby main server must use to reach the primary database Default: —</td>
</tr>
<tr>
<td>instance</td>
<td>Primary database instance name Default: —</td>
</tr>
<tr>
<td>backup-sync</td>
<td>Whether database backup file synchronization is enabled When the parameter is enabled, each database backup file set is copied to the peer main database station after the backup completes. You must ensure that there is sufficient network bandwidth between the main database stations before you enable this parameter. See the NSP NFM-P Planning Guide for information about the bandwidth requirements of database backup file synchronization. You must set the parameter to the same value on each main server. Default: false</td>
</tr>
</tbody>
</table>
### Table 11-8  Standby main server parameters — redundancy, database  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alignment</td>
<td>Whether automatic database alignment is enabled. If automatic database alignment is enabled, a main server and database attempt to assume a common role, primary or standby, after an event such as a server activity switch or database failover. In a geographically dispersed system, the function helps to ensure that a main server communicates with the local database in order to reduce the network latency between the components. For more information about database alignment, see the NFM-P system Administrator Guide. Default: false</td>
</tr>
<tr>
<td>prefer-instance</td>
<td>The name of the database instance with which the standby main server is to align. The parameter is configurable when the alignment parameter is enabled. Default: —</td>
</tr>
<tr>
<td>reinstatiation-delay</td>
<td>The delay, in minutes, between the completion of a database failover and the automatic reinstatiation of the standby database. A value of 0 disables automatic database reinstatiation. Default: 60</td>
</tr>
</tbody>
</table>

Configure the peer-server redundancy parameters in the following table, and then enter back ↵.

### Table 11-9  Standby main server parameters — redundancy, peer-server

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>The primary main server IP address that the standby main server uses for general communication. Default: —</td>
</tr>
<tr>
<td>hostname</td>
<td>The primary main server hostname that the standby main server uses for general communication. If the TLS certificate contains the FQDN, you must specify the FQDN as the parameter value. The parameter is configurable and mandatory when the hostname parameter in the client level is configured. Default: —</td>
</tr>
</tbody>
</table>
### Table 11-9  Standby main server parameters — redundancy, peer-server  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| rsync-ip    | The primary main server IP address that the standby main server uses for data synchronization  
Default: —                                                                                                                                     |
| public-ip   | The IP address that the GUI and XML API clients must use to reach the standby main server  
Default: —                                                                                                                                     |
| jndi-port   | The TCP port on the primary main server station used for EJB JNDI messaging to GUI clients  
It is recommended that you accept the default unless another application uses the port, or there is a firewall between the GUI clients and the primary main server.  
Default: 1099                                                                                                                                   |
| ip-to-auxes | The primary main server IP address that the auxiliary servers must use to reach the primary main server  
You must configure the parameter if the NFM-P system includes one or more auxiliary servers.  
Default: —                                                                                                                                     |
| snmp-ipv4   | The IPv4 address that the managed NEs must use to reach the primary main server                                                                                                                                 |
| snmp-ipv6   | The IPv6 address that the managed NEs must use to reach the primary main server                                                                                                                                 |
| snmp-port   | The TCP port on the primary main server station used for SNMP communication with the managed NEs  
Default: 162                                                                                                                                     |
| traplog-id  | The SNMP trap log ID associated with the primary main server  
Default: 98                                                                                                                                 |

Enter the following:

```
<main configure redundancy> back
```

The prompt changes to `<main configure>`.

As required, configure the mediation parameters in the following table, and then enter `back`.
Note: Some device types do not support an SNMP port value other than 162. Before you configure the `snmp-port` parameter to a value other than the default, you must ensure that each device type in the managed network supports the port value.

Table 11-10  Standby main server parameters — mediation

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| nat            | Whether NAT is used between the main servers and the managed NEs  
                | Default: false |
| snmp-ipv4      | The IPv4 address that the managed NEs must use to reach the standby main server  
                | Default: IPv4 address of primary network interface |
| snmp-ipv6      | The IPv6 address that the managed NEs must use to reach the standby main server  
                | Default: IPv6 address of primary network interface |
| snmp-port      | The TCP port on the standby main server station that the managed NEs must use to reach the standby main server  
                | Default: 162 |
| traplog-id     | The SNMP trap log ID associated with the standby main server  
                | Default: 98 |

The standby main server requires a copy of the NFM-P TLS keystore and truststore files that are used by the primary main server.

Copy the keystore and truststore files from the `/opt/nsp/os/tls` directory on the primary main server station to a temporary location on the standby main server station, and record the location for use in Step 89.

Caution: You must not copy the files to the `/opt/nsp/os/tls` directory on the standby main server station, or the TLS configuration fails.

Note: The `ns` user must be the owner of the directory path to the location.

Configure the `tls` parameters in the following table, and then enter `back` ↓.

Table 11-11  Standby main server parameters — tls

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| keystore-file  | The absolute path of the TLS keystore file  
                | To enable automated TLS deployment, enter `no keystore-file`.  
                | Default: — |
Table 11-11  Standby main server parameters — tls (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keystore-pass</td>
<td>The TLS keystore password</td>
</tr>
<tr>
<td></td>
<td>Default: available from technical support</td>
</tr>
<tr>
<td>truststore-file</td>
<td>The absolute path of the TLS truststore file</td>
</tr>
<tr>
<td></td>
<td>To enable automated TLS deployment, enter <code>no truststore-file</code>.</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>truststore-pass</td>
<td>The TLS truststore password</td>
</tr>
<tr>
<td></td>
<td>Default: available from technical support</td>
</tr>
<tr>
<td>alias</td>
<td>The alias specified during keystore generation</td>
</tr>
<tr>
<td></td>
<td>You must configure the parameter.</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>pki-server</td>
<td>If you are using the automated TLS deployment method, the IP address or hostname of the PKI server</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>pki-server-port</td>
<td>If you are using the automated TLS deployment method, the TCP port on which the PKI server listens for and services requests</td>
</tr>
<tr>
<td></td>
<td>Default: 2391</td>
</tr>
<tr>
<td>webdav</td>
<td>Whether WebDAV access to eNodeB activation data is enabled</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
</tbody>
</table>

If required, configure the oss parameters in the following table, and then enter `back`.

Note: The parameters are configurable only if the main server configuration does not include one or more auxiliary servers.

Table 11-12  Standby main server parameters — oss

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>secure</td>
<td>Whether communication between the main servers and the XML API clients is secured using TLS</td>
</tr>
<tr>
<td></td>
<td>Default: secure</td>
</tr>
<tr>
<td>public-ip</td>
<td>The IP address that the XML API clients must use to reach the standby main server</td>
</tr>
<tr>
<td></td>
<td>Default: IP address of primary network interface</td>
</tr>
<tr>
<td>corba-3gpp</td>
<td>Whether the NFM-P 3GPP interface is enabled</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
</tbody>
</table>
Table 11-12  Standby main server parameters — oss  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>xml-output</td>
<td>The directory in which to store the output of XML API file export operations</td>
</tr>
<tr>
<td></td>
<td>Default: /opt/nsp/nfmp/server/xml_output</td>
</tr>
</tbody>
</table>

If the NFM-P includes an auxiliary database, configure the auxdb parameters in the following table, and then enter back ↵.

Table 11-13  Standby main server parameters — auxdb

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enabled</td>
<td>Whether the auxiliary database is enabled in the main server configuration</td>
</tr>
<tr>
<td>ip-list</td>
<td>A comma-separated list of the auxiliary database station IP addresses that are accessible to the main server</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>oam-test-results</td>
<td>Whether the auxiliary database is to store OAM test results</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
<tr>
<td>redundancy-level</td>
<td>Boolean value that specifies whether the auxiliary database is to replicate data among multiple stations</td>
</tr>
<tr>
<td></td>
<td>If the auxiliary database is deployed on a single station, you must set the parameter to 0.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution:</strong> After you configure an auxdb parameter and apply the main server configuration, you cannot modify the redundancy-level parameter.</td>
</tr>
<tr>
<td></td>
<td>Default: 1</td>
</tr>
</tbody>
</table>

As required, configure the aa-stats parameters in the following table, and then enter back ↵.

Table 11-14  Standby main server parameters — aa-stats

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enabled</td>
<td>Whether the NFM-P is to collect AA accounting statistics</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
</tbody>
</table>
Table 11-14  Standby main server parameters — aa-stats (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>formats</td>
<td>AA accounting statistics file formats; the options are the following:</td>
</tr>
<tr>
<td></td>
<td>• ipdr — IPDR format</td>
</tr>
<tr>
<td></td>
<td>• ram — 5670 RAM format</td>
</tr>
<tr>
<td></td>
<td>• ipdr,ram — IPDR and 5670 RAM formats</td>
</tr>
<tr>
<td></td>
<td>The parameter is configurable when the enabled parameter is set to true.</td>
</tr>
<tr>
<td></td>
<td>Default: ram</td>
</tr>
<tr>
<td>aux-db storage</td>
<td>Whether the NFM-P is to store the statistics in an auxiliary database</td>
</tr>
<tr>
<td></td>
<td>The parameter is configurable when the enabled parameter is set to true.</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
</tbody>
</table>

Perform one of the following to specify the registry servers for NSP inter-module communication:

a. If the NSP system includes the NSD and NRC, specify the IP address of each NSD and NRC server; enter the following:
   `<main configure> registry ip-list address1;address2 back`  
   where `address1` and `address2` are the public IP addresses of the NSD and NRC servers

   **Note:** If the NSD and NRC system is standalone, only `address1` is required.

b. If the NSP system includes only the NFM-P, enter the following:
   `<main configure> registry ip-list address1;address2 back`  
   where `address1` and `address2` are the IP addresses that the NFM-P main servers use to communicate with each other

Verify the main server configuration.

1. Enter the following:
   `<main configure> show-detail`  
   The main server configuration is displayed.

2. Review each parameter to ensure that the value is correct.

3. Configure one or more parameters, if required; see Chapter 3, “Using samconfig” for information about using the samconfig utility.

4. When you are certain that the configuration is correct, enter the following:
   `<main configure> back`    
   The prompt changes to `<main>`.
Enter the following:
<main> apply </main>
The configuration is applied.

Enter the following:
<main> exit </main>
The samconfig utility closes.

Start the standby main server.

**Note:** If you did not specify a license file during the installation, you cannot start the main server until you import a license. See “Software and license configuration procedures” in the *NSP NFM-P System Administrator Guide* for information about importing a license.

1. Enter the following:
   ```bash
   cd /opt/nsp/nfmp/server/nms/bin
   ```
2. Enter the following:
   ```bash
   ./nmsserver.bash start
   ```
3. Enter the following:
   ```bash
   ./nmsserver.bash appserver_status
   ```
The server status is displayed; the server is fully initialized if the status is the following:

   Application Server process is running. See nms_status for more detail.

   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

If the NFM-P system includes one or more NSP Flow Collectors, configure the following on each NSP Flow Collector, as described in 7.12 “To configure NSP Flow Collector communication” (p. 219):

On the NFM-P Configuration tab:
- NFM-P Standby panel—all parameters
- NFM-P XML API Service panel—Redundancy parameter, which must be set to true

If the NFM-P system includes one or more analytics servers, enable redundancy support on each analytics server; see the NSP documentation for information.
Reinstantiate standby database

100
Open an NFM-P GUI client as the admin user.

101
Choose Administration→System Information from the main menu. The System Information form opens.

102
Click Re-Instantiate Standby.

103
Click Yes to confirm the action. The reinstatement begins, and the GUI status bar displays reinstatement information.

**Note:** Database reinstatement takes considerable time if the database contains a large amount of statistics data.

You can also use the System Information form to monitor the reinstatement progress. The Last Attempted Standby Re-instantiation Time is the start time; the Standby Re-instantiation State changes from In Progress to Success when the reinstatement is complete.

104
When the reinstatement is complete, close the System Information form.

105
Use an NFM-P GUI client to perform sanity testing of the newly redundant system.

Configure and enable firewalls

106
If you intend to use any firewalls between the NFM-P components, and the firewalls are disabled, configure and enable each firewall.

Perform one of the following.

a. Configure each external firewall to allow the required traffic using the port assignments in the *NSP NFM-P Planning Guide*, and enable the firewall.

b. Configure and enable Firewalld on each component station, as required.
   1. Use an NFM-P template to create the Firewalld rules for the component, as described in the *NSP NFM-P Planning Guide*.
   2. Log in to the station as the root user.
   3. Open a console window.
   4. Enter the following:
5. Enter the following:

```
# systemctl enable firewalld
```

6. Close the console window.

End of steps
To convert a standalone NFM-P system to a redundant system.
# 12 NFM-P conversion to IPv6

## 12.1 Overview

### 12.1.1 Purpose

This chapter describes the conversion of inter-component communication from IPv4 to IPv6 in a standalone or redundant NFM-P system.

### 12.1.2 Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>501</td>
</tr>
<tr>
<td>Introduction</td>
<td>502</td>
</tr>
<tr>
<td>General information</td>
<td>502</td>
</tr>
<tr>
<td>System conversion to IPv6 workflow</td>
<td>503</td>
</tr>
<tr>
<td>To perform the pre-conversion tasks</td>
<td>503</td>
</tr>
<tr>
<td><strong>NFM-P system conversion to IPv6</strong></td>
<td>508</td>
</tr>
<tr>
<td>To convert a standalone NFM-P system to IPv6</td>
<td>508</td>
</tr>
<tr>
<td>To convert a redundant NFM-P system to IPv6</td>
<td>518</td>
</tr>
</tbody>
</table>
Introduction

12.2 General information

12.2.1 Description

CAUTION

Service Disruption

Failure to follow the requirements and restrictions that apply to NFM-P system deployment has serious consequences.

Converting an NFM-P system to IPv6 requires a thorough understanding of the applicable restrictions and requirements. It is essential that you plan, document, and test the conversion procedure in advance in a lab deployment that is representative of the target live network. Contact technical support to assess the conversion requirements of your NFM-P system.

It is strongly recommended that you engage the technical support upgrade service for a system conversion to IPv6 in a large or complex network.

CAUTION

Service Disruption

An NFM-P system conversion to IPv6 fails unless the requirements and restrictions described in Chapter 2, “Before you begin” and the NSP NFM-P Planning Guide are observed, and specific conditions are in place.

Before you attempt to perform a procedure in this chapter, the following must be true.

• Each required IPv6 interface is plumbed and operational; see the RHEL documentation for information about enabling and configuring an IPv6 interface.

• The NFM-P system is at the release described in this guide; you cannot combine an upgrade and a conversion to IPv6 in one operation.

• If the system to be converted is a newly upgraded system, the system is fully initialized. An upgraded main server performs crucial post-upgrade tasks during initialization.

• Each NFM-P component is running and operational.

CAUTION

Service Disruption

An NFM-P system conversion to IPv6 involves a network management outage.

You must perform a conversion only during a maintenance period of sufficient duration.

The NFM-P samconfig utility is used for component configuration and deployment. See Chapter 3, “Using samconfig” for information about the samconfig utility.
Before you attempt an NFM-P system conversion to IPv6, you must perform 12.4 “To perform the pre-conversion tasks” (p. 503) to collect the required information and ensure that the required conditions are in place.

**Note:** The Bash shell is the supported command shell for RHEL CLI operations.

**Table 12-1  NFM-P IPv6 conversion procedures list**

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.4 “To perform the pre-conversion tasks” (p. 503)</td>
<td>Prepare a standalone or redundant NFM-P system for conversion to IPv6 by ensuring the correct conditions are in place, gathering the required information, and backing up the configuration files and database.</td>
</tr>
<tr>
<td>12.5 “To convert a standalone NFM-P system to IPv6” (p. 508)</td>
<td>Configure a standalone NFM-P system to use IPv6 for inter-component communication.</td>
</tr>
<tr>
<td>12.6 “To convert a redundant NFM-P system to IPv6” (p. 518)</td>
<td>Configure a redundant NFM-P system to use IPv6 for inter-component communication.</td>
</tr>
</tbody>
</table>

### 12.3 System conversion to IPv6 workflow

#### 12.3.1 Description

The following is the sequence of high-level actions required to convert a standalone or redundant NFM-P system from IPv4 to IPv6 inter-component communication.

#### 12.3.2 Stages

1. Perform the pre-conversion tasks; see 12.4 “To perform the pre-conversion tasks” (p. 503).

2. To convert a standalone NFM-P system to IPv6, perform 12.5 “To convert a standalone NFM-P system to IPv6” (p. 508).

3. To convert a redundant NFM-P system to IPv6, perform 12.6 “To convert a redundant NFM-P system to IPv6” (p. 518).

### 12.4 To perform the pre-conversion tasks

#### 12.4.1 Description

The following steps describe the actions that you must perform in advance of a standalone or redundant NFM-P system conversion to IPv6.

**Note:** You require the following user privileges:
To perform the pre-conversion tasks

- on the main server station and each auxiliary server station — root, nsp
- on the main database station — root

**Note:** The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:

- # — root user
- bash$ — nsp

### 12.4.2 Steps

#### Perform security preconfiguration

1. If the NFM-P TLS certificate requires an update to function in the IPv6 system, generate and distribute the required TLS files for the system, as described in 6.11 "Workflow for manual TLS deployment" (p. 105).

#### Clear failed deployments

2. Clear all outstanding failed deployments; see "To view and manage failed deployments" in the *NSP NFM-P User Guide*.

#### Back up configuration files

3. Make a backup copy of the `/opt/nsp/nfmp/server/nms/config/nms-server.xml` file on each main server station.

4. Copy the file to a secure location that is unaffected by the conversion.

#### Gather required information

5. Obtain and record the following information for each main database:
   - root user password

6. Obtain and record the following information for each main and auxiliary server:
   - root user password
Close unrequired clients

7

Close the open NFM-P GUI and XML API client sessions.
1. Open an NFM-P GUI client using an account with security management privileges, such as admin.
3. Click on the Sessions tab.
4. Click Search. The form lists the open GUI and XML API client sessions.
5. Identify the GUI session that you are using based on the value in the Client IP column.
6. Select all sessions except your current session and click Close Session.
7. Click Yes to confirm the action.
8. Click Search to refresh the list and verify that only the current session is open.

Close LogViewer

8

Close the LogViewer utility, if it is open.

Verify database archive log synchronization

9

If the NFM-P system is redundant, ensure that no database archive log gap exists between the primary and standby main databases.

Note: If you attempt a conversion to IPv6 when an archive log gap exists, the conversion fails.

1. In the open client GUI, view the Standby DB entry in the status bar.
2. If the entry reads "Database archive log gap", you must reinstantiate the standby database. Otherwise, go to Step 10.
3. Choose Administration→System Information from the main menu. The System Information form opens.
4. Click Re-Instantiate Standby.
5. Click Yes to confirm the action. The reinstatiation begins, and the GUI status bar displays reinstatiation information.

Note: Database reinstatiation takes considerable time if the database contains a large amount of statistics data.
You can also use the System Information form to monitor the reinstatiation progress. The Last Attempted Standby Re-instantiation Time is the start time; the Standby Re-instantiation State changes from In Progress to Success when the reinstatiation is complete.

6. When the reinstatiation is complete, close the System Information form.

Verify database alignment

10

If the NFM-P system is redundant, ensure that the main database that you want as the primary database is the current primary database.

Note: This step may involve a main database switchover, which can take considerable time.

1. In the open client GUI, choose Administration→System Information from the main menu. The System Information form opens.

2. View the IPAddress and Hostname values in the Primary Database Server panel and the PreferredDB setting in the Primary Server panel.

3. If the PreferredDB value does not match the IPAddress value, perform a database switchover. See the “NFM-P database management” chapter of the NSP NFM-P System Administrator Guide for information about performing a database switchover.

Back up database

11

CAUTION
Data Loss

The path of the main database backup directory must not include the main database installation directory, or data loss may occur.

Ensure that the backup directory path that you specify does not include /opt/nsp/nfmp/db.

Note: Before the NFM-P performs a database backup, it deletes the contents of the specified backup directory. Ensure that the backup directory that you specify does not contain files that you want to retain.

You must perform a database backup before you convert an NFM-P system to IPv6. Perform one of the following NSP NFM-P System Administrator Guide procedures to back up the main database:

- “To back up the main database from the client GUI”
- “To back up the main database from a CLI”
Update hostname mappings

12

Update the /etc/hosts file on each main server, main database, and auxiliary server station, as required, to associate each component hostname with an IPv6 address instead of an IPv4 address.

END OF STEPS
NFM-P system conversion to IPv6

12.5 To convert a standalone NFM-P system to IPv6

12.5.1 Description

The following steps describe how to change the communication between components in a standalone NFM-P system from IPv4 to IPv6. Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

**Note:** You require the following user privileges:
- on each main and auxiliary server station — root, nsp
- on each main database station — root

**Note:** The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:
- `#` — root user
- `bash$` — nsp user

12.5.2 Steps

**Disable automatic main server startup**

1

Prevent the main server from starting in the event of a power disruption during the conversion.

1. Log in to the main server station as the root user.
2. Open a console window.
3. Enter the following:
   ```
   # systemctl disable nfmp-main-config.service
   ```
4. Enter the following:
   ```
   # systemctl disable nfmp-main.service
   ```

**Stop main server**

2

**Note:** This step marks the beginning of the network management outage.

Stop the main server.

1. Enter the following to switch to the nsp user:
   ```
   # su - nsp
   ```
2. Enter the following:
3. Enter the following:

```
bash$ ./nmsserver.bash stop
```

4. Enter the following:

```
bash$ ./nmsserver.bash appserver_status
```

The server status is displayed; the server is fully stopped if the status is the following:

Application Server is stopped

If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform
the next step until the server is fully stopped.

Stop main database

Stop the main database and proxy services.
1. Log in to the main database station as the root user.
2. Open a console window.
3. Enter the following to stop the Oracle proxy:

```
# systemctl stop nfmp-oracle-proxy.service
```

4. Enter the following to stop the main database:

```
# systemctl stop nfmp-main-db.service
```

Configure main database

Enter the following:

```
# samconfig -m db
```

The following is displayed:

Start processing command line inputs...

<db>

Enter the following:

```
<db> configure ip address
```

where address is the IPv6 address that the other NFM-P components must use to reach the
database

The prompt changes to <db configure>. 

---

Release 18.9
September 2018
Issue 1

3HE-14075-AAAC-TQZZA 509
If required, configure the **ip-validation** parameters in the following table to enable IP validation, which restricts database access to only the specified server components, and then enter `back`.

**Note:** When you enable IP validation on an NFM-P system that includes one or more statistics-collection auxiliary servers, you must configure the `remote-servers` parameter; otherwise, the servers cannot reach the database.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>main-one</td>
<td>Public IPv6 address of main server</td>
</tr>
<tr>
<td></td>
<td>Configuring the parameter enables IP validation.</td>
</tr>
<tr>
<td>remote-servers</td>
<td>Comma-separated list of the public IPv6 addresses of the statistics-collection auxiliary servers.</td>
</tr>
</tbody>
</table>

Verify the database configuration.

1. Enter the following:
   
   `<db configure> show-detail`
   
   The database configuration is displayed.

2. Review each parameter to ensure that the value is correct.

3. Configure one or more parameters, if required; see Chapter 3, “Using samconfig” for information about using the samconfig utility.

4. When you are certain that the configuration is correct, enter the following:

   `<db configure> back`

   The prompt changes to `<db>`.

Enter the following to apply the configuration changes:

```bash
<db> apply
```

The changes are applied.

Enter the following:

```bash
<db> exit
```

The samconfig utility closes.
Configure auxiliary servers

10

If the NFM-P system includes auxiliary servers, perform Step 11 to Step 21 on each auxiliary server station. Otherwise, go to Step 22.

11

Stop the auxiliary server.
1. Log in to the auxiliary server station as the nsp user.
2. Open a console window.
3. Enter the following:
   ```bash
   cd /opt/nsp/nfmp/auxserver/nms/bin
   ```
4. Enter the following:
   ```bash
   ./auxnmsserver.bash auxstop
   ```
5. Enter the following:
   ```bash
   ./auxnmsserver.bash auxappserver_status
   ```
   The auxiliary server is stopped when the following message is displayed:
   Auxiliary Server is stopped
   If the command output indicates that the server is not completely stopped, wait five minutes and then re-enter the command in this step to check the server status.
   Do not proceed to the next step until the server is completely stopped.

12

Enter the following to switch to the root user:
```bash
su -
```

13

Enter the following:
```bash
# samconfig -m aux
```
The following is displayed:
Start processing command line inputs...
<aux>

14

Enter the following:
```bash
<aux> configure ip address
```
where address is the auxiliary server IPv6 address that the managed NEs must use to reach the auxiliary server
The prompt changes to <aux configure>.
Enter the following, and then enter `back` ↓.

```xml
<aux configure> main-server ip-one address ↓
```

where `address` is the main server IPv6 address that the auxiliary server must use to reach the main server.

---

Enter the following:

```xml
<aux configure> data-sync local-ip address ↓
```

where `address` is the IPv6 address of the interface on this station that the peer auxiliary server in an auxiliary server pair must use to reach this auxiliary server.

The prompt changes to `<aux configure data-sync>`.

---

Enter the following, and then enter `back` ↓.

```xml
<aux configure data-sync> peer-ip address ↓
```

where `address` is the IPv6 address of the interface on the peer auxiliary server station in an auxiliary server pair that this auxiliary server must use to reach the other auxiliary server.

---

If the XML API clients require IPv6 access, enter the following, and then enter `back` ↓.

```xml
<aux configure> oss public-ip address ↓
```

where `address` is the IPv6 address that the XML API clients must use to reach the auxiliary server.

---

Verify the auxiliary server configuration.

1. Enter the following:

   ```xml
   <aux configure> show-detail ↓
   ```

   The auxiliary server configuration is displayed.

2. Review each parameter to ensure that the value is correct.

3. Configure one or more parameters, if required; see Chapter 3, “Using samconfig” for information about using the samconfig utility.

4. When you are certain that the configuration is correct, enter the following:

   ```xml
   <aux configure> back ↓
   ```

   The prompt changes to `<aux>`.

---

Enter the following:

```xml
<aux> apply ↓
```
The configuration is applied.

Enter the following:

<aux> exit

The samconfig utility closes.

Configure main server

Enter the following:

# samconfig -m main

The following is displayed:

Start processing command line inputs...

<main>

Enter the following:

<main> configure ip address

where address is the main server IPv6 address that the database must use to reach the main server.

The prompt changes to <main configure>.

As required, configure the client parameters as described in the following table, and then enter back.

Table 12-3  Standalone main server parameters — client

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| nat       | Not applicable to IPv6  
If the parameter is enabled, disable the parameter. |
| hostname  | The main server hostname, if the GUI clients, XML API clients, and auxiliary servers are to use hostnames, rather than IP addresses, for communication with the main server  
Modify the value if the hostname changes as part of the conversion to IPv6.  
If the TLS certificate contains the FQDN, you must use the FQDN value to configure the hostname parameter. |
Table 12-3  Standalone main server parameters — client  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>public-ip</td>
<td>The IPv6 address that the GUI and XML API clients must use to reach the main server. The parameter is configurable and mandatory when the hostname parameter is unconfigured.</td>
</tr>
</tbody>
</table>
| delegates | A list of the client delegate servers, in the following format: 
- address1;path1,address2;path2...addressN;pathN 
where 
an address value is a client delegate server IP address 
a path value is the absolute file path of the client delegate server installation location 
Replace each IPv4 address with the appropriate IPv6 address. |

25

Enter the following, and then enter `back ↵`.

```
<main configure> database ip address 
```

where `address` is the IPv6 address of the database

26

If you need to enable IPv6 for communication with the managed network, enter the following, and then enter `back ↵`.

```
<main configure> mediation snmp-ipv6 address 
```

where `address` is the main server IPv6 address that the managed NEs must use to reach the main server

The prompt changes to `<main configure mediation>`.

27

To disable IPv4 for communication with the managed network, perform the following steps.

1. Enter the following:
   ```
   <main configure> mediation no snmp-ipv4 
   ```
2. Enter the following:
   ```
   <main configure mediation> no nat 
   ```
3. Enter the following:
   ```
   <main configure mediation> back 
   ```

28

Perform one of the following.

a. If the NFM-P system does not include auxiliary servers, and the XML API clients require IPv6
access, enter the following, and then enter `back`:

```
<main configure> oss public-ip address
```

where `address` is the IPv6 address that the XML API clients must use to reach the main server

b. If the NFM-P system includes auxiliary servers, configure the `aux` parameters in the following table, and then enter `back`:

Table 12-4  Standalone main server parameters — aux

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-to-auxes</td>
<td>The primary main server IPv6 address that the auxiliary servers must use to reach the main server</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>preferred-list</td>
<td>Comma-separated list of Preferred auxiliary server IPv6 addresses</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>reserved-list</td>
<td>Comma-separated list of Reserved auxiliary server IPv6 addresses</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>peer-list</td>
<td>Comma-separated list of Remote auxiliary server IPv6 addresses</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
</tbody>
</table>

Configure the `tls` parameters in the following table, and then enter `back`:

Table 12-5  Standalone main server parameters — tls

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keystore-file</td>
<td>The absolute path of the TLS keystore file</td>
</tr>
<tr>
<td></td>
<td>To enable automated TLS deployment, enter <code>no keystore-file</code>.</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>keystore-pass</td>
<td>The TLS keystore password</td>
</tr>
<tr>
<td></td>
<td>Default: available from technical support</td>
</tr>
<tr>
<td>truststore-file</td>
<td>The absolute path of the TLS truststore file</td>
</tr>
<tr>
<td></td>
<td>To enable automated TLS deployment, enter <code>no truststore-file</code>.</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>truststore-pass</td>
<td>The TLS truststore password</td>
</tr>
<tr>
<td></td>
<td>Default: available from technical support</td>
</tr>
</tbody>
</table>
Table 12-5  Standalone main server parameters — tls  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alias</td>
<td>The alias specified during keystore generation</td>
</tr>
<tr>
<td></td>
<td>You must configure the parameter.</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>pki-server</td>
<td>If you are using the automated TLS deployment method, the IP address or host name of the PKI server</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>pki-server-port</td>
<td>If you are using the automated TLS deployment method, the TCP port on which the PKI server listens for and services requests</td>
</tr>
<tr>
<td></td>
<td>Default: 2391</td>
</tr>
<tr>
<td>webdav</td>
<td>Whether WebDAV access to eNodeB activation data is enabled on the main server</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
</tbody>
</table>

30

Perform one of the following to specify the registry servers for NSP inter-module communication:

a. If the NSP system includes the NSD and NRC, specify the IP address of each NSD and NRC server; enter the following:
   <main configure> registry ip-list address1;address2 back 
   where address1 and address2 are the public IP addresses of the NSD and NRC servers

   **Note:** If the NSD and NRC system is standalone, only address1 is required.

b. If the NSP system includes only the NFM-P, enter the following:
   <main configure> registry ip-list address back 
   where address is the main server private IPv6 address

31

Verify the main server configuration.

1. Enter the following:
   <main configure> show-detail
   The main server configuration is displayed.

2. Review each parameter to ensure that the value is correct.

3. Configure one or more parameters, if required; see Chapter 3, “Using samconfig” for information about using the samconfig utility.

4. When you are certain that the configuration is correct, enter the following:
   <main configure> back
   The prompt changes to <main>.
Enter the following:
<main> apply</main>
The configuration is applied.

Enter the following:
<main> exit</main>
The samconfig utility closes.

Start main server

Enter the following to enable the main server startup:

```
# systemctl enable nfmp-main.service
```

Start the main server.
1. Log in as the nsp user on the main server station.
2. Open a console window.
3. Enter the following:
   ```
bash$ cd /opt/nsp/nfmp/server/nms/bin
   ```
4. Enter the following:
   ```
bash$ ./nmsserver.bash start
   ```
5. Enter the following:
   ```
bash$ ./nmsserver.bash appserver_status
   ```
   The server status is displayed; the server is fully initialized if the status is the following:
   Application Server process is running. See nms_status for more detail.
   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

Start auxiliary servers

If the NFM-P system includes auxiliary servers, start each auxiliary server.
1. Log in to the auxiliary server station as the nsp user.
2. Open a console window.
3. Enter the following:
NFM-P conversion to IPv6
NFM-P system conversion to IPv6
To convert a redundant NFM-P system to IPv6

```
bash$ /opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash auxstart
```

The auxiliary server starts.

Verify converted system using GUI client

37

Use an NFM-P GUI client to perform sanity testing of the converted system.

Note: If an IP address is specified for NFM-P client access, ensure that you use the IPv6 address, rather than the IPv4 address, for the client connection.

---

12.6 To convert a redundant NFM-P system to IPv6

12.6.1 Description

The following steps describe how to change the communication between components in a redundant NFM-P system from IPv4 to IPv6. Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

Note: You require the following user privileges:

- on each main and auxiliary server station — root, nsp
- on each main database station — root

Note: The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:

- # — root user
- bash$ — nsp user

12.6.2 Steps

Disable automatic startup, standby main server

1

Prevent the standby main server from starting in the event of a power disruption during the conversion.

1. Log in as the root user on the standby main server station.
2. Open a console window.
3. Enter the following:

   ```
   # systemctl disable nfmp-main-config.service
   ```
4. Enter the following:

   ```
   # systemctl disable nfmp-main.service
   ```
Stop standby main server

Stop the standby main server.
1. Enter the following to switch to the nsu user:
   
   ```bash
   # su - nsu
   ```

2. Enter the following:
   
   ```bash
   bash$ cd /opt/nsp/nfmp/server/nms/bin
   ```

3. Enter the following:
   
   ```bash
   bash$. /nmsserver.bash stop
   ```

4. Enter the following:
   
   ```bash
   bash$. /nmsserver.bash appserver_status
   ```

   The server status is displayed; the server is fully stopped if the status is the following:

   Application Server is stopped

   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform
   the next step until the server is fully stopped.

Stop reserved auxiliary servers

If the NFM-P system includes auxiliary servers, perform the following steps on each reserved
auxiliary server station.

1. Log in to the auxiliary server station as the nsu user.

2. Open a console window.

3. Enter the following:
   
   ```bash
   bash$ /opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash auxstop
   ```

   The auxiliary server stops.

Stop standby main database

Stop the standby database and proxy services.

1. Log in to the standby main database station as the root user.

2. Open a console window.

3. Enter the following to stop the Oracle proxy:
   
   ```bash
   # systemctl stop nfmp-oracle-proxy.service
   ```

4. Enter the following to stop the main database:
   
   ```bash
   # systemctl stop nfmp-main-db.service
   ```
Disable automatic startup, primary main server

5

Prevent the primary main server from starting in the event of a power disruption during the conversion.

1. Log in to the primary main server station as the root user.
2. Open a console window.
3. Enter the following:
   
   ```
   # systemctl disable nfmp-main-config.service
   ```
4. Enter the following:
   
   ```
   # systemctl disable nfmp-main.service
   ```

Stop primary main server

6

Stop the primary main server.

ℹ️ Note: This step marks the beginning of the network management outage.

1. Enter the following to switch to the nsp user:
   
   ```
   # su - nsp
   ```
2. Enter the following:
   
   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin
   ```
3. Enter the following:
   
   ```
   bash$ ./nmsserver.bash stop
   ```
4. Enter the following:
   
   ```
   bash$ ./nmsserver.bash appserver_status
   ```
   
   The server status is displayed; the server is fully stopped if the status is the following:
   
   Application Server is stopped
   
   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

Stop preferred auxiliary servers

7

If the NFM-P system includes auxiliary servers, perform the following steps on each preferred auxiliary server station.

1. Log in as the nsp user.
2. Open a console window.
3. Enter the following:
   
   ```
   bash$ /opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash auxstop
   ```
The auxiliary server stops.

Stop primary main database

8

Stop the primary database and proxy services.
1. Log in to the primary main database station as the root user.
2. Open a console window.
3. Enter the following to stop the Oracle proxy:
   
   ```
   # systemctl stop nfmp-oracle-proxy.service
   ```
4. Enter the following to stop the main database:
   
   ```
   # systemctl stop nfmp-main-db.service
   ```

Configure primary main database

9

Enter the following:

```bash
# samconfig -m db
```

The following is displayed:

Start processing command line inputs...
<db>

10

Enter the following:

```bash
<db> configure ip address
```

where `address` is the IPv6 address of this database

The prompt changes to `<db configure>`.

11

Enter the following, and then enter `back`:

```bash
<db configure> redundant ip address
```

where `address` is the IPv6 address of the peer database

12

If required, configure the `ip-validation` parameters in the following table to enable IP validation, which restricts database access to only the specified server components, and then enter `back`:

Note: When you enable IP validation on an NFM-P system that includes one or more statistics-collection auxiliary servers, you must configure the `remote-servers` parameter; otherwise, the servers cannot reach the database.
Verify the database configuration.

1. Enter the following:
   ```
   <db configure> show-detail
   ```
   The database configuration is displayed.

2. Review each parameter to ensure that the value is correct.

3. Configure one or more parameters, if required; see Chapter 3, “Using samconfig” for information about using the samconfig utility.

4. When you are certain that the configuration is correct, enter the following:
   ```
   <db configure> back
   ```
   The prompt changes to <db>.

Enter the following to apply the configuration changes:

```sql
<db> apply
```
The changes are applied.

Enter the following:

```sql
<db> exit
```
The samconfig utility closes.

Enter the following:

```
# ssh-keyscan -t rsa standby_database_IPv6_address
>>/opt/nsp/nfmp/oracle12r1/.ssh/known_hosts
```
where `standby_database_IPv6_address` is the IPv6 address that you are assigning to the standby main database.
Configure primary main server

17 Log in as the root user on the primary main server station.

18 Open a console window.

19 Enter the following:
```
# samconfig -m main
```
The following is displayed:
```
Start processing command line inputs...
<main>
```

20 Enter the following:
```
<main> configure ip address
```
where **address** is the main server IPv6 address that each database must use to reach the main server
The prompt changes to `<main configure>`.

21 As required, configure the **client** parameters as described in the following table, and then enter **back**.

*Table 12-7  Primary main server parameters — client*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| nat         | Not applicable to IPv6  
If the parameter is enabled, disable the parameter. |
| hostname    | The main server hostname, if the GUI clients, XML API clients, and auxiliary servers are to use hostnames, rather than IP addresses, for communication with the main server  
Modify the value if the hostname changes as part of the conversion to IPv6.  
If the TLS certificate contains the FQDN, you must use the FQDN value to configure the hostname parameter. |
**Table 12-7** Primary main server parameters — client  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>public-ip</td>
<td>The IPv6 address that the GUI and XML API clients must use to reach the main server. The parameter is configurable and mandatory when the hostname parameter is unconfigured.</td>
</tr>
</tbody>
</table>
| delegates  | A list of the client delegate servers, in the following format: 
`address1;path1,address2;path2...addressN;pathN`  
where an address value is a client delegate server IP address  
a path value is the absolute file path of the client delegate server installation location  
Replace each IPv4 address with the appropriate IPv6 address. |

22

Enter the following, and then enter **back ↵**:

```
<main configure> database ip address ↵
```

where *address* is the IPv6 address of the primary database

23

To enable IPv6 for communication with the managed network, enter the following, and then enter **back ↵**:

```
<main configure> mediation snmp-ipv6 address ↵
```

where *address* is the main server IPv6 address that the managed NEs must use to reach the main server

24

To disable IPv4 for communication with the managed network, perform the following steps.

1. Enter the following:
   ```
   <main configure> mediation no snmp-ipv4 ↵
   ```
2. Enter the following:
   ```
   <main configure> no nat ↵
   ```
3. Enter the following:
   ```
   <main configure> back ↵
   ```
   The prompt changes to `<main configure>.

25

Perform one of the following.

a. If the NFM-P system does not include auxiliary servers, and the XML API clients require IPv6
access, enter the following, and then enter back ↓:

```
<main configure> oss public-ip address ↓
```

where address is the IPv6 address that the XML API clients must use to reach the main server

b. If the NFM-P system includes auxiliary servers, configure the aux parameters in the following table, and then enter back ↓.

**Table 12-8 Primary main server parameters — aux**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| ip-to-auxes    | The primary main server IPv6 address that the auxiliary servers must use to reach the main server  
                  Default: —                                                                                             |
| preferred-list | Comma-separated list of Preferred auxiliary server IPv6 addresses  
                  Default: —                                                                                             |
| reserved-list  | Comma-separated list of Reserved auxiliary server IPv6 addresses  
                  Default: —                                                                                             |
| peer-list      | Comma-separated list of Remote auxiliary server IPv6 addresses  
                  Default: —                                                                                             |

If required, configure the tls parameters in the following table, and then enter back ↓.

**Table 12-9 Primary main server parameters — tls**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| keystore-file  | The absolute path of the TLS keystore file  
                  To enable automated TLS deployment, enter `no keystore-file`.  
                  Default: —                                                                                             |
| keystore-pass  | The TLS keystore password  
                  Default: available from technical support                                                                 |
| truststore-file| The absolute path of the TLS truststore file  
                  To enable automated TLS deployment, enter `no truststore-file`.  
                  Default: —                                                                                             |
| truststore-pass| The TLS truststore password  
                  Default: available from technical support                                                                 |
Table 12-9  Primary main server parameters — tls (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alias</td>
<td>The alias specified during keystore generation. You must configure the parameter. Default: —</td>
</tr>
<tr>
<td>pki-server</td>
<td>If you are using the automated TLS deployment method, the IP address or hostname of the PKI server. Default: —</td>
</tr>
<tr>
<td>pki-server-port</td>
<td>If you are using the automated TLS deployment method, the TCP port on which the PKI server listens for and services requests. Default: 2391</td>
</tr>
<tr>
<td>webdav</td>
<td>Whether WebDAV access to eNodeB activation data is enabled. Default: false</td>
</tr>
</tbody>
</table>

27 Enter the following:

<main configure> redundancy enabled

The prompt changes to <main configure redundancy>.

28 Enter the following:

<main configure redundancy> ip-to-peer address

where address is the IPv6 address that the peer main server must use to reach this main server for general communication.

29 Enter the following:

<main configure redundancy> rsync-ip address

where address is the IPv6 address that the peer main server must use to reach this main server for data synchronization.

30 Enter the following, and then enter back:

<main configure redundancy> database ip address

where address is the IPv6 address of the standby database.

31 Configure the peer-server redundancy parameters in the following table, and then enter back.
Table 12-10  Primary main server parameters — redundancy, peer-server

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| ip          | The IPv6 address that this main server must use to reach the peer main server for general communication  
               Default: —                                                                                                                                 |
| rsync-ip    | The IPv6 address that this main server must use to reach the peer main server for data synchronization 
               Default: —                                                                                                                                 |
| public-ip   | The IPv6 address that the GUI and XML API clients must use to reach the peer main server  
               The parameter is configurable if the public-ip parameter is configured in Step 21. 
               Default: —                                                                                                                                 |
| hostname    | The hostname that the GUI and XML API clients must use to reach the peer main server  
               The parameter is configurable if the hostname parameter is configured in Step 21. 
               Default: —                                                                                                                                 |
| ip-to-auxes | The IPv6 address that the auxiliary servers must use to reach the peer main server  
               You must configure the parameter if the NFM-P system includes one or more auxiliary servers. 
               Default: —                                                                                                                                 |
| snmp-ipv6   | The IPv6 address that the managed NEs must use to reach the peer main server  
               Configure the parameter only if you need to enable IPv6 for communication with managed NEs |

32

Enter the following:

<main configure redundancy> back

The prompt changes to <main configure>.

33

Perform one of the following to specify the registry servers for NSP inter-module communication:

a. If the NSP system includes the NSD and NRC, specify the IP address of each NSD and NRC server; enter the following:

<main configure> registry ip-list address1;address2 back

where address1 and address2 are the public IP addresses of the NSD and NRC servers
**Note:** If the NSD and NRC system is standalone, only address1 is required.

b. If the NSP system includes only the NFM-P, enter the following:

```bash
<main configure> registry ip-list address1;address2 back
```

where address1 and address2 are the IP addresses that the NFM-P main servers use to communicate with each other.

---

34

Verify the main server configuration.

1. Enter the following:

```bash
<main configure> show-detail
```

The main server configuration is displayed.

2. Review each parameter to ensure that the value is correct.

3. Configure one or more parameters, if required; see Chapter 3, “Using samconfig” for information about using the samconfig utility.

4. When you are certain that the configuration is correct, enter the following:

```bash
<main configure> back
```

The prompt changes to `<main>`.

---

35

Enter the following:

```bash
<main> apply
```

The configuration is applied.

---

36

Enter the following:

```bash
<main> exit
```

The samconfig utility closes.

**Configure preferred auxiliary servers**

---

37

If the NFM-P system does not include auxiliary servers, go to Step 52. Otherwise, perform Step 38 to Step 50 on each preferred auxiliary server station.

---

38

Log in as the root user.

---

39

Open a console window.
Enter the following:
```
# samconfig -m aux
```
The following is displayed:
```
Start processing command line inputs...
<aux>
```

Enter the following:
```
<aux> configure ip address
```
where `address` is the auxiliary server IPv6 address that the managed NEs must use to reach the auxiliary server.
The prompt changes to `<aux configure>`.

Enter the following:
```
<aux configure> main-server ip-one address
```
where `address` is the IPv6 address that the auxiliary server must use to reach the primary main server.
The prompt changes to `<aux configure main-server>`.

Enter the following, and then enter `back`:
```
<aux configure main-server> ip-two address
```
where `address` is the IPv6 address that the auxiliary server must use to reach the standby main server.

Enter the following:
```
<aux configure> data-sync local-ip address
```
where `address` is the IPv6 address of the interface on this station that the peer auxiliary server in an auxiliary server pair must use to reach this auxiliary server.
The prompt changes to `<aux configure data-sync>`.

Enter the following, and then enter `back`:
```
<aux configure data-sync> peer-ip address
```
where `address` is the IPv6 address of the interface on the peer auxiliary server station in an auxiliary server pair that this auxiliary server must use to reach the other auxiliary server.
Configure the \texttt{tls} parameters in the following table, and then enter \texttt{back} ↓.

\textbf{Table 12-11} Auxiliary server parameters — tls

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keystore-file</td>
<td>The absolute path of the TLS keystore file \texttt{To enable automated TLS deployment, enter no keystore-file. Default: —}</td>
</tr>
<tr>
<td>keystore-pass</td>
<td>The TLS keystore password \texttt{Default: available from technical support}</td>
</tr>
<tr>
<td>pki-server</td>
<td>If you are using the automated TLS deployment method, the IP address or hostname of the PKI server \texttt{Default: —}</td>
</tr>
<tr>
<td>pki-server-port</td>
<td>If you are using the automated TLS deployment method, the TCP port on which the PKI server listens for and services requests \texttt{Default: 2391}</td>
</tr>
</tbody>
</table>

If the XML API clients require IPv6 access, enter the following, and then enter \texttt{back} ↓:
\texttt{<aux configure> oss public-ip address ↓}

where \texttt{address} is the IPv6 address that the XML API clients must use to reach the auxiliary server.

The prompt changes to \texttt{<aux configure oss>}.  

Verify the auxiliary server configuration.

1. Enter the following:
\texttt{<aux configure> show-detail ↓}

   The auxiliary server configuration is displayed.

2. Review each parameter to ensure that the value is correct.

3. Configure one or more parameters, if required; see Chapter 3, “Using samconfig” for information about using the samconfig utility.  

4. When you are certain that the configuration is correct, enter the following:
\texttt{<aux configure> back ↓}

   The prompt changes to \texttt{<aux>}.  

Enter the following:
\texttt{<aux> apply ↓}
The configuration is applied.

Enter the following:

```bash
<aux> exit
```

The same config utility closes.

### Start preferred auxiliary servers

If the NFM-P system includes auxiliary servers, perform the following steps on each preferred auxiliary server station.

1. Log in as the nsp user.
2. Open a console window.
3. Enter the following:
   ```bash
   bash$ /opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash auxstart
   ```

   The auxiliary server starts.

### Enable automatic startup, primary main server

Enable the automatic startup of the primary main server.

1. Log in as the nsp user on the primary main server station.
2. Open a console window.
3. Enter the following to disable the main server startup:
   ```bash
   # systemctl enable nfmp-main.service
   ```

### Start primary main server

Start the primary main server.

**Note:** The primary main server startup marks the end of the network management outage.

1. Enter the following on the standby main server station:
   ```bash
   # su - nsp
   ```
2. Enter the following:
   ```bash
   bash$ cd /opt/nsp/nfmp/server/nms/bin
   ```
3. Enter the following:
   ```bash
   bash$ ./nmsserver.bash start
   ```
4. Enter the following:
bash$ ./nmsserver.bash appserver_status

The server status is displayed; the server is fully initialized if the status is the following:
Application Server process is running. See nms_status for more detail.

If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

Configure standby main database

54
Log in as the root user on the standby main database station.

55
Open a console window.

56
Enter the following:
# samconfig -m db
The following is displayed:
Start processing command line inputs...
<db>

57
Enter the following:
<db> configure ip address
where address is the IPv6 address that the other NFM-P components must use to reach the standby main database
The prompt changes to <db configure>.

58
Enter the following:
<db configure> redundant ip address
where address is the IPv6 address of the primary database
The prompt changes to <db configure redundant>.

59
Enter the following, and then enter back:
<db configure redundant> instance instance_name
where instance_name is the primary database instance name
If required, configure the ip-validation parameters in the following table to enable IP validation, which restricts database access to only the specified server components, and then enter back.

**Note:** When you enable IP validation on an NFM-P system that includes one or more statistics-collection auxiliary servers, you must configure the remote-servers parameter; otherwise, the servers cannot reach the database.

### Table 12-12  Standby database parameters — ip-validation

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>main-one</td>
<td>Public IPv6 address of standby main server</td>
</tr>
<tr>
<td></td>
<td>Configuring the parameter enables IP validation.</td>
</tr>
<tr>
<td>main-two</td>
<td>Public IPv6 address of primary main server</td>
</tr>
<tr>
<td>remote-servers</td>
<td>Comma-separated list of the public IPv6 addresses of the statistics-collection auxiliary servers</td>
</tr>
</tbody>
</table>

Verify the database configuration.

1. Enter the following:
   ```
   <db configure> show-detail
   ``
   The database configuration is displayed.

2. Review each parameter to ensure that the value is correct.

3. Configure one or more parameters, if required; see Chapter 3, "Using samconfig" for information about using the samconfig utility.

4. When you are certain that the configuration is correct, enter the following:
   ```
   <db configure> back
   ``
   The prompt changes to `<db>`.

Enter the following to apply the configuration changes:

```
<db> apply
```

The changes are applied.

Enter the following:

```
<db> exit
```

The samconfig utility closes.
Enter the following:

```
# ssh-keyscan -t rsa primary_database_IPv6_address
>>/opt/nsp/nfmp/oracle12r1/.ssh/known_hosts
```

where `primary_database_IPv6_address` is the IPv6 address of the primary main database

**Configure standby main server**

65

Log in to the standby main server station as the root user.

66

Open a console window.

67

Enter the following:

```
# samconfig -m main
```

The following is displayed:

Start processing command line inputs...

<main>

68

Enter the following:

```
<main> configure ip address
```

where `address` is the main server IPv6 address that each database must use to reach the main server

The prompt changes to `<main configure>`.

69

As required, configure the client parameters as described in the following table, and then enter `back`.

**Table 12-13  Standby main server parameters — client**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| nat       | Not applicable to IPv6  
            If the parameter is enabled, disable the parameter. |
Table 12-13  Standby main server parameters — client  (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>The main server hostname, if the GUI clients, XML API clients, and auxiliary servers are to use hostnames, rather than IP addresses, for communication with the main server. Modify the value if the hostname changes as part of the conversion to IPv6. If the TLS certificate contains the FQDN, you must use the FQDN value to configure the hostname parameter.</td>
</tr>
<tr>
<td>public-ip</td>
<td>The IPv6 address that the GUI and XML API clients must use to reach the main server. The parameter is configurable and mandatory when the hostname parameter is unconfigured.</td>
</tr>
<tr>
<td>delegates</td>
<td>A list of the client delegate servers, in the following format: address1;path1,address2;path2...addressN;pathN where an address value is a client delegate server IP address and a path value is the absolute file path of the client delegate server installation location. Replace each IPv4 address with the appropriate IPv6 address.</td>
</tr>
</tbody>
</table>

Enter the following, and then enter back ↓:

```
<main configure> database ip address ↓
```

where address is the IPv6 address of the standby database.

If you need to enable IPv6 for communication with the managed network, enter the following, and then enter back ↓:

```
<main configure> mediation snmp-ipv6 address ↓
```

where address is the main server IPv6 address that the managed NEs must use to reach the main server.

If you need to disable IPv4 for communication with the managed network, perform the following steps.

1. Enter the following:
   ```
   <main configure mediation> no snmp-ipv4 ↓
   ```

2. Enter the following:
   ```
   <main configure mediation> no nat ↓
   ```
3. Enter the following:

```
<main configure mediation> back
```

Perform one of the following.

a. If the NFM-P system does not include auxiliary servers, and the XML API clients require IPv6 access, enter the following, and then enter `back`:

```
<main configure> oss public-ip address
```

where `address` is the IPv6 address that the XML API clients must use to reach the main server.

b. If the NFM-P system includes auxiliary servers, configure the `aux` parameters in the following table, and then enter `back`:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-to-auxes</td>
<td>The primary main server IPv6 address that the auxiliary servers must use to reach the main server. Default: —</td>
</tr>
<tr>
<td>preferred-list</td>
<td>Comma-separated list of Preferred auxiliary server IPv6 addresses. Default: —</td>
</tr>
<tr>
<td>reserved-list</td>
<td>Comma-separated list of Reserved auxiliary server IPv6 addresses. Default: —</td>
</tr>
<tr>
<td>peer-list</td>
<td>Comma-separated list of Remote auxiliary server IPv6 addresses. Default: —</td>
</tr>
</tbody>
</table>

The standby main server requires a copy of the NFM-P TLS keystore and truststore files that are used by the primary main server.

Copy the keystore and truststore files from the `/opt/nsp/os/tls` directory on the primary main server station to a temporary location on the standby main server station, and record the location for use in Step 89 Step 75.

**Caution:** You must not copy the files to the `/opt/nsp/os/tls` directory on the standby main server station, or the TLS configuration fails.

**Note:** The `nsp` user must be the owner of the directory path to the location.

Configure the `tls` parameters in the following table, and then enter `back`:

```
Table 12-15  Standby main server parameters — tls

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keystore-file</td>
<td>The absolute path of the TLS keystore file</td>
</tr>
<tr>
<td></td>
<td>To enable automated TLS deployment, enter <code>no keystore-file</code>.</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>keystore-pass</td>
<td>The TLS keystore password</td>
</tr>
<tr>
<td></td>
<td>Default: available from technical support</td>
</tr>
<tr>
<td>truststore-file</td>
<td>The absolute path of the TLS truststore file</td>
</tr>
<tr>
<td></td>
<td>To enable automated TLS deployment, enter <code>no truststore-file</code>.</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>truststore-pass</td>
<td>The TLS truststore password</td>
</tr>
<tr>
<td></td>
<td>Default: available from technical support</td>
</tr>
<tr>
<td>alias</td>
<td>The alias specified during keystore generation</td>
</tr>
<tr>
<td></td>
<td>You must configure the parameter.</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>pki-server</td>
<td>If you are using the automated TLS deployment method, the IP address or</td>
</tr>
<tr>
<td></td>
<td>hostname of the PKI server</td>
</tr>
<tr>
<td></td>
<td>Default: —</td>
</tr>
<tr>
<td>pki-server-port</td>
<td>If you are using the automated TLS deployment method, the TCP port on which</td>
</tr>
<tr>
<td></td>
<td>the PKI server listens for and services requests</td>
</tr>
<tr>
<td></td>
<td>Default: 2391</td>
</tr>
<tr>
<td>webdav</td>
<td>Whether WebDAV access to eNodeB activation data is enabled</td>
</tr>
<tr>
<td></td>
<td>Default: false</td>
</tr>
</tbody>
</table>

Enter the following:

```
<main configure> redundancy enabled
```

The prompt changes to `<main configure redundancy>`.

Enter the following:

```
<main configure redundancy> ip-to-peer address
```

where `address` is the IPv6 address that the peer main server must use to reach this main server for general communication.
<main configure redundancy> rsync-ip address

where address is the IPv6 address that the peer main server must use to reach this main server for data synchronization

Enter the following, and then enter back:
<main configure redundancy> database ip address

where address is the IPv6 address of the primary database

Configure the peer-server redundancy parameters in the following table, and then enter back.

Table 12-16  Standby main server parameters — redundancy, peer-server

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>The IPv6 address that this main server must use to reach the peer main server for general communication</td>
</tr>
<tr>
<td>rsync-ip</td>
<td>The IPv6 address that this main server must use to reach the peer main server for data synchronization</td>
</tr>
<tr>
<td>public-ip</td>
<td>The IPv6 address that the GUI and XML API clients must use to reach the peer main server</td>
</tr>
<tr>
<td>hostname</td>
<td>The hostname that the GUI and XML API clients must use to reach the peer main server</td>
</tr>
<tr>
<td>ip-to-auxes</td>
<td>The IPv6 address that the auxiliary servers must use to reach the peer main server</td>
</tr>
<tr>
<td>snmp-ipv6</td>
<td>The IPv6 address that the managed NEs must use to reach the peer main server</td>
</tr>
</tbody>
</table>

You must configure the parameter if the NFM-P system includes one or more auxiliary servers.

Configure the parameter only if you need to enable IPv6 for communication with managed NEs.
Enter the following:
<main configure redundancy> back

The prompt changes to <main configure>.

Perform one of the following to specify the registry servers for NSP inter-module communication:

a. If the NSP system includes the NSD and NRC, specify the IP address of each NSD and NRC server; enter the following:
<main configure> registry ip-list address1;address2 back

where address1 and address2 are the public IP addresses of the NSD and NRC servers

Note: If the NSD and NRC system is standalone, only address1 is required.

b. If the NSP system includes only the NFM-P, enter the following:
<main configure> registry ip-list address1;address2 back

where address1 and address2 are the IP addresses that the NFM-P main servers use to communicate with each other

Verify the main server configuration.
1. Enter the following:
<main configure> show-detail

The main server configuration is displayed.

2. Review each parameter to ensure that the value is correct.

3. Configure one or more parameters, if required; see Chapter 3, “Using samconfig” for information about using the samconfig utility.

4. When you are certain that the configuration is correct, enter the following:
<main configure> back

The prompt changes to <main>.

Enter the following:
<main> apply

The configuration is applied.

Enter the following:
<main> exit

The samconfig utility closes.
Configure reserved auxiliary servers

86

If the NFM-P system does not include auxiliary servers, go to Step 100. Otherwise, perform Step 87 to Step 98 on each reserved auxiliary server station.

87

Log in as the root user.

88

Enter the following:

```
# samconfig -m aux
```

The following is displayed:

```
Start processing command line inputs...
<aux>
```

89

Enter the following:

```
<aux> configure ip address
```

where `address` is the auxiliary server IPv6 address that the managed NEs must use to reach the auxiliary server.

The prompt changes to `<aux configure>`.

90

Enter the following:

```
<aux configure> main-server ip-one address
```

where `address` is the standby main server IPv6 address that the auxiliary server must use to reach the main server.

The prompt changes to `<aux configure main-server>`.

91

Enter the following, and then enter back:

```
<aux configure main-server> ip-two address
```

where `address` is the primary main server IPv6 address that the auxiliary server must use to reach the main server.

92

Enter the following:

```
<aux configure> data-sync local-ip address
```

where `address` is the IPv6 address of the interface on this station that the peer auxiliary server in an auxiliary server pair must use to reach this auxiliary server.
The prompt changes to `<aux configure data-sync>`.

Enter the following and then enter `back`:

```
<aux configure data-sync> peer-ip address
```

where `address` is the IPv6 address of the interface on the peer auxiliary server station in an auxiliary server pair that this auxiliary server must use to reach the other auxiliary server.

Configure the `tls` parameters in the following table, and then enter `back`:

### Table 12-17 Auxiliary server parameters — `tls`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keystore-file</td>
<td>The absolute path of the TLS keystore file. To enable automated TLS deployment, enter <code>no keystore-file</code>. Default: —</td>
</tr>
<tr>
<td>keystore-pass</td>
<td>The TLS keystore password. Default: available from technical support</td>
</tr>
<tr>
<td>pki-server</td>
<td>If you are using the automated TLS deployment method, the IP address or hostname of the PKI server. Default: —</td>
</tr>
<tr>
<td>pki-server-port</td>
<td>If you are using the automated TLS deployment method, the TCP port on which the PKI server listens for and services requests. Default: 2391</td>
</tr>
</tbody>
</table>

If the XML API clients require IPv6 access, enter the following, and then enter `back`:

```
<aux configure> oss public-ip address
```

where `address` is the IPv6 address that the XML API clients must use to reach the auxiliary server.

Verify the auxiliary server configuration.

1. Enter the following:
   ```
   <aux configure> show-detail
   ```
   The auxiliary server configuration is displayed.
2. Review each parameter to ensure that the value is correct.
3. Configure one or more parameters, if required; see Chapter 3, "Using samconfig" for information about using the samconfig utility.
4. When you are certain that the configuration is correct, enter the following:

`<aux configure> back`

The prompt changes to `<aux>`.

---

Enter the following:

`<aux> apply`

The configuration is applied.

---

Enter the following:

`<aux> exit`

The samconfig utility closes.

**Start reserved auxiliary servers**

99

If the NFM-P system includes auxiliary servers, perform the following steps on each reserved auxiliary server station.

1. Log in as the nsp user.
2. Open a console window.
3. Enter the following:
   ```bash
   /opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash auxstart
   ```

   The auxiliary server starts.

**Enable automatic startup, standby main server**

100

Enable the automatic startup of the standby main server.

1. Log in to the standby main server station as the root user.
2. Open a console window.
3. Enter the following to disable the main server startup:
   ```bash
   systemctl enable nfmp-main.service
   ```

**Start standby main server**

101

Start the standby main server.

1. Enter the following to switch to the nsp user:
   ```bash
   su - nsp
   ```
2. Enter the following:
   
   ```bash
   cd /opt/nsp/nfmp/server/nms/bin
   ```

3. Enter the following:
   
   ```bash
   ./nmsserver.bash start
   ```

4. Enter the following:
   
   ```bash
   ./nmsserver.bash appserver_status
   ```

   The server status is displayed; the server is fully initialized if the status is the following:
   
   Application Server process is running. See nms_status for more detail.

   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

**Verify converted system using GUI client**

Use an NFM-P GUI client to perform sanity testing of the converted system.

**Note:** If IP addresses are specified for NFM-P client access, ensure that you use the required IPv6 address, rather than the IPv4 address, for the client connection.
To convert a redundant NFM-P system to IPv6
13 NFM-P uninstallation

13.1 Overview

13.1.1 Purpose

This chapter describes how to uninstall the software components of a standalone or redundant NFM-P system.

13.1.2 Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.1 Overview</td>
<td>545</td>
</tr>
<tr>
<td>13.2 Introduction</td>
<td>545</td>
</tr>
<tr>
<td>13.3 NFM-P system uninstallal workflow</td>
<td>546</td>
</tr>
<tr>
<td>13.4 To uninstall an NSP Flow Collector</td>
<td>547</td>
</tr>
<tr>
<td>13.5 To uninstall an auxiliary server</td>
<td>548</td>
</tr>
<tr>
<td>13.6 To uninstall an auxiliary database</td>
<td>550</td>
</tr>
<tr>
<td>13.7 To uninstall a main server</td>
<td>552</td>
</tr>
<tr>
<td>13.8 To uninstall a main database</td>
<td>554</td>
</tr>
</tbody>
</table>

13.2 Introduction

13.2.1 Description

This chapter describe how to uninstall the following NFM-P components:

- main server
- main database
- auxiliary database
- auxiliary server
- NSP Flow Collector

The following chapters describe GUI client uninstallation:

- Chapter 14, “Single-user client deployment”
- Chapter 15, “Client delegate server deployment”

**Note:** The uninstallation of an NFM-P component does not remove any associated RHEL Firewalld chains.

**Note:** The Bash shell is the supported command shell for RHEL CLI operations.
Complete NFM-P system uninstallation

13.3 “NFM-P system uninstallation workflow” (p. 546) describes how to install a complete NFM-P system.

A complete NFM-P system uninstallation has the following requirements.
• No NFM-P component is running when the uninstallation begins.
• You must uninstall the NFM-P components in the reverse order of the installation.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.4 “To uninstall an NSP Flow Collector” (p. 547)</td>
<td>Remove the NSP Flow Collector software.</td>
</tr>
<tr>
<td>13.5 “To uninstall an auxiliary server” (p. 548)</td>
<td>Remove the NFM-P auxiliary server software.</td>
</tr>
<tr>
<td>13.6 “To uninstall an auxiliary database” (p. 550)</td>
<td>Remove the NFM-P auxiliary database software.</td>
</tr>
<tr>
<td>13.7 “To uninstall a main server” (p. 552)</td>
<td>Remove the NFM-P main server software.</td>
</tr>
<tr>
<td>13.8 “To uninstall a main database” (p. 554)</td>
<td>Remove the main database software.</td>
</tr>
</tbody>
</table>

13.3 NFM-P system uninstallation workflow

13.3.1 Description
The following is the sequence of high-level actions required to uninstall a standalone or redundant NFM-P system.

13.3.2 Stages

1
Uninstall the single-user GUI clients; see Chapter 14, “Single-user client deployment”.

2
Uninstall the client delegate servers; see Chapter 15, “Client delegate server deployment”.

3
If the system includes one or more NSP Flow Collectors, perform 13.4 “To uninstall an NSP Flow Collector” (p. 547) on each NSP Flow Collector.

4
If the system includes one or more auxiliary servers, perform 13.5 “To uninstall an auxiliary server” (p. 548).

5
If the system includes an auxiliary database, perform 13.6 “To uninstall an auxiliary database” (p. 550).
6 Uninstall each main server, or remove all NSP software from a collocated main server and database station; perform 13.7 “To uninstall a main server” (p. 552).

7 Uninstall each main database; perform 13.8 “To uninstall a main database” (p. 554).

13.4 To uninstall an NSP Flow Collector

13.4.1 Description

The following steps describe how to remove the NSP Flow Collector software from a station.

- **Note:** You require root user privileges on the NSP Flow Collector station.
- **Note:** A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

13.4.2 Steps

1 Log in to the NSP Flow Collector station as the root user.

2 Open a console window.

3 Stop the NSP Flow Collector; enter the following:

```
# /opt/nsp/flow/dcp/bin/dcpctl.sh stop
```

The command displays a series of status messages as the NSP Flow Collector stops.

- **Note:** To stop the NSP Flow Collector without displaying status messages, you can use the following command:

```
# systemctl stop nsp-flow-collector.service
```

4 Enter the following commands in sequence to remove the software packages:

```
# yum remove nsp-flow-collector
# yum remove nsp-nfmp-config
# yum remove nsp-nfmp-jre
```

After you enter a command, the yum utility resolves any dependencies and displays the following prompt:

```
Installed size: nn M
```
Is this ok [y/N]:

Enter y. The following is displayed:
- Downloading packages:
- Running transaction check
- Running transaction test
- Transaction test succeeded
- Running transaction
- Uninstalling the NSP package...

As each package removal completes, the following is displayed:
- Complete!

Return to Step 4 as required to remove the next package in the sequence.

When all packages are removed, enter the following to reboot the station:

```
# systemctl reboot
```

The station reboots.

Remove the /opt/nsp/flow directory and contents.

Close the console window.

END OF STEPS

13.5 To uninstall an auxiliary server

13.5.1 Description

The following steps describe how to remove the NFM-P auxiliary server software from a station.

**Note:** In a redundant NFM-P system, you must uninstall the auxiliary servers in the following order:
- reserved auxiliary servers of primary main server
- preferred auxiliary servers of primary main server

**Note:** You require the following user privileges on the auxiliary server station:
- root
13.5.2 Steps

1. Stop the auxiliary server.
   
   1. Log in to the auxiliary server station as the nsp user.
   2. Open a console window.
   3. Enter the following:
      
      ```bash
      cd /opt/nsp/nfmp/auxserver/nms/bin
      ```
   4. Enter the following:
      
      ```bash
      ./auxnmsserver.bash auxstop
      ```
   5. Enter the following:
      
      ```bash
      ./auxnmsserver.bash auxappserver_status
      ```
      
      The auxiliary server is stopped when the following message is displayed:
      
      Auxiliary Server is stopped
      
      If the command output indicates that the server is not completely stopped, wait five minutes and then re-enter the command in this step to check the server status. Do not proceed to the next step until the server is completely stopped.

2. Enter the following to switch to the root user:
   
   ```bash
   su -
   ```

3. Enter the following commands in sequence to remove the NFM-P packages:
   
   ```bash
   # yum remove nsp-nfmp-aux-server
   # yum remove nsp-nfmp-config
   # yum remove nsp-nfmp-jre
   ```
   
   After you enter a command, the yum utility resolves any dependencies and displays the following prompt:
   
   Installed size: nn G
   
   Is this ok [y/N]:

Note: The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:

- `#` — root user
- `bash$` — nsp user
Enter y. The following is displayed:
- Downloading packages:
- Running transaction check
- Running transaction test
- Transaction test succeeded
- Running transaction
- Uninstalling the NFM-P package...

As each package removal completes, the following is displayed:
- Complete!

Return to Step 4 as required to remove the next package in the sequence.

When all packages are removed, enter the following to reboot the auxiliary server station:

```
# systemctl reboot
```

The station reboots.

Remove the /opt/nsp/nfmp/auxserver directory and contents.

---

### 13.6 To uninstall an auxiliary database

#### 13.6.1 Description

**CAUTION**

Data Loss

*Performing this procedure permanently erases all auxiliary database data.*

*Before you perform this procedure, ensure that you have a backup of the auxiliary database, if the data is of value.*

The following steps describe how to delete an NFM-P auxiliary database and remove the auxiliary database software from all auxiliary database stations.

**Note:** You require the following user privileges on each auxiliary database station:
- root
- dba user
Note: A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

13.6.2 Steps

1. Log in to an auxiliary database station as the root user.

2. Open a console window.

3. Enter the following:
   
   ```
   # /opt/nsp/nfmp/auxdb/install/bin/auxdbAdmin.sh uninstall
   ```

   The script displays the following message and prompt:
   
   THIS ACTION WILL ERASE YOUR DATABASE
   Please type 'YES' to continue

4. Enter YES. You are prompted for the dba password.

5. Enter the password.
   
   The following messages are displayed as the database is stopped and the database objects are removed from each station:
   
   Stopping auxiliary database ...
   Dropping auxiliary database ...
   Removing data and catalog directories from all nodes

6. Perform the following steps on each auxiliary database station.
   
   1. Log in to the station as the root user.
   2. Open a console window.
   3. Enter the following to remove the auxiliary database packages:
      
      ```
      # yum erase vertica nsp-nfmp-aux-db nsp-nfmp-jre
      ```

      The yum utility resolves any package dependencies and displays the following prompt:
      
      Remove 3 Package(s)
      Installed size: nnn M
      Is this ok [y/N]:

   4. Enter y. The packages are removed.
5. When all packages are removed, enter the following to reboot the station:
   
   ```
   # systemctl reboot
   ```
   
   The station reboots:

6. Remove the /opt/nsp/nfmp/auxdb directory and contents.

---

### 13.7 To uninstall a main server

#### 13.7.1 Description

**CAUTION**

**Service Disruption**

*This procedure requires that you stop the NFM-P main server and database software, which is service-affecting.*

*Perform this procedure only during a scheduled maintenance period.*

The following steps describe how to remove the NFM-P main server software from a station.

**Note:** To avoid a server activity switch in a redundant NFM-P system, you must uninstall the main servers in the following order:

- standby main server
- primary main server

**Note:** You require the following user privileges on the main server station:

- root
- nsp

**Note:** The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:

- # —root user
- bash$ —nsp user

#### 13.7.2 Steps

1. Stop the main server.

   1. Log in to the main server station as the nsp user.
   2. Open a console window.
   3. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin
   ```
4. Enter the following:
   bash$ ./nmsserver.bash stop

5. Enter the following:
   bash$ ./nmsserver.bash appserver_status
   The server status is displayed; the server is fully stopped if the status is the following:
   Application Server is stopped
   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform
   the next step until the server is fully stopped.

2

Enter the following to switch to the root user:
bash$ su -

3

Open a console window.

4

Perform one of the following.

a. If the main server and database are on separate stations in a distributed deployment,
   perform the following steps.
   1. Enter the following:
      # /opt/nsp/Uninstaller/uninstall.sh
      The following prompt is displayed:
      WARNING: This will remove all the nsp software from the system.
      The nsp and oracle users will NOT be removed.
      Do you want to continue? [Yes/No]:
   2. Enter Yes. The software is removed.

b. If the main server and database are collocated on one station, perform the following steps.
   1. Enter the following:
      # yum remove nsp-nfmp-main-server
      # yum remove nsp-nfmp-nspos
      # yum remove nspos-ansible
      # yum remove nspos-postgresql
      # yum remove nspos-jre
      After you enter a command, the yum utility resolves any dependencies and displays the
      following prompt:
      Installed size: nn G
      Is this ok [y/N]:
   2. Enter y. The following is displayed:
13.8 To uninstall a main database

13.8.1 Description

The following steps describe how to remove the NFM-P main database software from a station.

**Note:** You require root user privileges on the main database station.

13.8.2 Steps

1. Log in to the main database station as the root user.

2. Open a console window.

3. Perform one of the following.

   a. If the main database and main server are collocated on one station, enter the following commands in sequence:
Note: The yum utility stops the database before removing the software.

```bash
# yum remove nsp-nfmp-main-db
download
# yum remove nsp-nfmp-oracle
download
```

b. If the main database and main server are on separate stations, enter the following commands in sequence:

Note: The yum utility stops the database before removing the software.

```bash
# yum remove nsp-nfmp-main-db
download
# yum remove nsp-nfmp-oracle
download
# yum remove nsp-nfmp-config
# yum remove nsp-nfmp-jre
```

After you enter a command, the yum utility resolves any package dependencies and displays the following prompt:

```
Installed size: nn G
Is this ok [y/N]:
```

4. Enter y. The following is displayed:

```
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Uninstalling the NFM-P package...
As each package removal completes, the following is displayed:
Complete!
```

5. Return to Step 3 as required to remove the next package in the sequence.

6. When all packages are removed, enter the following to reboot the main database station:

```bash
# systemctl reboot
download
```

The station reboots.

7. Remove the /opt/nsp/nfmp/oracle12r1 directory and the database directories, as required.

END OF STEPS
NFM-P uninstallation
To uninstall a main database
Part III: NFM-P client deployment

Overview

Purpose

This part describes how to deploy an NFM-P single-user GUI client or client delegate server.

Contents

| Chapter 14, Single-user client deployment | 559 |
| Chapter 15, Client delegate server deployment | 581 |
14 Single-user client deployment

14.1 Overview

14.1.1 Purpose

This chapter describes NFM-P single-user GUI client installation, upgrade, and uninstallation.

14.1.2 Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.1 Overview</td>
<td>559</td>
</tr>
<tr>
<td>Introduction</td>
<td>560</td>
</tr>
<tr>
<td>14.2 Single-user GUI client deployment</td>
<td>560</td>
</tr>
<tr>
<td>14.3 To install the Oracle JRE on a RHEL station</td>
<td>561</td>
</tr>
<tr>
<td>Single-user GUI client installation</td>
<td>564</td>
</tr>
<tr>
<td>14.4 To install a single-user GUI client</td>
<td>564</td>
</tr>
<tr>
<td>Single-user GUI client upgrade</td>
<td>569</td>
</tr>
<tr>
<td>14.5 To upgrade an NFM-P Release 17 or 5620 SAM single-user GUI client</td>
<td>569</td>
</tr>
<tr>
<td>14.6 To upgrade an NFM-P Release 18 single-user GUI client</td>
<td>572</td>
</tr>
<tr>
<td>Single-user GUI client uninstallation</td>
<td>578</td>
</tr>
<tr>
<td>14.7 To uninstall a single-user GUI client</td>
<td>578</td>
</tr>
</tbody>
</table>
Introduction

14.2 Single-user GUI client deployment

14.2.1 Description
The procedures in this chapter describe single-user GUI client deployment operations in a standalone or redundant NFM-P system. You must comply with the general requirements in Chapter 2, “Before you begin”, and any specific requirements in this chapter, before you attempt to deploy a single-user GUI client.

14.2.2 Platform requirements
Single-user GUI client deployment is supported on the following platforms:
  • Mac OS X
  • Microsoft Windows
  • RHEL

Note: Single-user client deployment on any platform requires a specific Oracle JRE. See the NSP NFM-P Planning Guide for the minimum required Oracle JRE version.

General
The following are the security requirements for single-user client deployment:
  • Installation, upgrade, and uninstallation require only local user privileges.
  • Only the user that installs the client software, or a user with sufficient privileges, such as root or a local administrator, can start a single-user client.
  • Uninstallation must be performed by the user that installs the client software, or by a user with sufficient privileges, such as root or a local administrator.

Note: Single-user client installation requires a supported web browser on the client station. See the NSP NFM-P Planning Guide for browser support information.

Mac OS X
A Mac OS X client upgrade from NFM-P Release 17 or from the 5620 SAM is not supported. You must uninstall each such client before a system upgrade, as described in the 5620 SAM and NFM-P pre-upgrade procedures, and then install the new client software, as described at the end of the system upgrade procedure.

Microsoft Windows
The following are the supported Microsoft Windows versions for single-user client deployment:
  • Windows Server 2008 R2
  • Windows Server 2012 R2
  • Windows 7, 32- and 64-bit editions
  • Windows 8 Enterprise, 64-bit edition
• Windows 8.1 Enterprise, 64-bit edition
• Windows 10 Pro, 32- and 64-bit editions

RHEL
A RHEL single-user GUI client station must have:
• a supported OS release and patch level, as described in the NSP NFM-P Planning Guide
• the required RHEL OS configuration and packages, as described in Chapter 4, “RHEL OS configuration”
• the required Oracle JRE version; see 14.3 “To install the Oracle JRE on a RHEL station” (p. 561) for information about JRE installation on RHEL

Note: The Bash shell is the supported command shell for RHEL CLI operations.

14.2.3 Single-user GUI client deployment procedures

Table 14-1 Single-user GUI client deployment procedures

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3 “To install the Oracle JRE on a RHEL station” (p. 561)</td>
<td>Install the required Oracle JRE for single-user client or client delegate server deployment on a RHEL station.</td>
</tr>
<tr>
<td>14.4 “To install a single-user GUI client” (p. 564)</td>
<td>Install the single-user GUI client software.</td>
</tr>
<tr>
<td>14.5 “To upgrade an NFM-P Release 17 or 5620 SAM single-user GUI client” (p. 569)</td>
<td>Upgrade the NFM-P Release 17 or 5620 SAM single-user GUI client software.</td>
</tr>
<tr>
<td>14.6 “To upgrade an NFM-P Release 18 single-user GUI client” (p. 572)</td>
<td>Upgrade the NFM-P Release 18 single-user GUI client software.</td>
</tr>
<tr>
<td>14.7 “To uninstall a single-user GUI client” (p. 578)</td>
<td>Remove the single-user GUI client software from a station.</td>
</tr>
</tbody>
</table>

14.3 To install the Oracle JRE on a RHEL station

14.3.1 Description
The following steps describe how to install the required Oracle JRE on a RHEL station for single-user client or client delegate server deployment.

Note: You require root user privileges on the client or client delegate server station.

Note: A leading # symbol in a CLI command represents the RHEL prompt for the root user; do not include the leading # symbol when you type a command.

14.3.2 Steps

1. Log in to the client or client delegate server station.

**Note:** The packages must be in rpm format; download only a file that has an rpm extension. The filename format is the following:

```
jre-version-linux-x64.rpm
```

where `version` is the Java version identifier, for example, `8u40`, which represents version 8, update 40.

Open a console window.

Enter the following to install the JRE package:

```
# /bin/rpm -ivh path/filename
```

where

- `path` is the absolute path to the downloaded file
- `filename` is the name of the downloaded file

Enter the following commands in sequence to install the Java component:

```
# alternatives --install /usr/bin/java java /usr/java/jreR.r.r_nn/bin/java 1
# alternatives --set java /usr/java/jreR.r.r_nn/bin/java
```

where

- `R.r.r` is the Java release identifier, for example, 1.8.0
- `nn` is the JRE update identifier, for example, 40

Enter the following commands in sequence to install the javaws component:

```
# alternatives --install /usr/bin/javaws javaws /usr/java/jreR.r.r_nn/bin/javaws 1
# alternatives --set javaws /usr/java/jreR.r.r_nn/bin/javaws
```

where

- `R.r.r` is the Java release identifier, for example, 1.8.0
- `nn` is the JRE update identifier, for example, 40

Perform one of the following.

a. Enter the following commands in sequence to install the 32-bit Mozilla browser plug-in:
To install the Oracle JRE on a RHEL station

8

Close the console window.

End of steps
Single-user GUI client installation

14.4 To install a single-user GUI client

14.4.1 Description

The following steps describe how to install the single-user GUI client software.

- **Note:** Before you perform the procedure, you must ensure that the correct Oracle JRE version is installed on the client station. See the *NSP NFM-P Planning Guide* for the minimum required Oracle JRE version.

- **Note:** The main server to which the client connects must be running when you perform this procedure.

- **Note:** You require local user privileges on the client station.

14.4.2 Steps

1. Log in to the client station.

2. Verify that you have the required access permissions to create the client installation directory; see your system administrator for information about access permissions.

3. Use a browser on the client station to open the following URL:

   https://server

   where server is the main server IP address or hostname

   - **Note:** An IPv6 address must be enclosed in brackets, for example: [2001:0DB8:3EA6:2B43::11A1]

   The NSP sign-in page is displayed, as shown in Figure 14-1, “NSP sign-in page” (p. 565).
Enter your NSP user credentials and click SIGN IN.

**Note:** The default login credentials are the following:

- Username—admin
- Password—available from technical support

The NSP Launchpad is displayed.

Click on the Network Functions Manager - Packet icon. The form shown in Figure 14-2, "Install NFM-P" (p. 566) is displayed.
6 Click START DOWNLOAD.

7 Your browser may display one or more security prompts about downloading or running a JNLP file.
   Acknowledge each prompt, as required, in order to proceed. If the browser prompts you to choose an application to open the JNLP file with, specify Java Web Start, or javaws. A form like the following is displayed.

Figure 14-3 Do you want to run this application?

![Figure 14-3](image)
Click Run. The form shown in Figure 14-4, “Install NFM-P Version Release” (p. 566) opens.

**Figure 14-4 Install NFM-P Version Release**

Select I accept the terms of the License Agreement, specify the client installation directory, and click Ok.

The client installation begins, and the panel shown in Figure 14-5, “Updating...” (p. 568) is displayed. The panel uses separate bars to indicate the overall and current task progress.
When the installation is complete, the client GUI opens, and an NSP NFM-P Client (server) desktop shortcut is created, where server is the NFM-P main server IP address or hostname.

END OF STEPS
14.5 To upgrade an NFM-P Release 17 or 5620 SAM single-user GUI client

14.5.1 Description
The following steps describe how to upgrade the NFM-P Release 17 or 5620 SAM software on a single-user GUI client station.

Note: A Mac OS X client upgrade from NFM-P Release 17 or from the 5620 SAM is not supported. You must uninstall each such client before a system upgrade, as described in the 5620 SAM and NFM-P pre-upgrade procedures, and then install the new client software, as described at the end of the system upgrade procedure.

Note: The main server to which the client connects must be upgraded and running when you perform this procedure.

Note: If you are not the original installer of the client software, you require the following user privileges on the client station:
• Microsoft Windows—local administrator
• RHEL—root

14.5.2 Steps

1. Log in to the client station.

2. Close the client GUI, if it is open.

3. If you are upgrading from the 5620 SAM, delete the 5620 SAM client desktop shortcut.

4. Use a browser on the client station to open the following URL:
   https://server

   where server is the main server IP address or hostname

   If you are not currently logged in, the NSP sign-in page is displayed, as shown in Figure 14-6, "NSP sign-in page" (p. 570).
Enter the login credentials and click SIGN IN. The NSP Launchpad is displayed.

Click Network Functions Manager - Packet. Your browser may display one or more security prompts about downloading or running a JNLP file. Acknowledge each prompt, as required, in order to proceed. If the browser prompts you to choose an application to open the JNLP file with, specify Java Web Start, or javaws.

When a form like the following is displayed; click Run.

The panel shown in Figure 14-8, “Updating...” (p. 571) is displayed.
Click Update client.

The client upgrade begins, and the panel shown in Figure 14-9, “Updating...” (p. 572) is displayed. The panel uses separate bars to indicate the overall and current task progress.

When the upgrade is complete, the NFM-P client GUI opens.

An “NSP NFM-P Client (server)” desktop shortcut is created, where server is the NFM-P main server IP address or hostname.
14.6 To upgrade an NFM-P Release 18 single-user GUI client

14.6.1 Description

The following steps describe how to upgrade the NFM-P Release 18 software on a single-user GUI client station.

To upgrade an NFM-P Release 17 or 5620 SAM client, see 14.5 “To upgrade an NFM-P Release 17 or 5620 SAM single-user GUI client” (p. 569).

**Note:** The main server to which the client connects must be upgraded and running when you perform this procedure.

**Note:** If you are not the original installer of the client software, you require the following user privileges on the client station:

- Mac OS X, Microsoft Windows—local administrator
- RHEL—root
14.6.2 Steps

1. Log in to the client station.

2. Close the client GUI, if it is open.

3. Double-click on the NSP NFMP Client desktop icon. A form like the following is displayed.

   Figure 14-10 Do you want to run this application?

   ![Application Run Confirmation]

   Do you want to run this application?
   Publisher: Nokia Solutions and Networks US LLC
   Locations: https://123.456.789.0

   The application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the location and publisher above.

   Do not open the app from the publisher and location above

   More Information Run Cancel

4. Click Run.

   The panel shown in Figure 14-11, "Updating..." (p. 574) is displayed.
Click Update client.

The client delegate server upgrade begins, and the panel shown in Figure 14-12, "Updating..." (p. 575) is displayed. The panel uses separate bars to indicate the overall and current task progress.
If you are not currently logged in, the splash screen shown in Figure 14-13, “Waiting for user authentication” (p. 576) opens, and the NSP sign-in page is displayed, as shown in Figure 14-14, “NSP sign-in page” (p. 577).

Enter the required login credentials on the NSP sign-in page and click SIGN IN. The NSP Launchpad is displayed, and the client GUI opens.
Figure 14-13  Waiting for user authentication

NSP  Network Functions Manager - Packet

NFM-P Model 13.3 MAIN Service Pack 8035

Server:

NFM-P:138:120.200.164

Waiting for user authentication.
Verify that the GUI is operational and correctly displayed.

END OF STEPS
14.7 To uninstall a single-user GUI client

14.7.1 Description

The following steps describe how to remove the single-user GUI client software from a station.

Note: The main server to which the client connects must be running when you perform this procedure.

Note: If you are not the original installer of the client software, you require the following user privileges on the client station:
- Mac OS X, Microsoft Windows—local administrator
- RHEL—root

14.7.2 Steps

1. Log in to the client station.

2. Close the client GUI, if it is open.

3. Use a browser on the client station to open one of the following URLs:
   - http://server:8085/client, if TLS for client access is disabled
   - https://server:8444/client, if TLS for client access is enabled
   where server is the main server IP address or hostname

Note: An IPv6 address must be enclosed in brackets, for example: [2001:0DB8:3EA6:2B43::11A1]

The page shown in Figure 14-15, “NSP Network Functions Manager - Packet client” (p. 579) opens..
Click Uninstall NFM-P client. Your browser may display one or more security prompts about downloading or running a JNLP file. Acknowledge each prompt, as required, in order to proceed. If the browser prompts you to choose an application to open the JNLP file with, specify Java Web Start, or javaws. A form like the following is displayed.

Click Run. The client uninstaller opens.

Click Yes to begin the uninstallation.

When the uninstallation is complete, click OK to close the uninstaller.
8 Remove any files that remain in the client installation directory.

9 If a client desktop shortcut is present, delete the shortcut.

END OF STEPS
15 Client delegate server deployment

15.1 Overview

15.1.1 Purpose
This chapter describes NFM-P client delegate server installation, upgrade, and uninstallation.

15.1.2 Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1 Overview</td>
<td>581</td>
</tr>
<tr>
<td>Introduction</td>
<td>582</td>
</tr>
<tr>
<td>15.2 Client delegate server deployment</td>
<td>582</td>
</tr>
<tr>
<td>Client delegate server installation</td>
<td>584</td>
</tr>
<tr>
<td>15.3 To install a client delegate server</td>
<td>584</td>
</tr>
<tr>
<td>15.4 To add a client delegate server to an existing system</td>
<td>592</td>
</tr>
<tr>
<td>Client delegate server upgrade</td>
<td>596</td>
</tr>
<tr>
<td>15.5 To upgrade an NFM-P Release 17 or 5620 SAM client delegate server</td>
<td>596</td>
</tr>
<tr>
<td>15.6 To upgrade an NFM-P Release 18 client delegate server</td>
<td>600</td>
</tr>
<tr>
<td>Client delegate server uninstallation</td>
<td>606</td>
</tr>
<tr>
<td>15.7 To uninstall a client delegate server</td>
<td>606</td>
</tr>
</tbody>
</table>
15.2 Client delegate server deployment

15.2.1 Description

This chapter describes client delegate server deployment in a standalone or redundant NFM-P system. You must comply with the general requirements in Chapter 2, “Before you begin” and the specific requirements in this chapter before you attempt to deploy a client delegate server.

**Note:** A client delegate server upgrade from a 5620 SAM release is not supported. You must uninstall the existing client delegate server software, and then install the new software, as described in 15.5 “To upgrade an NFM-P Release 17 or 5620 SAM client delegate server” (p. 596).

15.2.2 Platform requirements

Client delegate server deployment is supported on the following platform types:

- RHEL
- Microsoft Windows

**General**

If the NFM-P system uses a firewall, you must ensure that the firewall allows traffic to pass between the remote client stations and the client delegate servers. See the NSP NFM-P Planning Guide for a list of the ports that must be open on each component.

**Note:** Client delegate server deployment on any platform requires a specific Oracle JRE. See the NSP NFM-P Planning Guide for information about the required Oracle JRE version.

**Note:** Adding a client delegate server to an existing NFM-P system requires root and nsp user privileges on each main server station.

**Microsoft Windows**

The following are the supported Microsoft Windows versions for client delegate server deployment:

- Windows Server 2008 R2
- Windows Server 2012 R2

**Note:** Client delegate server deployment on Windows requires local Administrator user privileges.

**RHEL**

A RHEL client delegate server station must have:

- a supported OS release and patch level, as described in the NSP NFM-P Planning Guide
- the required RHEL OS configuration and packages, as described in Chapter 4, “RHEL OS configuration”
• the required Oracle JRE version; see 14.3 “To install the Oracle JRE on a RHEL station” (p. 561) for JRE installation information on RHEL

Note: A remote station that connects to a RHEL client delegate server requires X.11 or native X display redirection; X-window emulation software is not supported.

Note: Client delegate server deployment on RHEL requires root user privileges.

Note: The Bash shell is the supported command shell for RHEL CLI operations.

15.2.3 Client delegate server deployment procedures

Table 15-1  Client delegate server deployment procedures

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.3 “To install a client delegate server” (p. 584)</td>
<td>Install the client delegate server software on a RHEL or Microsoft Windows station.</td>
</tr>
<tr>
<td>15.4 “To add a client delegate server to an existing system” (p. 592)</td>
<td>Add a new client delegate server to an existing NFM-P system.</td>
</tr>
<tr>
<td>15.5 “To upgrade an NFM-P Release 17 or 5620 SAM client delegate server” (p. 596)</td>
<td>Upgrade the client delegate server software on a RHEL or Microsoft Windows station.</td>
</tr>
<tr>
<td>15.6 “To upgrade an NFM-P Release 18 client delegate server” (p. 600)</td>
<td>Upgrade the client delegate server software on a RHEL or Microsoft Windows station.</td>
</tr>
<tr>
<td>15.5 “To upgrade an NFM-P Release 17 or 5620 SAM client delegate server” (p. 596)</td>
<td>Upgrade the client delegate server software on a RHEL or Microsoft Windows station.</td>
</tr>
<tr>
<td>15.7 “To uninstall a client delegate server” (p. 606)</td>
<td>Remove the client delegate server software from a RHEL or Microsoft Windows station.</td>
</tr>
</tbody>
</table>
Client delegate server installation

15.3 To install a client delegate server

15.3.1 Description

The following steps describe how to install the client delegate server software on a RHEL or Microsoft Windows station.

**Note:** Before you perform the procedure, the client delegate server address and installation directory must be configured on each main server during installation or upgrade, or as described in 15.4 “To add a client delegate server to an existing system” (p. 592).

**Note:** The main server to which the client delegate server connects must be running and operational when you perform the procedure.

**Note:** You require the following user privileges on the client delegate server station:

- RHEL—root
- Windows—local Administrator user

15.3.2 Steps

1. Perform 15.4 “To add a client delegate server to an existing system” (p. 592) to add the client delegate server information to each main server configuration.

2. Log in to the client delegate server station.

3. Verify that you have the required access permissions to create the client delegate server installation directory; see your system administrator for information about access permissions.

4. Use a browser on the client delegate server station to open one of the following URLs:
   - http://server:8085/clientdelegate, if TLS for client access is disabled
   - https://server:8444/clientdelegate, if TLS for client access is enabled
   where server is the main server IP address or hostname

**Note:** An IPv6 address must be enclosed in brackets, for example:

[2001:0DB8:3EA6:2B43::11A1]

The page shown in Figure 15-1, “NSP Network Functions Manager - Packet client delegate” (p. 585) opens.
Click Install or Launch NSP Network Functions Manager - Packet client delegate. Your browser may display one or more security prompts about downloading or running a JNLP file. Acknowledge each prompt, as required, in order to proceed. If the browser prompts you to choose an application to open the JNLP file with, specify Java Web Start, or javaws. A form like the following is displayed.

Click Run. The window shown in Figure 15-3, “Install NFM-P Version Release” (p. 586) opens.
Select I accept the terms of the License Agreement and click Ok.

The client delegate server installation begins, and the panel shown in Figure 15-4, “Updating...” (p. 587) is displayed. The panel uses separate bars to indicate the overall and current task progress.
When the installation is complete, the window shown in Figure 15-5, "Network Functions Manager - Packet client" (p. 588) opens, and an "NSP NFM-P Client (server)" desktop shortcut is created, where server is the NFM-P main server IP address or hostname.
Click Open launchpad. A web browser opens and displays the NSP sign-in page, as shown in Figure 15-6, "NSP sign-in page" (p. 589).
9

Enter the login credentials and click SIGN IN.

**Note:** The default login credentials are the following:

- Username—admin
- Password—available from technical support

The NSP Launchpad is displayed.

10

Click Network Functions Manager – Packet. Your browser may display one or more security prompts about downloading or running a JNLP file.

Acknowledge each prompt, as required, in order to proceed. If the browser prompts you to choose an application to open the JNLP file with, specify Java Web Start, or javaws.

A form like the following is displayed.

*Figure 15-6* NSP sign-in page

*Figure 15-7* Do you want to run this application?
11  Click Run. The local client GUI opens.

12  Verify that the GUI is correctly displayed and operational.

13  Close the client GUI.

**Configure remote client access on RHEL client delegate server**

14  A client delegate server installation on RHEL creates a RHEL user group named nsp. A user that opens a remote client session must belong to the nsp user group.

Add each user that requires client access to the nsp user group on the client delegate server station.

15  As required, preserve the GUI preferences of each RHEL single-user client user that is migrating to the client delegate server.

1. Log in to the single-user client station as the user that installed the client, or as a user that has read access to the client files and directories.

2. Copy all files in the `RHEL_home\nsp\guiPreference` directory to the same directory on the client delegate server station, where `RHEL_home` is the RHEL user home directory.

16  As required, preserve the GUI preferences of each Windows single-user client user that is migrating to the client delegate server.

1. Log in to the single-user client station as the user that installed the client, or as a user that has read access to the client files and directories.

2. Copy all files in the `Win_home\nsp\guiPreference` directory to the following directory on the client delegate server station:

   ```
   RHEL_home\nsp\guiPreference
   ```

   where

   - `Win_home` is the Windows user home directory, which is defined in the USERPROFILE environment variable
   - `RHEL_home` is the RHEL user home directory
Perform the following steps on each RHEL station that is to open a client GUI session through
the client delegate server.
1. Open a remote login session on the client delegate server.
2. Configure display redirection from the client delegate server station to the current station.
3. Open a client GUI session on the station to verify that the client connects successfully:

Configure remote client access on Windows client delegate server

As required, preserve the GUI preferences of each Windows single-user client user that is
migrating to the client delegate server.
1. Log in to the single-user client station as the user that installed the client, or as a user that
has read access to the client files and directories.
2. Copy all files in the Win_home/.nsp/guiPreference directory to the same directory on the
client delegate server station, where Win_home is the Windows user home directory, which
is defined in the USERPROFILE environment variable.

As required, preserve the GUI preferences of each RHEL single-user client user that is
migrating to the client delegate server.
1. Log in to the single-user client station as the user that installed the client, or as a user that
has read access to the client files and directories.
2. Copy all files in the RHEL_home/.nsp/guiPreference directory to the following directory on
the client delegate server station:
   Win_home/.nsp/guiPreference
   where
   RHEL_home is the RHEL user home directory
   Win_home is the Windows user home directory, which is defined in the USERPROFILE
   environment variable

If the client delegate server is installed on Windows, perform the following steps on each
Windows station that is to open a client GUI session through the client delegate server.
1. Open a Windows remote desktop session on the client delegate server station.
2. Use a browser in the remote desktop session to open the appropriate URL:
   • http://server:8085/clientdelegate, if TLS for client access is disabled
   • https://server:8444/clientdelegate, if TLS for client access is enabled
   where server is the main server IP address or hostname
3. Click Install or Launch NSP Network Functions Manager - Packet client delegate. Your
   browser may display one or more security prompts about downloading or running a JNLP
   file.
4. Acknowledge each security prompt, as required. If the browser prompts you to choose an application to open the JNLP file with, specify Java Web Start, or javaws.

5. The client GUI opens, and a desktop shortcut is created for opening subsequent GUI sessions.

Verify remote client operation

Open the client GUI from a remote station to verify the client delegate server connectivity and operation.

END OF STEPS

15.4 To add a client delegate server to an existing system

15.4.1 Description

CAUTION

Service Disruption

This procedure requires a restart of each main server in the NFM-P system, which is service-affecting.

Perform this procedure only during a scheduled maintenance period.

The following steps describe how to add a new client delegate server to an existing NFM-P system.

Note: You require the following user privileges on each main server station:

- root
- nsp

Note: CLI commands use the following to represent the CLI prompt:

- #—the prompt for the root user
- bash$—the prompt for the nsp user

Do not type the leading # symbol or bash$ when you enter a command.

15.4.2 Steps

1. If the system is deployed in a standalone configuration, go to Step 7.

2. Perform Step 7 to Step 19 on the standby main server.
Perform Step 7 to Step 19 on the primary main server.

Perform Step 20 on the primary main server station.

When the primary main server is fully operational, perform Step 20 on the standby main server station.

Go to Step 21.

Log in to the main server station as the root user.

Open a console window.

Stop the main server.
1. Enter the following to switch to the nsp user:
   # su - nsp
2. Enter the following:
   bash$ cd /opt/nsp/nfmp/server/nms/bin
3. Enter the following:
   bash$ ./nmsserver.bash stop
4. Enter the following:
   bash$ ./nmsserver.bash appserver_status
   The server status is displayed; the server is fully stopped if the status is the following:
   Application Server is stopped
   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

Enter the following to switch back to the root user:
   bash$ exit

Enter the following:
Client delegate server deployment
Client delegate server installation
To add a client delegate server to an existing system

# samconfig -m main
The following is displayed:
Start processing command line inputs...
<main>

12 Enter the following:
<main> configure client
The prompt changes to <main configure client>.

13 Enter the following:
<main configure client> show
The client configuration of the main server is displayed. The delegates parameter lists the current client delegate servers.

14 Enter the following:
<main configure client> delegates current_list,new_address;path
where
current_list is the comma-separated list of client delegate servers in the current main server configuration
new_address is the IP address or hostname of the new client delegate server
path is the absolute file path of the client installation location on the client delegate server station

15 Enter the following:
<main configure client> back
The prompt changes to <main configure>.

16 Enter the following:
<main configure> show-detail
The main server configuration is displayed.

17 If the configuration is correct, enter the following:
<main configure> back
The prompt changes to <main>.
Enter the following:
<main> apply ↵
The configuration is applied.

Enter the following:
<main> exit ↵
The samconfig utility closes.

Start the main server.
1. Enter the following to switch to the nsp user:
   # su - nsp ↵
2. Enter the following:
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↵
3. Enter the following:
   bash$ ./nmsserver.bash start ↵
4. Enter the following:
   bash$ ./nmsserver.bash appserver_status ↵
The server status is displayed; the server is fully initialized if the status is the following:
   Application Server process is running. See nms_status for more detail.
   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

Close the open console windows.

END OF STEPS
15.5 To upgrade an NFM-P Release 17 or 5620 SAM client delegate server

15.5.1 Description

The following steps describe how to upgrade the NFM-P Release 17 or 5620 SAM client delegate server software on a RHEL or Microsoft Windows station.

**Note:** The main server to which the client delegate server connects must be upgraded and running when you perform this procedure.

**Note:** You require the following user privileges on the client delegate server station:

- RHEL—root
- Windows—local Administrator user

15.5.2 Steps

1. Close each remote client GUI session that the client delegate server hosts.

2. Log in to the client delegate server station.

3. Close the local client GUI, if it is open.

4. If you are upgrading from the 5620 SAM, delete the 5620 SAM client desktop shortcut.

5. If you are upgrading a Release 17.3 or later client delegate server, go to Step 7.

6. Perform one of the following.
   
a. If the client delegate server is installed on RHEL, perform the following steps.
      
      1. Uninstall the client delegate server software.
         
         **Note:** You must use the uninstallation procedure in the installation and upgrade guide for the existing client delegate server release, and not the uninstallation procedure in this guide.

   2. Back up the following directory for each remote client user on the station to a secure location on a separate station:
RHEL_home/.nsp/guiPreference
where RHEL_home is the RHEL user home directory

3. Commission a new station, or recommission the existing client delegate server station, according to the platform specifications in this guide and in the NSP NFM-P Planning Guide.

4. Perform 15.3 “To install a client delegate server” (p. 584) on the newly commissioned client delegate server station.

5. Create the required RHEL user accounts for remote client access.

6. Restore the backup files from substep 2 for each remote client user.

7. Go to Step 12.

b. If the client delegate server is installed on Windows, and the initial client delegate server installation was performed using a web browser, go to Step 7.

c. If the client delegate server is installed on Windows, and the initial client delegate server installation was performed using the GUI-based installer, perform the following steps.

1. Uninstall the client delegate server software.

   Note: You must use the uninstallation procedure in the installation and upgrade guide for the existing client delegate server release, and not the uninstallation procedure in this guide.

2. Perform 15.3 “To install a client delegate server” (p. 584) on the newly commissioned client delegate server station.

3. Go to Step 12.

7

Use a browser on the client delegate server station to open the following URL:

https://server

where server is the main server IP address or hostname

Note: An IPv6 address must be enclosed in brackets, for example:
[2001:0DB8:3EA6:2B43::11A1]

The NSP sign-in page is displayed, as shown in Figure 15-8, "NSP sign-in page" (p. 598).
Enter the login credentials and click SIGN IN. The NSP Launchpad is displayed.

Click Network Functions Manager - Packet. Your browser may display one or more security prompts about downloading or running a JNLP file. Acknowledge each prompt, as required, in order to proceed. If the browser prompts you to choose an application to open the JNLP file with, specify Java Web Start, or javaws. A form like the following is displayed.

Click Run.
The panel shown in Figure 15-10, “Updating...” (p. 598) is displayed.

Click Update client.

The client delegate server upgrade begins, and the panel shown in Figure 15-11, “Updating...” (p. 600) is displayed. The panel uses separate bars to indicate the overall and current task progress.

When the upgrade is complete, the local NFM-P client GUI opens.

An “NSP NFM-P Client (server)” desktop shortcut is created, where server is the NFM-P main server IP address or hostname.
Verify that the GUI is operational and correctly displayed.

**END OF STEPS**

15.6 To upgrade an NFM-P Release 18 client delegate server

15.6.1 Description

The following steps describe how to upgrade the NFM-P Release 18 client delegate server software on a RHEL or Microsoft Windows station.

**Note:** The main server to which the client delegate server connects must be upgraded and running when you perform this procedure.

**Note:** You require the following user privileges on the client delegate server station:

- RHEL—root
- Windows—local Administrator user
15.6.2 Steps

1. Close each remote client GUI session that the client delegate server hosts.

2. Log in to the client delegate server station.

3. Close the local client GUI, if it is open.

4. Double-click on the NSP NFM-P Client desktop icon.
   A form like the following is displayed.

   **Figure 15-12**  Do you want to run this application?

   ![Do you want to run this application? form](image)

   Do not show this alert for apps from the publisher and location above

5. Click Run.
   The panel shown in **Figure 15-13, “Updating...”** (p. 602) is displayed.
Click Update client.

The client delegate server upgrade begins, and the panel shown in Figure 15-14, “Updating...” (p. 603) is displayed. The panel uses separate bars to indicate the overall and current task progress.
If you are not currently logged in, the splash screen shown in Figure 15-15, “Waiting for user authentication” (p. 604) opens, and the NSP sign-in page is displayed, as shown in Figure 15-16, “NSP sign-in page” (p. 605).

Enter the required login credentials on the NSP sign-in page and click SIGN IN. The NSP Launchpad is displayed, and the client GUI opens.
Figure 15-15  Waiting for user authentication

**NSP** Network Functions Manager - Packet

NFM-P Release 13.3 MAIN Service Pack 8035

Server:

```
NFM-P:138:120.200.164
```

Waiting for user authentication.

© 2018 Nokia.
Verify that the GUI is operational and correctly displayed.

END OF STEPS
Client delegate server uninstallation

15.7 To uninstall a client delegate server

15.7.1 Description

The following steps describe how to remove the client delegate server software.

**Note:** The main server to which the client delegate server connects must be running when you perform this procedure.

**Note:** If you are not the original installer of the client software, you require the following user privileges on the client station:

- RHEL—root
- Windows—local Administrator user

15.7.2 Steps

1. Log into the client delegate server station.

2. Close the local client GUI, if it is open.

3. Use a browser on the client delegate server station to open one of the following URLs:
   - http://server:8085/clientdelegate, if TLS for client access is disabled
   - https://server:8444/clientdelegate, if TLS for client access is enabled

   where server is the main server IP address or hostname

   **Note:** An IPv6 address must be enclosed in brackets, for example:
   
   [2001:0DB8:3EA6:2B43::11A1]

   The page shown in Figure 15-17, “NSP Network Functions Manager - Packet client delegate” (p. 607) opens.
Click Uninstall NSP Network Functions Manager - Packet client delegate. Your browser may display one or more security prompts about downloading or running a JNLP file. Acknowledge each prompt, as required, in order to proceed. If the browser prompts you to choose an application to open the JNLP file with, specify Java Web Start, or javaws. A form like the following is displayed.

The client uninstaller opens. Click Yes to begin the uninstallation.

When the uninstallation is complete, click OK to close the uninstaller.
Remove any files that remain in the client delegate server installation directory.

8

If a client desktop shortcut is present, delete the shortcut.

9

If the client delegate server is installed on Windows, the uninstallation does not remove the desktop shortcuts of remote users; the shortcuts must be manually removed.

To remove the desktop shortcut for a remote user, perform the following steps.

1. Open a Windows remote desktop session as the remote user on the client delegate server station.

2. In the remote desktop session, open Windows Control Panel.

3. Open the Java applet in Control Panel. The General tab is displayed.


5. Select Applications from the Show drop-down list. A list of Java applications is displayed.

6. Right-click on the NSP Network Functions Manager - Packet entry and click Delete. The entry is removed, and the client shortcut is removed from the Windows desktop of the user.

END OF STEPS