NSP
Network Services Platform

Release 23.11

Installation and Upgrade Guide

3HE-18969-AAAC-TQZZA
Issue 4
May 2024

Legal notice

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

This document includes Nokia proprietary and confidential information, which may not be distributed or disclosed to any third parties without the prior written consent of Nokia.

This document is intended for use by Nokia's customers ("You"/"Your") in connection with a product purchased or licensed from any company within Nokia Group of Companies. Use this document as agreed. You agree to notify Nokia of any errors you may find in this document; however, should you elect to use this document for any purpose(s) for which it is not intended, You understand and warrant that any determinations You may make or actions You may take will be based upon Your independent judgment and analysis of the content of this document.

Nokia reserves the right to make changes to this document without notice. At all times, the controlling version is the one available on Nokia's site.

No part of this document may be modified.

NO WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF AVAILABILITY, ACCURACY, RELIABILITY, TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, IS MADE IN RELATION TO THE CONTENT OF THIS DOCUMENT. IN NO EVENT WILL NOKIA BE LIABLE FOR ANY DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL OR ANY LOSSES, SUCH AS BUT NOT LIMITED TO LOSS OF PROFIT, REVENUE, BUSINESS INTERRUPTION, BUSINESS OPPORTUNITY OR DATA THAT MAY ARISE FROM THE USE OF THIS DOCUMENT OR THE INFORMATION IN IT, EVEN IN THE CASE OF ERRORS IN OR OMISSIONS FROM THIS DOCUMENT OR ITS CONTENT.

Contents

Auxiliary database upgrade from Release 22.9 or later

About this document

Purpose

The *NSP Installation and Upgrade Guide* is intended for a technology officer, network planner, or system administrator who intends to perform a Network Services Platform deployment function.

Scope

WARNING

System Failure

Attempting to use any information or procedure in this guide on a system that is not deployed as described in this guide, for example, an NSP appliance or NSP Server deployment, may result a catastrophic system failure.

You must use the information and procedures in the NSP Installation and Upgrade Guide only on a system deployed as described in the NSP Installation and Upgrade Guide.

The scope of this document is limited to NSP system and component deployment within the constraints and requirements described in the *NSP Planning Guide*.

The *NSP Installation and Upgrade Guide* includes information about platform commissioning, and has workflows and procedures for deployment functions such as the following:

- installation
- upgrade
- integration with other systems
- platform conversion

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:

- Documentation Center
- Technical support

How to comment

Please send your feedback to Documentation Feedback.

Part I: Getting started

Overview

Purpose

This part of the *NSP Installation and Upgrade Guide* provides an introduction with workflows for supported deployment scenarios, and also describes how to commission the host platform of an NSP component.

Contents

1 Before you begin

NSP deployment overview

1.1 Where do I start?

1.1.1 The planning phase

Before you consider deploying a new NSP system, upgrading or adding to a system, or modifying a system in any way, the reader is strongly encouraged to become familiar with the following guides:

- *NSP System Architecture Guide*, for the product description, NSP deployment options, and NSP access information
- *NSP Planning Guide*, for pre-deployment requirements, system specifications, restrictions, and special considerations
- *NSP Release Notice*, for release-specific information that may apply to your deployment, and technical updates not captured in other NSP guides

After you identify your deployment requirements under consultation with a Nokia representative, the response to an NSP Platform Sizing Request that you submit to Nokia provides the required parameters for your deployment operation.

1.1.2 Using this guide

After the planning phase, you must become familiar with the relevant content in this and the subsequent Part I: “Getting started” chapters, which describe NSP platform preparation.

When the platform configuration is established, your planned deployment action can proceed using the required procedures in Part II: “NSP system deployment”, for system-level NSP deployment operations, and Part III: “NSP component deployment”, for operations specific to NSP components that are deployed outside an NSP cluster.

1.2 NSP deployment terms and concepts

1.2.1 Introduction

The NSP deployment and administration guides use specific terms to describe some basic elements of an NSP system. The following topics define commonly used terms used in the NSP system documentation that may be unfamiliar to the reader.

Note: Although the usage of each term is typically as described, a specific context may include a variant of the term.

1.2.2 Station

A station is a physical processing entity that has one native OS instance, or hosts OS instances in multiple VMs. The term station is typically used only for low-level configuration operations to distinguish the VM from the entity on which the VM is deployed.

The term “host station” is sometimes used to clearly indicate the physical station that hosts a specific function.

1.2.3 NSP deployer host

The NSP deployer host is a VM from which you deploy the container environment for an NSP cluster.

1.2.4 NSP cluster

An NSP cluster is a group of one or more VMs in a Kubernetes container environment that host NSP software and functions. An NSP system deployment includes at least one NSP cluster.

1.2.5 NSP cluster member

An NSP cluster member is a VM in an NSP cluster. An NSP cluster member is also called a cluster node, depending on the context.

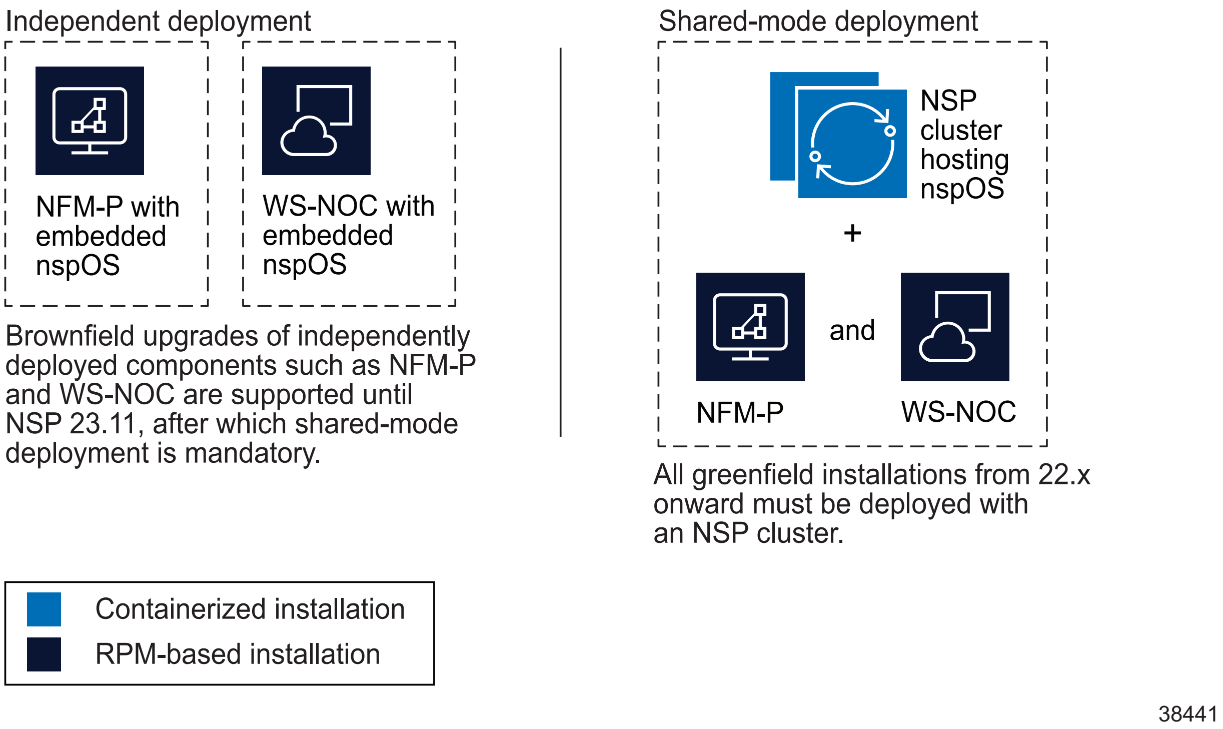
1.2.6 NSP cluster host

The NSP cluster host is a specific NSP cluster member from which NSP deployment operations in the cluster are performed. Typically, node 1 of a cluster is chosen as the NSP cluster host.

1.2.7 Independent and shared-mode deployments

A shared-mode deployment is an NSP deployment in which the WS-NOC or NFM-P components share a central set of NSP platform resources in the NSP cluster, instead of using the nspOS embedded in the NFM component. If you add an independently deployed system to an NSP deployment, the independent system stops using the embedded local nspOS, and instead uses the shared nspOS hosted by the NSP.

The following graphic depicts the two types of deployments currently supported:


Independent deployment
NFM-P with embedded nspOS
WS-NOC with embedded nspOS
Brownfield upgrades of independently deployed components such as NFM-P and WS-NOC are supported until NSP 23.11, after which shared-mode deployment is mandatory.
Shared-mode deployment
NSP cluster hosting nspOS
+
NFM-P
and
WS-NOC
All greenfield installations from 22.x onward must be deployed with an NSP cluster.
Containerized installation
RPM-based installation
38441

Deployment scenarios

1.3 NSP fault tolerance and disaster recovery

1.3.1 HA and DR deployments

NSP system components support high-availability, or HA, deployment, which uses redundant warm-standby components for local fault tolerance. In addition, each of the following scenarios supports disaster-recovery, or DR, deployment of identical NSP systems at geographically distant sites.

See “System redundancy and fault tolerance” in the *NSP System Architecture Guide* for more information about the supported redundancy models, and for system failure and recovery scenarios.

1.4 Workflow to deploy classic IP management

1.4.1 Description

The following is the sequence of high-level actions required to deploy classic IP management.

Note: Before you attempt to deploy an NSP component, you must review and comply with the deployment requirements and restrictions in the *NSP Planning Guide*.

1.4.2 Stages

1

Install an NSP cluster. Perform 7.4 “To install the NSP” (p. 193).

2

Classic IP management requires the NFM-P; see“NFM-P installation” (p. 431) for standalone or redundant NFM-P installation information.

1.5 Workflow to deploy resource control

1.5.1 Description

The following is the sequence of high-level actions required to deploy resource control.

Note: Before you attempt to deploy an NSP component, you must review and comply with the deployment requirements and restrictions in the *NSP Planning Guide*.

1.5.2 Stages

1

Install an NSP cluster. Perform 7.4 “To install the NSP” (p. 193).

Note: This deployment type requires the Control and Visualization Starter licensed package.

2

If you are deploying the IPRC, install the VSR-NRC; see 14.6 “VSR-NRC installation overview” (p. 426) for information.

1.6 Workflow to deploy the Simulation tool

1.6.1 Description

The following is the sequence of high-level actions required to deploy the Simulation tool.

Note: Before you attempt to deploy an NSP component, you must review and comply with the deployment requirements and restrictions in the *NSP Planning Guide*.

1.6.2 Stages

1

Perform procedure 7.4 “To install the NSP” (p. 193) to install an NSP cluster.

During the configuration phase of the installation, you must specify the following in addition to the other parameters that you configure; see 6.1 “NSP configuration file” (p. 173) for information about configuring NSP deployment parameters:

- Set the deployment type, as shown below

```
nsp:
  deployment:
    type: deployment_type
```

  where *deployment_type* is one of the following:
  - live deployment—ip-mpls-sim
  - lab or trial deployment—lab

- Enable the Simulation installation option and disable NSP Platform - Logging and Monitoring.

```
    installationOptions:
     - name: “NSP Platform - Base Services”
       id: platform-baseServices
#      - name: "NSP Platform - Logging and Monitoring"
#        id: platform-loggingMonitoring
     - name: “Simulation”
       id: simulation
```

- Set the opensearch option in the logging section of the file to false, as shown below:

  Note: The opensearch option is set to true by default, so must be deliberately set to false.

```
logging:
      forwarding:
        applicationLogs:
          opensearch:
            enabled: false
```

1.7 Workflow to deploy classic IP and model-driven management

1.7.1 Description

The following is the sequence of high-level actions required to deploy classic IP and model-driven management.

Note: Before you attempt to deploy an NSP component, you must review and comply with the deployment requirements and restrictions in the *NSP Planning Guide*.

Note: Some components of an NSP system can be at different releases; see the *NSP Release Notice* for component release compatibility information.

Note: User group properties are component-specific. When a user of a specific NSP component requires authorization to access an additional component, the user group must be re-created in the new component in order for them to access the functions associated with the new component. Instructions for creating a user group are in the component documentation.

1.7.2 Stages

1

Install an NSP cluster. Perform 7.4 “To install the NSP” (p. 193).

NOTE: For a deployment of this type, the Service Activation and Configuration licensed package is required.

2

Install the NFM-P, as described in “NFM-P installation” (p. 431); configure the NFM-P to use the PKI server for TLS.

3

If you are adding an existing NFM-P system to the NSP cluster, add the servers to the NFM-P system; perform 11.3 “To integrate the NSP and NFM-P” (p. 327).

4

Perform 11.7 “To install the NSP templates for NSP service management on the NFM-P” (p. 344) to install the NSP templates on the NFM-P.

5

Install the VSR-NRC; see 14.6 “VSR-NRC installation overview” (p. 426).

6

In a deployment of this type, the NSP uses the VSR-NRC to obtain IGP topology data by default. To configure the NSP to receive IGP topology from the CPAA instead, perform 13.21 “To change the IGP topology data source” (p. 397).

1.8 Workflow to deploy model-driven management only

1.8.1 Description

The following is the sequence of high-level actions required to deploy NSP model-driven management.

Note: Before you attempt to deploy an NSP component, you must review and comply with the deployment requirements and restrictions in the *NSP Planning Guide*.

Note: User group properties are component-specific. When a user of a specific NSP component requires authorization to access an additional component, the user group must be re-created in the new component in order for them to access the functions associated with the new component. Instructions for creating a user group are in the component documentation.

1.8.2 Stages

1

Install an NSP cluster. Perform 7.4 “To install the NSP” (p. 193).

NOTE: For a deployment of this type, the Service Activation and Configuration licensed package is required.

2

Install the VSR-NRC. See 14.6 “VSR-NRC installation overview” (p. 426) for information.

1.9 Workflow to upgrade small scale optical and classic IP management

1.9.1 Description

The following is the sequence of high-level actions required to upgrade small-scale optical and classic IP management.

Note: Before you attempt to deploy an NSP component, you must review and comply with the deployment requirements and restrictions in the *NSP Planning Guide*.

Note: Some components of an NSP system can be at different releases; see the *NSP Release Notice* for component release compatibility information.

Note: The NFM-P must be upgraded before the WS-NOC is upgraded.

1.9.2 Stages

1

Upgrade the NFM-P, as described in “NFM-P system upgrade from Release 22.6 or earlier” (p. 628).

2

Upgrade the WS-NOC, as described in the *WS-NOC HW and OS Installation Guide* and the *WS-NOC Installation Guide*.

1.10 Workflow to deploy optical and classic IP management

1.10.1 Description

The following is the sequence of high-level actions required to deploy optical and classic IP management.

ℹ **Note:** Before you attempt to deploy an NSP component, you must review and comply with the deployment requirements and restrictions in the *NSP Planning Guide*.

ℹ **Note:** Some components of an NSP system can be at different releases; see the *NSP Release Notice* for component release compatibility information.

ℹ **Note:** User group properties are component-specific. When a user of a specific NSP component requires authorization to access an additional component, the user group must be re-created in the new component in order for them to access the functions associated with the new component. Instructions for creating a user group are in the component documentation.

1.10.2 Stages

1

Install an NSP cluster. Perform 7.4 “To install the NSP” (p. 193).

NOTE: For a deployment of this type, both the Service Activation and Configuration and the Multi-Layer Discovery and Visualization licensed packages are required.

2

Install the NFM-P, as described in “NFM-P installation” (p. 431); configure the NFM-P to use the PKI server for TLS.

3

If you are adding an existing NFM-P system to the NSP cluster, add the servers to the NFM-P system; perform 11.3 “To integrate the NSP and NFM-P” (p. 327).

4

Perform 11.7 “To install the NSP templates for NSP service management on the NFM-P” (p. 344) to install the NSP templates on the NFM-P.

5

Install the WS-NOC, as described in the *WS-NOC HW and OS Installation Guide* and the *WS-NOC Installation Guide*.

6

If you are adding the NSP cluster to an existing WS-NOC system, add the servers to the WS-NOC system; perform 11.8 “To integrate a containerized Release 21.12, 22.6, 22.12, 23.6, or 23.12 WS-NOC and the NSP” (p. 345).

Note: The WS-NOC information must also be added to the NSP configuration.

7

Perform 11.6 “To map external user groups to predefined WS-NOC roles” (p. 342).

8

Install the VSR-NRC. See 14.6 “VSR-NRC installation overview” (p. 426) for more information.

9

In a deployment of this type, the NSP uses the VSR-NRC to obtain IGP topology data by default. To configure the NSP to receive IGP topology from the CPAA instead, perform 13.21 “To change the IGP topology data source” (p. 397).

10

Install third-party optical controllers using the NSP cluster; see the *NSP IP/Optical Coordination Guide* or the Network Developer Portal for more information.

1.11 Workflow to deploy large-scale optical and classic IP management

1.11.1 Description

The following is the sequence of high-level actions required to deploy large-scale optical and classic IP management.

Note: Before you attempt to deploy an NSP component, you must review and comply with the deployment requirements and restrictions in the *NSP Planning Guide*.

Note: Some components of an NSP system can be at different releases; see the *NSP Release Notice* for component release compatibility information.

Note: User group properties are component-specific. When a user of a specific NSP component requires authorization to access an additional component, the user group must be re-created in the new component in order for them to access the functions associated with the new component. Instructions for creating a user group are in the component documentation.

1.11.2 Stages

1

Install an NSP cluster. Perform 7.4 “To install the NSP” (p. 193).

2

Install the NFM-P, as described in “NFM-P installation” (p. 431); configure the NFM-P to use the PKI server for TLS.

3

If you are adding an existing NFM-P system to the NSP cluster, add the servers to the NFM-P system; perform 11.3 “To integrate the NSP and NFM-P” (p. 327).

4

Install the WS-NOC, as described in the *WS-NOC HW and OS Installation Guide* and the *WS-NOC Installation Guide*.

5

If you are adding an NSP cluster to an existing WS-NOC system, perform 11.8 “To integrate a containerized Release 21.12, 22.6, 22.12, 23.6, or 23.12 WS-NOC and the NSP” (p. 345).

Note: The WS-NOC information must also be added to the NSP configuration file.

6

Perform 11.6 “To map external user groups to predefined WS-NOC roles” (p. 342).

2 NSP disk setup and partitioning

2.1 Overview

2.1.1 Purpose

This chapter describes the NSP disk commissioning options, and lists the partitioning requirements for NSP components in trial and live network environments.

2.1.2 Contents

NSP disk deployment

2.2 Introduction

2.2.1 Disk commissioning methods

A physical or virtual station that hosts NSP software requires a specific disk partitioning scheme. You can create the required disk partitions on the station:

- during the deployment of an NSP RHEL OS disk image, as described in 2.2.2 “NSP disk-image deployment” (p. 28)
- after a manual RHEL OS installation, using one of the component-specific partitioning schemes in the following:
    - “Disk partitioning for trial deployments” (p. 41)
    - “Disk partitioning for live deployments” (p. 50)

Note: Deploying an NSP disk image is the recommended method.

Note: Before you deploy any NSP software in a VMware VM, you must install the latest VMware Tools software.

Note: The disk capacity required for the /opt/nsp/nfmp/nebackup partition depends on the number and types of devices in your managed network; see 2.2.3 “Sizing the NFM-P NE backup partition” (p. 29) for information.

Supported file systems

For OS-deployed disk partitions such as /, /home, /tmp, /opt, and /var, the NSP supports ext4 or XFS, with the following exception:

- The /var/log and /var/log/audit partitions require XFS.

For NSP application partitions such as /opt/nsp and child partitions, ext4 is required, with the following exceptions:

- /opt/nsp/nfmp/auxdb/backup on an NSP auxiliary database, which can be mounted as ext3, ext4, or NFS
- /extra, which can be mounted as ext4 or XFS

Additional disk configuration

Regardless of the disk deployment method, each partition created after the OS installation requires the additional configuration described in 2.6 “To configure and mount an NSP disk partition” (p. 39).

2.2.2 NSP disk-image deployment

Disk images for deploying an NSP RHEL OS instance are available in the following formats:

- qcow2
- OVA

The following images are available in each format:

- NSP deployer host / NSP cluster VM image
- image for components deployed outside NSP cluster

ℹ **Note:** NSP RHEL image deployment is authorized only for NSP or CLM software installation, and not for the installation of any other Nokia or third-party product.

An NSP RHEL disk image:

- contains only the RHEL OS
- has all required and optional OS packages to support NSP software deployment
- does not include any product-specific packages or application files
- has SELinux enabled in permissive mode

NSP qcow2 image deployment

For NSP qcow2 image deployment, see 2.3 “To deploy an NSP RHEL qcow2 disk image” (p. 30).

NSP OVA image deployment

Deploying the NSP on VMWare has the following requirements.

- You must ensure that each non-LVM partition is mounted using the partition UUID, rather than the block device name; see 2.4 “To configure disk partitions using device UUIDs” (p. 36) for information.
- If you use cloud-init to set the IP address of an NSP VM on VMWare, you must perform 2.5 “To apply the VMware cloud-init workaround” (p. 38) before you attempt to install any NSP software on the VM.

For general NSP OVA image deployment information, see the documentation for your virtualization environment.

ℹ **Note:** For an NSP deployer host or NSP cluster VM deployed using the OVA image, it is strongly recommended that you mount the /opt directory on a separate hard disk that has sufficient capacity to allow for future expansion.

2.2.3 Sizing the NFM-P NE backup partition

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
- average configuration backup size
- number of backups retained per NE

ℹ **Note:** Uninstalling a main server does not delete or otherwise affect the saved NE configuration backup files.

The partition size is the amount of space required for the backup files of all managed NE types. You must calculate the space required for each NE type using the following formula, and then use the sum of the NE space requirements as the partition size:

data capacity = backup size × number of NEs × backups per NE × 2.5

Table 2-1, “Configuration backup file sizes by NE type” (p. 30) lists the backup size values.

Note: The formula is a guideline for planning purposes only; the actual size may require adjustment. It is recommended that you use the size of the largest backup per NE type in your network as the backup size, and multiply the result by 2.5, as shown in the formula. This calculation accounts for network and NE backup growth, and accommodates the storage of compressed archive files.

Table 2-1 Configuration backup file sizes by NE type

NE type	Backup size
1830 VWM OSU	128 kbytes
7210 SAS	200 kbytes
7450 ESS, 7750 SR, 7950 XRS	1.5 Mbytes
7705 SAR	250 kbytes
OmniSwitch	30 kbytes
Wavence	1.5 Mbytes

2.3 To deploy an NSP RHEL qcow2 disk image

2.3.1 Purpose

Perform this procedure to deploy a qcow2 disk image on a station that is to host NSP software.

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

2.3.2 Steps

Check host station OS compatibility

1

Check the *NSP Release Notice* to ensure that the OS version of the host station supports the creation of VMs at the RHEL version that the NSP requires.

2

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

3

If the host station OS version supports NSP VM creation, enter the following; otherwise, update the host OS version as required:

```
# osinfo-query os | grep rhel | grep -v - ↵
```

A list of supported RHEL variants is listed, for example:

```
rhel7.8 | Red Hat Enterprise Linux 7.8 | 7.8 | http://redhat.
com/rhel/7.8

rhel7.9 | Red Hat Enterprise Linux 7.9 | 7.9 | http://redhat.
com/rhel/7.9

rhel8.0 | Red Hat Enterprise Linux 8.0 | 8.0 | http://redhat.
com/rhel/8.0

rhel8.1 | Red Hat Enterprise Linux 8.1 | 8.1 | http://redhat.
com/rhel/8.1

rhel8.2 | Red Hat Enterprise Linux 8.2 | 8.2 | http://redhat.
com/rhel/8.2
```

4

Record the appropriate RHEL version number in the left column, which is one of the following:

- the version that matches the NSP-supported RHEL version, if listed
- the version that is less than but closest to the supported NSP RHEL version; in the output example, the version to record is 8.2, as the NSP supports a higher RHEL version that is not listed

Prepare required images

5

Log in to the host station as the root user.

6

Download one of the following files from the NSP downloads page on the Nokia Support portal to a local directory on the station:

- NSP_K8S_PLATFORM_RHEL8_*yy_mm*.qcow2—for NSP deployer host or NSP cluster VM
- NSP_RHEL8_*yy_mm*.qcow2—for component outside NSP cluster, such as NFM-P server / database, NSP Flow Collector / Flow Collector Controller, NSP analytics server

where *yy_mm* represents the year and month of issue

7

Open a console window.

8

Enter the following:

```
# dnf -y install virt-install libguestfs-tools ↵
```

9

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, NSP_Server_A

10

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 the response to your Platform Sizing Request.

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

   ```
   # qemu-img resize -f raw "raw_image.img" sizeG ↵
   ```

   where

   raw_image is the raw disk image name specified in Step 9

   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 NSP component 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 the response to your Platform Sizing Request.

   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, NSP_Server_A_Complete, for an image that is to contain all NSP component server partitions, or NSP_Server_A_Software, for an image that is to contain only the /opt/nsp partition

   size is the required disk size, in Gbytes

11

The raw image files that you create in Step 10 are in sparse format; you must convert the image to non-sparse format, which provides optimal disk performance.

Perform the following steps for each raw disk image created in Step 10.

1. Enter the following:

   ```
   # cp --sparse=never raw_image.img non-sparse_image.img ↵
   ```

   raw_image is the name of a raw disk image created in Step 10

   non-sparse_image is the name to assign to the non-sparse image

   A *non-sparse_image*.img file is created.

2. Delete the *raw_image*.img file, which is no longer required.

Deploy VMs

12

Enter the following once for each VM to deploy the VM:

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

```
# virt-install --connect qemu:///system --ram RAM --vcpu=vCPUs -n
instance --os-type=linux --os-variant=variant --disk path="image_
name", device=disk,bus=virtio,format=raw,io=native,cache=none
--network bridge=bridge_name --import & ↵
```

where

RAM is the required amount of VM RAM in the response to your Platform Sizing Request, in Mbytes; for example, 64 Gbytes is expressed as 65536, which is 64 x 1024 Mbytes

vCPUs is the required number of vCPU threads in the response to your Platform Sizing Request

instance is the name to assign to the VM

variant is the OS version recorded in Step 4, for example, 8.2

image_name is the name of the raw or non-sparse disk image created for the VM

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

13

Enter the following to open a console session on the VM:

```
# virsh console VM ↵
```

where VM is the VM name

You are prompted for credentials.

14

Enter the following credentials:

- username—root
- password—*available from technical support*

A virtual serial console session opens on the VM.

15

Configure the RHEL OS as required for the NSP component; for example:

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

Note: If an NFM-P system integrated with the NSP uses hostnames, the NSP cluster VMs must be able to resolve each NFM-P hostname using DNS.

16

Perform one of the following; see "Disk partitioning for trial deployments" (p. 41) or "Disk partitioning for live deployments" (p. 50) for component-specific partitioning schemes.

> **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

   For each directory, enter the following and then respond to the prompts; use the directory size value from the response to your Platform Sizing Request:

   ```
   # 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 17.

   b. If you are not using LVM, perform the following steps.

   1. Enter the following for each sub-disk:

      ```
      # mkfs fs_type -L path /dev/devicen ↵
      ```

      where

      fs_type is the file system type; see "Supported file systems" (p. 28) for partition-specific file system support

      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; see “Supported file systems” (p. 28) for partition-specific file system support

4. Save and close the file.

5. Enter the following:

```
# mount -a ↵
```

6. Go to Step 19.

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

```
# 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

17

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/nsp/nfmp/nebackup partition before you mount the /opt/nsp partition.

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

1. Enter the following to create a logical volume:

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

   where

   volume is the name to assign to the logical volume

   size is the required volume size in the response to your Platform Sizing Request

   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:

   ```
   # mkdir directory ↵
   ```

   where *directory* is the name of the directory to associate with the volume, for example, /opt/nsp

3. Enter the following:

```
# mkfs fs_type -L directory /dev/group/volume ↵
```

where

fs_type is the file system type; see “Supported file systems” (p. 28) for partition-specific file system support

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; see “Supported file systems” (p. 28) for partition-specific file system support
6. Save and close the file.
7. Enter the following:

   ```
   # mount -a ↵
   ```

Perform optional security hardening

18

Optionally, for greater system security, you can remove the world permissions from RHEL compiler executable files, as described in A.1 “Resetting GCC-compiler file permissions” (p. 1093).

19

Close the open console windows.

END OF STEPS

2.4 To configure disk partitions using device UUIDs

2.4.1 Purpose

If you deploy an NSP VM in a VMware environment, you must mount each non-LVM partition using the block-device UUID, and not the block-device name.

Perform this procedure to change the block-device identifier for each non-LVM partition from the device name to the device UUID.

2.4.2 Steps

1

Log in as the root user on the station that hosts the partition.

2

Open a console window.

3

Enter the following:

```
# grep /dev/sd /etc/fstab ↵
```

The devices and associated partitions are listed; a line like the following is displayed for each partition:

```
/dev/device  path    fs_type    noatime    1 2
```

where

device is the block-device name

path is the mount point, for example, /opt

fs_type is the file system type, for example, ext4 or xfs

4

Perform the following steps for each listed partition:

1. Enter the following

   ```
   # blkid | grep /dev/device ↵
   ```

   One or more lines like the following are displayed, depending on the number of partitions on the device:

   ```
   /dev/device: UUID="device_UUID" BLOCK_SIZE="4096" TYPE="fs_type"
   PARTUUID="partition_UUID"
   ```

2. Record the *device_UUID* value.

5

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

6

Use the recorded *device_UUID* values to modify the fstab entries.

The fstab entry example in Step 3 changes from:

```
/dev/device  path    fs_type    noatime    1 2
```

to:

```
UUID=device_UUID  path    fs_type    noatime    1 2
```

7

Close the /etc/fstab file.

8

Close the console window.

END OF STEPS

2.5 To apply the VMware cloud-init workaround

2.5.1 Purpose

The following VMware knowledge-base article describes how the cloud-init configuration fails to persist through a reboot, and instead defaults to DHCP.

https://kb.vmware.com/s/article/71264

If you deploy an NSP VM in a VMware environment, you must apply a VMware workaround described in the article before you attempt to install any NSP software on the VM.

Perform this procedure to apply the workaround from VMware.

2.5.2 Steps

1

Log in as the root user on the station that hosts the partition.

2

Open a console window.

3

Open the following file using a text editor such as vi:

/etc/cloud/cloud.cfg

4

Add the following line:

manual_cache_clean: True

5

Save and close the file.

6

Close the console window.

END OF STEPS

2.6 To configure and mount an NSP disk partition

2.6.1 Purpose

Perform this procedure on each NSP disk partition on a station that you create after the RHEL OS installation. The procedure is valid for a station that hosts any NSP component type.

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

2.6.2 Steps

1

Log in as the root user on the station that hosts the partition.

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   fs_type  barrier=0,noatime    1 2
```

b. For a partition in an OpenStack VM, add the following entry:

```
/dev/device   mount_point   fs_type  noatime    1 2
```

c. For a non-LVM partition in a VMWare VM, add the following entry:

```
UUID=UUID   mount_point   fs_type  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

fs_type is the file system type, for example, ext4 or xfs

UUID is the block-device UUID; see 2.4 “To configure disk partitions using device UUIDs” (p. 36) for information about obtaining a blick-device UUID

7

Optionally, in accordance with ANSSI and CIS specifications, configure the following partitions using the following mount options:

ℹ **Note:** Configuring the mount options is strongly recommended.

ℹ **Note:** If you choose to configure the options, you must do so before any NSP software is installed on the station.

ℹ **Note:** The /var partition options are only partially ANSSI-compliant; see the *NSP Security Hardening Guide* for CIS recommendations and the NSP support for each.

```
/boot xfs nodev,noexec,nosuid 0 0
/home xfs nodev,noexec,nosuid 0 0
/tmp xfs nodev,noexec,nosuid 0 0
/var xfs nodev,nosuid 0 0
```

8

Optionally, to meet the CIS noexec requirement for the /var/tmp directory, add the following line to bind the directory to the /tmp partition; see the *NSP Security Hardening Guide* for information:

```
/tmp /var/tmp none bind 0 0
```

9

Save and close the /etc/fstab file.

10

Enter the following to reboot the station:

```
# systemctl reboot ↵
```

The station reboots.

END OF STEPS

Disk partitioning for trial deployments

2.7 Trial partitioning requirements, NSP deployer host and cluster VMs

2.7.1 Trial NSP deployer host partitioning scheme

CAUTION

Service Disruption

Each disk partition described in this section must be a mounted partition, and not a symbolic link. The use of symbolic links to represent partitions is not supported.

Do not use a symbolic link to represent an NSP partition under any circumstances.

Note: See the *NSP Planning Guide* for information about the supported disk types.

The following table lists the disk partitions required for the NSP deployer host in a trial NSP deployment.

Table 2-2 Trial partitioning scheme, NSP deployer host

Partition	Content	Size (Gbytes)
/	Root	26
/boot	Boot partition	0.5
/home	User home directories	0.5
/tmp	Temporary files	4
/opt	NSP registry, operating data, and software for Kubernetes installer and NSP deployer	275
/var	System data	64
/var/log	System logs	6
/var/log/audit	System audit logs	6

2.7.2 Trial NSP cluster VM partitioning scheme

CAUTION

Service Disruption

Each disk partition described in this section must be a mounted partition, and not a symbolic link. The use of symbolic links to represent partitions is not supported.

Do not use a symbolic link to represent an NSP partition under any circumstances.

An NSP cluster is deployed as one or more VMs that each use local storage. To facilitate NSP software deployment, each VM has the same partition layout.

The following table lists the disk partitions required for the trial deployment of an NSP cluster VM.

Table 2-3 Trial partitioning scheme, NSP cluster VM

Partition	Content	Size (Gbytes)
/	Root	30
/home	User home directories	0.5
/tmp	Temporary files	6
/var	System data	64
/var/log	System logs	6
/var/log/audit	System audit logs	6
/opt	NSP software, operating data, backups	200

2.8 Trial partitioning requirements, additional NSP components

2.8.1 Trial NSP Flow Collector Controller partitioning scheme

CAUTION

Service Disruption

Each disk partition described in this section must be a mounted partition, and not a symbolic link. The use of symbolic links to represent partitions is not supported.

Do not use a symbolic link to represent an NSP partition under any circumstances.

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

Table 2-4 Trial partitioning scheme, NSP Flow Collector Controller

Disks required: one 300 Gbyte or larger		
Partition	Content	Size (Gbytes)
swap	Swap space	16
/	Root	26
/home	User home directories	0.5
/tmp	Temporary files	4
/var	System data	64
/var/log	System logs	6
/var/log/audit	System audit logs	6

Table 2-4 Trial partitioning scheme, NSP Flow Collector Controller (continued)

Disks required: one 300 Gbyte or larger		
Partition	Content	Size (Gbytes)
/opt/nsp	NSP Flow Collector Controller software, operating data	10
/opt/nsp/flow/fcc/data/extraction	Extracted NFM-P network data model	20
/extra	NSP software storage	50

2.8.2 Trial NSP Flow Collector partitioning scheme

CAUTION

Service Disruption

Each disk partition described in this section must be a mounted partition, and not a symbolic link. The use of symbolic links to represent partitions is not supported.

Do not use a symbolic link to represent an NSP partition under any circumstances.

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

Table 2-5 Trial partitioning scheme, NSP Flow Collector

Disks required: one 300 Gbyte or larger		
Partition	Content	Size (Gbytes)
swap	Swap space	16
/	Root	26
/home	User home directories	0.5
/tmp	Temporary files	4
/var	System data	64
/var/log	System logs	6
/var/log/audit	System audit logs	6
/opt/nsp	NSP Flow Collector software, operating data	20
/opt/nsp/flow/fc/data/results	Collected statistics data files	57
/extra	NSP software storage	50

2.8.3 Trial collocated NSP Flow Collector Controller / Flow Collector partitioning scheme

CAUTION

Service Disruption

Each disk partition described in this section must be a mounted partition, and not a symbolic link. The use of symbolic links to represent partitions is not supported.

Do not use a symbolic link to represent an NSP partition under any circumstances.

The following table lists the disk partitions required for the trial deployment of an NSP Flow Collector Controller and Flow Collector that are collocated on one station.

Table 2-6 Trial partitioning scheme, collocated NSP Flow Collector Controller / Flow Collector

Disks required: one 300 Gbyte or larger		
Partition	Content	Size (Gbytes)
swap	Swap space	16
/	Root	26
/home	User home directories	0.5
/tmp	Temporary files	4
/var	System data	64
/var/log	System logs	6
/var/log/audit	System audit logs	6
/opt/nsp	NSP Flow Collector software, operating data	30
/opt/nsp/flow/fcc/data/extraction	Extracted NFM-P network data model	20
/opt/nsp/flow/fc/data/results	Collected statistics data files	57
/extra	NSP software storage	50

2.8.4 Trial NSP analytics server partitioning scheme

CAUTION

Service Disruption

Each disk partition described in this section must be a mounted partition, and not a symbolic link. The use of symbolic links to represent partitions is not supported.

Do not use a symbolic link to represent an NSP partition under any circumstances.

The following table lists the disk partitions required for the trial deployment of an NSP analytics server.

Table 2-7 Trial partitioning scheme, NSP analytics server

Disks required: one 300 Gbyte		
Partition	Content	Size (Gbytes)
swap	Swap space	16
/	Root	26
/home	User home directories	0.5
/tmp	Temporary files	4
/var	System data	64
/var/log	System logs	6
/var/log/audit	System audit logs	6
/opt/nsp	NSP analytics server software, operating data	75
/extra	NSP software storage	50

2.9 Trial partitioning requirements, NFM-P components

2.9.1 Trial collocated main server and database partitioning scheme

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

Table 2-8 Trial partitioning scheme, collocated main server and database

Disks required: • Physical deployment—two 300 Gbyte (RAID 0) • qcow deployment— minimum of 480 Gbytes, plus calculated /opt/nsp/nfmp/nebackup partition size		
Partition	Content	Size (Gbytes)
swap	Swap space	16
/	Root	26
/home	User home directories	0.5
/tmp	Temporary files	4
/var	System data	64
/var/log	System data	6
/var/log/audit	System data	6
/opt/nsp	NSP and NFM-P software, operating data	75
/opt/nsp/nfmp/dbbackup	Database backups	35
/opt/nsp/nfmp/nebackup	NE configuration backups	Network-specific [1]
/opt/nsp/nfmp/db	Database tablespaces	90

Table 2-8 Trial partitioning scheme, collocated main server and database (continued)

Disks required: • Physical deployment—two 300 Gbyte (RAID 0) • qcow deployment— minimum of 480 Gbytes, plus calculated /opt/nsp/nfmp/nebackup partition size		
Partition	Content	Size (Gbytes)
/opt/nsp/nfmp/db/archivelog	Database archive logs	35
/opt/nsp/nfmp/server/nms/log	NFM-P server logs	15
/opt/nsp/nfmp/server/xml_output	Output of XML API file export operations	10
/opt/nsp/os	NSP system files	40
/extra	NSP and NFM-P software storage	50

Notes:

1. Derived using the formula in 2.2.3 “Sizing the NFM-P NE backup partition” (p. 29)

2.9.2 Trial distributed main server partitioning scheme

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

Table 2-9 Trial partitioning scheme, main server, distributed system

Disks required: one 300 Gbyte, two 300 Gbyte, or one 600 Gbyte			
Partition	Content	Size (Gbytes)	
		One 300 Gbyte disk	Two 300 Gbyte or one 600 Gbyte disk
swap	Swap space	16	
/	Root	26	
/home	User home directories	0.5	
/tmp	Temporary files	4	
/var	System data	14 [1]	64
/var/log	System logs	6	
/var/log/audit	System audit logs	6	
/opt/nsp	Main server software, operating data	70	
/opt/nsp/nfmp/nebackup	NE configuration backups	Network-specific [2]	
/opt/nsp/nfmp/server/nms/log	NFM-P server logs	15	
/opt/nsp/nfmp/server/xml_output	Output of XML API file export operations	10	
/opt/nsp/os	NSP system files	40	

Table 2-9 Trial partitioning scheme, main server, distributed system (continued)

Disks required: one 300 Gbyte, two 300 Gbyte, or one 600 Gbyte			
Partition	Content	Size (Gbytes)	
		One 300 Gbyte disk	Two 300 Gbyte or one 600 Gbyte disk
/extra	NSP and NFM-P software storage	50	

Notes:

1. Insufficient capacity for application core files
2. Derived using the formula in 2.2.3 “Sizing the NFM-P NE backup partition” (p. 29)

2.9.3 Trial distributed main database partitioning scheme

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

Table 2-10 Trial partitioning scheme, main database, distributed system

Disks required: two 300 Gbyte (RAID 0)		
Partition	Content	Size (Gbytes)
swap	Swap space	16
/	Root	26
/home	User home directories	0.5
/tmp	Temporary files	4
/var	System data	64
/var/log	System logs	6
/var/log/audit	System audit logs	6
/opt/nsp/nfmp	Main database software	40
/opt/nsp/nfmp/dbbackup	Database backups	40
/opt/nsp/nfmp/db	Database tablespaces	100
/opt/nsp/nfmp/db/archivelog	Database archive logs	40
/opt/nsp/nfmp/db/redolog	Database redo logs	8
/extra	NSP and NFM-P software storage	50

2.9.4 Trial auxiliary server partitioning scheme

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

Table 2-11 Trial partitioning scheme, auxiliary server

Disks required: one 300 Gbyte, two 300 Gbyte, or one 600 Gbyte		Size (Gbytes)	
Partition	Content	One 300 Gbyte disk	Two 300 Gbyte or one 600 Gbyte disk
swap	Swap space	16	
/	Root	26	
/home	User home directories	0.5	
/tmp	Temporary files	4	
/var	System data	64	
/var/log	System logs	6	
/var/log/audit	System audit logs	6	
/opt/nsp	NFM-P server software, operating data	40	90
/opt/nsp/nfmp/auxserver/nms/log	NFM-P server logs	20	30
/opt/nsp/nfmp/auxserver/xml_output	Output of XML API file export operations	20	30
/extra	NSP and NFM-P software storage	50	

2.9.5 Trial auxiliary database partitioning scheme

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

For a multi-station auxiliary database, or a single-station database that has a high data rate, the /opt/nsp/nfmp/auxdb/backup partition has the following special requirements:

- It is strongly recommended that the partition is a remote mount point or directly attached storage connected by a minimum 10 Gbyte/s link.
- Each auxiliary database station requires a separate backup volume that is mounted as /opt/nsp/nfmp/auxdb/backup on the auxiliary database station.

  For example, if the specified auxiliary database backup location is /opt/nsp/nfmp/auxdb/backup, the auxiliary database stations require the following mount points:

  − station 1:

  `remote_host:station_1_backup_volume_path/opt/nsp/nfmp/auxdb/backup`

  − station 2:

  `remote_host:station_2_backup_volume_path/opt/nsp/nfmp/auxdb/backup`

  − station 3:

  `remote_host:station_3_backup_volume_path/opt/nsp/nfmp/auxdb/backup`
- The supported file systems for the backup location are ext3, ext4, and NFS.

Note: The /opt/nsp/nfmp/auxdb/backup partition can be a local mount point in a single-station database that has a low to moderate data rate.

Table 2-12 Trial partitioning scheme, auxiliary database

Disks required: two 300 Gbyte (RAID 0)		
Partition	Content	Size (Gbytes)
swap	Swap space	16
/	Root	26
/home	User home directories	0.5
/opt	NFM-P auxiliary database software	49
/tmp	Temporary files	4
/var	System data	64
/var/log	System logs	6
/var/log/audit	System audit logs	6
/opt/nsp/nfmp/auxdb/data	Auxiliary database data	335
/extra	NSP and NFM-P software storage	50
Required additional storage		
/opt/nsp/nfmp/auxdb/backup	Auxiliary database backup data	Equal to /opt/nsp/nfmp/auxdb/data

2.9.6 Trial single-user client or client delegate server partitioning scheme

The following table lists the partitions required for the trial deployment of a single-user client or client delegate server on RHEL.

Table 2-13 Trial partitioning scheme, single-user client or client delegate server

Disks required: one 300 Gbyte or larger		
Partition	Content	Size (Gbytes)
—	Swap space	16
/	Root, including /usr and /var	26
/opt/nsp	NFM-P client software	16
At operator discretion	Customer data; can be partitioned according to customer requirements	Remainder

Disk partitioning for live deployments

2.10 Live partitioning requirements, NSP deployer host and cluster VMs

2.10.1 Live NSP deployer host partitioning scheme

CAUTION

Service Disruption

Each disk partition described in this section must be a mounted partition, and not a symbolic link. The use of symbolic links to represent partitions is not supported.

Do not use a symbolic link to represent an NSP partition under any circumstances.

Note: See the *NSP Planning Guide* for information about the supported disk types.

The following table lists the disk partitions required for NSP deployer host VM deployment in a live network environment.

Table 2-14 Live partitioning scheme, NSP deployer host

Partition	Content	Size (Gbytes)
/	Root	26
/boot	Boot partition	0.5
/home	User home directories	0.5
/tmp	Temporary files	4
/opt	NSP registry, operating data, and software for Kubernetes installer and NSP deployer	275
/var	System data	64
/var/log	System logs	6
/var/log/audit	System audit logs	6

2.10.2 Live NSP cluster VM partitioning scheme

An NSP cluster is deployed as one or more VMs that each use local storage. To facilitate NSP software deployment, each VM has the same partition layout.

The following table lists the disk partitions required for the deployment of an NSP cluster VM in a live network environment.

Table 2-15 Live partitioning scheme, NSP cluster VM

Partition	Content	Size (Gbytes), by deployment profile	
		Basic / Standard	Enhanced
/	Root	26	
/home	User home directories	0.5	
/tmp	Temporary files	6	
/var	System data	64	
/var/log	System logs	6	
/var/log/audit	System audit logs	6	
/opt	NSP software, operating data, backups	600	800

2.11 Live partitioning requirements, additional NSP components

2.11.1 Live NSP Flow Collector Controller partitioning scheme

CAUTION

Service Disruption

Each disk partition described in this section must be a mounted partition, and not a symbolic link. The use of symbolic links to represent partitions is not supported.

Do not use a symbolic link to represent an NSP partition under any circumstances.

The following table lists the disk partitions required for the deployment of an NSP Flow Collector Controller in a live network environment.

Table 2-16 Live partitioning scheme, NSP Flow Collector Controller

Disks required: two 300 Gbyte (RAID 0)		
Partition	Content	Size (Gbytes)
swap	Swap space	16
/	Root	26
/home	User home directories	0.5
/tmp	Temporary files	4
/var	System data	64
/var/log	System logs	6
/var/log/audit	System audit logs	6
/opt/nsp	NSP Flow Collector Controller software, operating data	20
/opt/nsp/flow/fcc/data/extraction	Extracted NFM-P network data model	50

Table 2-16 Live partitioning scheme, NSP Flow Collector Controller (continued)

Disks required: two 300 Gbyte (RAID 0)		
Partition	Content	Size (Gbytes)
/extra	NSP software storage	50

2.11.2 Live NSP Flow Collector partitioning scheme

CAUTION

Service Disruption

Each disk partition described in this section must be a mounted partition, and not a symbolic link. The use of symbolic links to represent partitions is not supported.

Do not use a symbolic link to represent an NSP partition under any circumstances.

The following table lists the disk partitions required for the deployment of an NSP Flow Collector in a live network environment.

Table 2-17 Live partitioning scheme, NSP Flow Collector

Disks required: two 300 Gbyte (RAID 0)		
Partition	Content	Size (Gbytes)
swap	Swap space	16
/	Root	26
/home	User home directories	0.5
/tmp	Temporary files	4
/var	System data	64
/var/log	System logs	6
/var/log/audit	System audit logs	6
/opt/nsp	NSP Flow Collector software, operating data	50
/opt/nsp/flow/fc/data/results	Collected statistics data files	200
/extra	NSP software storage	50

2.11.3 Live collocated NSP Flow Collector Controller / Flow Collector partitioning scheme

CAUTION

Service Disruption

Each disk partition described in this section must be a mounted partition, and not a symbolic link. The use of symbolic links to represent partitions is not supported.

Do not use a symbolic link to represent an NSP partition under any circumstances.

The following table lists the disk partitions required for the deployment of an NSP Flow Collector Controller and Flow Collector that are collocated on one station in a live network environment.

Table 2-18 Live partitioning scheme, collocated NSP Flow Collector Controller and Flow Collector

Disks required: two 300 Gbyte		
Partition	Content	Size (Gbytes)
swap	Swap space	16
/	Root	26
/home	User home directories	0.5
/tmp	Temporary files	4
/var	System data	64
/var/log	System logs	6
/var/log/audit	System audit logs	6
/opt/nsp	NSP Flow Collector software, operating data	70
/opt/nsp/flow/fcc/data/extraction	Extracted NFM-P network data model	50
/opt/nsp/flow/fc/data/results	Collected statistics data files	200
/extra	NSP software storage	50

2.11.4 Live NSP analytics server partitioning scheme

CAUTION

Service Disruption

Each disk partition described in this section must be a mounted partition, and not a symbolic link. The use of symbolic links to represent partitions is not supported.

Do not use a symbolic link to represent an NSP partition under any circumstances.

The following table lists the disk partitions required for the deployment of an NSP analytics server in a live network environment.

Table 2-19 Live partitioning scheme, NSP analytics server

Disks required: one 300 Gbyte (RAID 0)		
Partition	Content	Size (Gbytes)
swap	Swap space	16
/	Root	26
/home	User home directories	0.5
/tmp	Temporary files	4
/var	System data	64
/var/log	System logs	6
/var/log/audit	System audit logs	6
/opt/nsp	NSP analytics server software, operating data	100
/extra	NSP software storage	50

2.12 Live partitioning requirements, NFM-P components

2.12.1 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 for a deployment in a live network environment.

Note: See the *NSP Planning Guide* and 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/oracle19.

2.12.2 Live collocated main server and database partitioning scheme

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

Table 2-20 Live partitioning scheme, collocated main server and database

Disks required: • Physical deployment—four 300 Gbyte (RAID 0) or eight 300 Gbyte (RAID 1+0) • qcow deployment—minimum of 558 Gbytes, plus calculated /opt/nsp/nfmp/nebackup partition size		Size (Gbytes)	
Partition	Content	Physical	qcow
swap	Swap space	16	
/	Root	26	
/home	User home directories	0.5	
/tmp	Temporary files	4	
/var	System data	64	
/var/log	System data	6	
/var/log/audit	System data	6	
/opt/nsp	NSP and NFM-P software, operating data	150	80
/opt/nsp/nfmp/db	Main database software, tablespaces	300	200
/opt/nsp/nfmp/db/archivelog	Database archive logs	120	70
/opt/nsp/nfmp/dbbackup	Main database backup sets	120	70
/opt/nsp/nfmp/nebackup	NE configuration backup files	Network-specific [1]	
/opt/nsp/nfmp/server/nms/log	NFM-P server logs	50	35
/opt/nsp/nfmp/server/xml_output	Output of XML API file export operations	20	10
/opt/nsp/os	NSP system files	90	
/extra	NSP and NFM-P software storage	50	

Notes:

1. Derived using the formula in 2.2.3 “Sizing the NFM-P NE backup partition” (p. 29)

2.12.3 Live distributed main server partitioning scheme

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

Table 2-21 Live partitioning scheme, main server, distributed system

Disks required: two 300 Gbyte (RAID 0), or four 300 Gbyte (RAID 0)			
Partition	Content	Size (Gbytes)	
		Two 300 Gbyte disks	Four 300 Gbyte disks
swap	Swap space	16	
/	Root	26	

Table 2-21 Live partitioning scheme, main server, distributed system (continued)

Disks required: two 300 Gbyte (RAID 0), or four 300 Gbyte (RAID 0)			
Partition	Content	Size (Gbytes)	
		Two 300 Gbyte disks	Four 300 Gbyte disks
/home	User home directories	0.5	
/tmp	Temporary files	4	
/var	System data	64	
/var/log	System logs	6	
/var/log/audit	System audit logs	6	
/opt/nsp	Main server software, operating data	150	
/opt/nsp/nfmp/nebackup	NE configuration backups	Network-specific [1]	
/opt/nsp/nfmp/server/nms/log	NFM-P server logs	50	
/opt/nsp/nfmp/server/xml_output	Output of XML API file export operations	20	
/opt/nsp/os	NSP system files	90	140
/extra	NSP and NFM-P software storage	50	

Notes:

1. Derived using the formula in 2.2.3 “Sizing the NFM-P NE backup partition” (p. 29)

2.12.4 Live distributed main database partitioning scheme

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

Table 2-22 Live partitioning scheme, main database, distributed system

Disks required: four 300 Gbyte (RAID 0) or six 300 Gbyte (RAID 0)		Size (Gbytes)	
Partition	Content	Four disks	Six disks
swap	Swap space	16	
/	Root	26	
/home	User home directories	0.5	
/tmp	Temporary files	4	
/var	System data	64	
/var/log	System logs	6	
/var/log/audit	System audit logs	6	
/opt/nsp/nfmp	Main database software	120	

Table 2-22 Live partitioning scheme, main database, distributed system (continued)

Disks required: four 300 Gbyte (RAID 0) or six 300 Gbyte (RAID 0)		Size (Gbytes)	
Partition	Content	Four disks	Six disks
/opt/nsp/nfmp/dbbackup	Database backups	120	200
/opt/nsp/nfmp/db	Database tablespaces	360	500
/opt/nsp/nfmp/db/archivelog	Database archive logs	120	570
/opt/nsp/nfmp/db/redolog	Database redo logs	30	
/extra	NSP and NFM-P software storage	50	

2.12.5 Live auxiliary server partitioning scheme

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

Table 2-23 Live partitioning scheme, statistics-collection auxiliary server

Disks required: four 300 Gbyte (RAID 0)		
Partition	Content	Size (Gbytes)
swap	Swap space	16
/	Root	26
/home	User home directories	0.5
/tmp	Temporary files	4
/var	System data	64
/var/log	System logs	6
/var/log/audit	System audit logs	6
/opt/nsp	Auxiliary server software, operating data	180
/opt/nsp/nfmp/auxserver/nms/log	Auxiliary server logs	50
/opt/nsp/nfmp/auxserver/xml_output	Output of XML API file export operations	150
/extra	NSP and NFM-P software storage	50

2.12.6 Live auxiliary database partitioning scheme

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

For a multi-station auxiliary database, or a single-station database that has a high data rate, the /opt/nsp/nfmp/auxdb/backup partition has the following special requirements:

- It is strongly recommended that the partition is a remote mount point or directly attached storage connected by a minimum 10 Gbyte/s link.

- Each auxiliary database station requires a separate backup volume that is mounted as /opt/nsp/nfmp/auxdb/backup on the auxiliary database station.

  For example, if the specified auxiliary database backup location is /opt/nsp/nfmp/auxdb/backup, the auxiliary database stations require the following mount points:

  − station 1:

    `remote_host:station_1_backup_volume_path/opt/nsp/nfmp/auxdb/backup`

  − station 2:

    `remote_host:station_2_backup_volume_path/opt/nsp/nfmp/auxdb/backup`

  − station 3:

    `remote_host:station_3_backup_volume_path/opt/nsp/nfmp/auxdb/backup`

- The supported file systems for the backup location are ext3, ext4, and NFS.

Note: The /opt/nsp/nfmp/auxdb/backup partition can be a local mount point in a single-station database that has a low to moderate data rate.

Table 2-24 Live partitioning scheme, auxiliary database

Disks required: two 300 Gbyte (RAID 1), plus data storage and database backup storage capacity described in table		Size (Gbytes)	
Partition	Content	Single-station	Multi-station
swap	Swap space	16	
/	Root	26	
/home	User home directories	0.5	
/opt	NFM-P auxiliary database software	100	
/tmp	Temporary files	4	
/var	System data	64	
/var/log	System logs	6	
/var/log/audit	System audit logs	6	
/extra	NSP and NFM-P software storage	50	
Data storage disks required, RAID 1+0:		Four 1.2-Tbyte	Twelve 600 Gbyte
/opt/nsp/nfmp/auxdb/data	Auxiliary database data	2200	3300
Database backup storage disks required, RAID 5:		Four 1.2-Tbyte	Five 1.2-Tbyte
/opt/nsp/nfmp/auxdb/backup [1]	Auxiliary database backup data	3300	4400

Notes:

1. Auxiliary database backups are optional but strongly recommended to protect against complete data loss due to disk failure, data corruption, or upgrade failure. The backups can be stored on a separate volume, as indicated in the table above, or on a remote mount point reachable over a minimum 10 Gbyte/s link. The

listed capacity is sufficient for at least one persisted backup.

2.12.7 Live single-user client or client delegate server partitioning scheme

The following table lists the partitions required for the live deployment of a single-user client or client delegate server on RHEL.

Table 2-25 Live partitioning scheme, single-user client or client delegate server

Disks required: one 300 Gbyte		
Partition	Content	Size (Gbytes)
swap	Swap space	16
/	Root, including /usr and /var	26
/opt/nsp	NFM-P client software	16
At operator discretion	Customer data; can be partitioned according to customer requirements	Remainder

3 RHEL OS deployment for the NSP

3.1 Overview

3.1.1 Purpose

This chapter describes the following:

- NSP RHEL OS installation methods
- RHEL OS requirements for NSP deployment

3.1.2 Contents

NSP RHEL OS deployment

3.2 Introduction

3.2.1 OS deployment methods

CAUTION

System Support Violation

You must ensure that the NSP supports each update that you apply to a RHEL OS in an NSP deployment. An automated update by a subscription manager may deploy an unsupported RHEL version that you must subsequently roll back.

In order to avoid the accidental deployment of an unsupported RHEL version on an NSP station, it is strongly recommended that you lock the supported release in your RHEL subscription manager.

Before you attempt to deploy the RHEL OS in an NSP system, you must review the *NSP Planning Guide* and the *NSP and CLM Host Environment Compatibility Reference* for information about the RHEL OS support by NSP release.

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

You can install the required RHEL OS instance for an NSP component by:

- deploying an NSP disk image, as described in 2.2.2 “NSP disk-image deployment” (p. 28)
- manually, as described in “Manual NSP RHEL OS installation” (p. 70)

Note: Deploying an NSP disk image is the recommended method.

Note: It is strongly recommended that you verify the message digest of each NSP image file or software bundle that you download from the Nokia Support portal. The download page includes the MD5, SHA256, and SHA512 checksums for comparison with the output of the RHEL md5sum, sha256sum, or sha512sum command. See the associated RHEL man page for command usage information.

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

3.2.2 Time synchronization requirement

CAUTION

Service Degradation

Some components, for example, members of an etcd cluster, fail to trust data integrity in the presence of a time difference. Failing to closely synchronize the system clocks among components complicates troubleshooting and may cause a service outage.

Ensure that you use only the time service described in this section to synchronize the NSP components.

The system clocks of the NSP components must always be closely synchronized. The RHEL chronyd service is the mandatory time-synchronization mechanism that you must engage on each NSP component during deployment.

Note: Only one time-synchronization mechanism can be active in an NSP system. Before you enable chronyd on an NSP component, you must ensure that no other time-synchronization mechanism, for example, the VMware Tools synchronization utility, is enabled.

3.2.3 Required RHEL 8 swappiness workaround

As noted by Red Hat, the RHEL 8 swappiness setting is ineffective. Special configuration is required to resolve the issue on a RHEL OS instance. Red Hat provides corrective steps that you must perform on any RHEL OS instance that is designated to host any of the following NSP components:

- NSP Flow Collector
- NSP Flow Collector Controller
- collocated NSP Flow Collector Controller and Flow Collector
- NSP analytics server
- NFM-P:
  - main server
  - main database
  - collocated main server and database
  - auxiliary server
  - auxiliary database

Note: You must apply the RHEL workaround before you attempt to deploy any NSP software on the OS instance.

3.3 “To apply the RHEL 8 swappiness workaround” (p. 66) describes how to apply the workaround, which configures the RHEL OS to use cgroups v2 rather than v1.

3.2.4 OS security

The NSP includes various security mechanisms and system hardening options. The following topics describe established or configurable during RHEL OS installation.

RHEL 8 crypto-policy setting

The NSP provides system-wide support for a RHEL 8 crypto-policy setting of FUTURE. The setting is enabled and preconfigured on an OS instance deployed using an NSP RHEL OS OEM image.

A manually deployed OS instance, however, requires the creation of a custom sub-policy, as described in 3.16 “ To enable the NSP crypto-policy function on a manually installed RHEL OS” (p. 88).

SELinux

All NSP components support deployment on a RHEL OS that has SELinux enabled in permissive or enforcing mode, except an auxiliary database, which supports SELinux only in permissive mode.

You cannot upgrade an NSP component on which SELinux is enabled in enforcing mode, so must switch to permissive mode before the upgrade. Switching to SELinux enforcing mode is done only after a component installation or upgrade.

Note: An NSP RHEL disk image has SELinux enabled in permissive mode by default.

See “What is SELinux?” in the *NSP System Administrator Guide* for information about enabling and troubleshooting SELinux in an NSP system, and about switching between SELinux permissive mode and enforcing mode.

Removing executable world permissions

Optionally, you can remove the world permissions from RHEL compiler executable files, as described in A.1 “Resetting GCC-compiler file permissions” (p. 1093).

3.2.5 Applying OS updates

WARNING

System Failure

You must not attempt to apply an OS update as described below on a system that is not deployed as described in this guide, or catastrophic system failure may result. For example, applying the OS update on an NSP appliance host or NSP Server host results in the uninstallation of virsh and virt-manager, and causes all VMs to be removed.

You must perform the OS-update procedure only on a system deployed as described in this guide.

If you are upgrading the NSP in a VM created using an NSP RHEL OS disk image, you must apply a RHEL update to the OS before you can upgrade the component, as described in 3.4 “To apply a RHEL update to an NSP image-based OS” (p. 67).

Note: If the upgrade includes a migration to a new RHEL OS version, for example, an upgrade from NSP Release 22.6 or earlier, the update is included in the new OS image that you deploy, so you do not need to perform the procedure.

3.3 To apply the RHEL 8 swappiness workaround

3.3.1 Purpose

Perform this procedure before you attempt to install NSP software on a RHEL OS instance that is to host any of the following components:

- NSP Flow Collector
- NSP Flow Collector Controller
- collocated NSP Flow Collector Controller and Flow Collector
- NSP analytics server
- NFM-P:
  - main server
  - main database
  - collocated main server and database
  - auxiliary server
  - auxiliary database

3.3.2 Steps

1

Log in to the station as the root user.

2

Enter the following:

```
# grubby --update-kernel=ALL --args="systemd.unified_cgroup_
hierarchy=1" ↵
```

The workaround is applied.

3

Enter the following:

```
# systemctl reboot ↵
```

The station reboots.

4

Close the console window.

End of steps

3.4 To apply a RHEL update to an NSP image-based OS

3.4.1 Purpose

WARNING

System Failure

You must not attempt to apply the OS update on a system that is not deployed as described in this guide, or catastrophic NSP system failure may result. For example, applying the OS update on an NSP appliance host or NSP Server host results in the uninstallation of virsh and virt-manager, and causes all VMs to be removed.

You must perform the procedure only on a system deployed as described in this guide.

Perform this procedure to update an NSP RHEL OS instance deployed using an NSP RHEL OS disk image. Such an OS update may include RHEL patches or security enhancements, and is typically applied as part of an NSP system upgrade.

Note: The procedure applies only to a RHEL OS instance deployed using an NSP RHEL OS disk image, and is not to be performed on a manually deployed OS.

Note: An NSP component that you are upgrading requires the latest available update for the installed RHEL version.

Applying an OS update

In order to apply an OS update, you must shut down the NSP component hosted by the OS. During an upgrade, you are directed to shut down a component before you apply an OS update.

You must shut down and restart NSP components in a specific order. For information about performing a graceful shutdown and restart of components in a standalone or DR NSP deployment, see “Workflow: stop and start DR NSP clusters” in the *NSP System Administrator Guide*.

CAUTION

Network Visibility Loss

Applying an NSP RHEL OS update requires the shutdown of the component receiving the update, and may cause a temporary loss of network visibility, depending on the deployment.

You must perform the procedure only during a scheduled maintenance period.

3.4.2 Steps

1

Log in as the root user on the station that hosts the OS.

2

Open a console window.

3

Stop the NSP software on the component, see the *NSP System Administrator Guide* for information, as required:

- NSP cluster
- NSP Flow Collector / Flow Collector Controller
- NSP analytics server
- NFM-P main server
- NFM-P main database
- NFM-P auxiliary server
- auxiliary database

4

Enter the following:

```
# mkdir -p /opt/OSUpdate ↵
```

5

Download the following compressed file for the new NSP release to the /opt/OSUpdate directory:

NSP_RHEL*n*_OEM_UPDATE_*yy_mm*.tar.gz

where

n is the major release of the RHEL version that you are updating, for example, 8

yy_mm is the issue date of the OS update

6

Enter the following:

```
# cd /opt/OSUpdate ↵
```

7

Enter the following to expand the downloaded file:

```
# tar -zxvf NSP_RHELn_OEM_UPDATE_yy_mm.tar.gz ↵
```

The update files are extracted to the following directory:

/opt/OSUpdate/*R_r*-RHEL*V.v*-*yy.mm.dd*

where

R_r is the NSP release that introduces the OS update

V.v is the RHEL version, for example, 8.6

yy.mm.dd is the issue date of the OS update

8

Enter the following:

```
# cd R_r-RHELV.v-yy.mm.dd ↵
```

9

Enter the following to perform the OS update:

```
# ./yum_update.sh ↵
```

10

CAUTION

Misconfiguration Risk

Performing this step on a station running NSP Release 21.11 or earlier may have undesirable effects including degraded system performance and restricted system access.

You must perform the step only on a Release 23.4 or later NSP component station.

Optionally, to align with OS-hardening best practices as defined by the Center for Information Security, or CIS, perform the following steps to set the default login umask to 0027.

1. Back up the following files to a secure location on a station outside the management network for safekeeping:
   - /etc/bashrc
   - /etc/profile
   - /etc/login.defs
2. Enter the following:

   ```
   # sed -i 's/^\([[:space:]]*\)\(umask\|UMASK\)[[:space:]][[:space:]]*[0-9][0-9][0-9]/\1\2 027/'  /etc/bashrc /etc/profile /etc/login.defs ↵
   ```
3. Log out.
4. Log in as the root user.
5. Enter the following:

   ```
   # umask ↵
   ```

   The current umask value is displayed.
6. Verify that the umask value is 0027.

11

Enter the following:

```
# systemctl reboot ↵
```

The station reboots.

12

Close the console window.

End of steps

Manual NSP RHEL OS installation

3.5 Overview

3.5.1 Purpose

This section describes the manual rollout of a RHEL OS instance for use in an NSP deployment.

3.5.2 Contents

3.6 Manually installing the RHEL OS for the NSP

3.6.1 RHEL OS installation requirements

CAUTION

Upgrade Failure

The NSP system locale must remain unchanged after the initial system installation; otherwise, a system upgrade fails. Also, in an NSP system that includes the NFM-P, the NSP and NFM-P locales must match.

Ensure that you set the system locale on a component only before NSP software installation, and not afterward.

CAUTION

Risk of excessive resource consumption

The RHEL gnome desktop may consume excessive memory and result in system performance degradation.

The NSP does not require the gnome desktop, which is provided for customer and support convenience. It is recommended that you disable the gnome desktop in each RHEL OS instance in an NSP deployment if you do not require the gnome desktop.

You can stop the gnome desktop using the following command as the root user:

```
systemctl stop gdm ↵
```

To disable the gnome desktop so that it does not start after a reboot, enter the following as the root user:

```
systemctl disable gdm ↵
```

CAUTION

Deployment Failure

NSP software deployment may fail if the RHEL OS configuration includes a parameter setting that the NSP does not support.

Each RHEL OS configuration setting for an NSP component must remain at the default unless otherwise specified in the NSP documentation.

Each NSP VM or physical station requires a specifically configured base OS environment and set of RHEL OS packages that are described in this section.

Note: A manually installed RHEL OS instance for an NSP component must be established as described in this section; otherwise, NSP component deployment on the OS fails.

Note: After you successfully install an NSP RHEL OS instance, you can optionally install one or more packages listed in 3.14 “Optional RHEL OS packages” (p. 87).

3.6.2 Installing the OS packages

The procedures and examples in the NSP documentation use the RHEL dnf utility to orchestrate RHEL OS package installation and management.

If an OS package has dependencies on any additional packages that are not listed in the package documentation, the dnf utility installs the packages to resolve the dependencies.

dnf installs packages from RHEL ISO images or package repositories. A package repository is one of the following:

- local—created during RHEL OS installation
- Internet-based—accessible by registering with the Red Hat Network

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

Note: dnf uses the RHEL rpm utility, which 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.

Using dnf

You can use one dnf command to install or uninstall multiple OS packages. If you do not specify the -y option shown in the command examples below, dnf prompts you before installing or uninstalling each package.

The package installation syntax is:

```
dnf -y install package_1 package_2 ... package_n ↵
```

The package uninstallation syntax is:

```
dnf -y remove package_1 package_2 ... package_n ↵
```

3.7 Workflow for manual NSP RHEL OS installation

3.7.1 Purpose

The following is the sequence of high-level actions required to install an instance of the RHEL OS for use in an NSP system.

3.7.2 Stages

1

Using the RHEL installer, choose “Minimal Install” as the Software Selection for the OS.

2

Install the required OS package set.

a. For an NSP deployer host or NSP cluster member, install the packages listed in 3.8 “Required RHEL OS packages for NSP container elements” (p. 74).

b. For a component that is deployed outside the container environment, install the packages listed in 3.9 “Required RHEL OS packages for ancillary NSP components” (p. 77).

3

Remove specific OS packages that are installed by default but not required.

a. For an NSP deployer host or NSP cluster member, remove the packages listed in 3.10 “RHEL OS packages to remove from NSP container elements” (p. 84).

b. For a component that is deployed outside the container environment, remove the packages listed in 3.11 “RHEL OS packages to remove from ancillary components” (p. 85).

4

Perform any additional package configuration described in 3.12 “Special OS requirements” (p. 86), as required.

5

If required, add the packages listed in 3.13 “Required additional OS packages, NFM-P single-user client or client delegate server” (p. 86).

6

Perform 3.15 “To verify the rngd service startup” (p. 87) to ensure that the RHEL rngd service is loaded and running.

7

Perform 3.16 “ To enable the NSP crypto-policy function on a manually installed RHEL OS” (p. 88) to secure the OS using a RHEL crypto-policy setting.

Note: You must enable the crypto-policy function before you attempt to install any NSP software on a station.

8

Perform 3.17 “To set the default Python version” (p. 90) to configure the default Python language version to the version required by the NSP.

9

On an NSP deployer host or NSP cluster station, perform 3.18 “To create the nsp user on a manually installed NSP cluster RHEL OS” (p. 91) to create the RHEL nsp user.

10

Perform 3.19 “To disable the RHEL firewalld service” (p. 91) to ensure that the RHEL firewalld service is inactive during NSP component deployment.

11

Optionally, perform 3.20 “To set the default umask to 0027” (p. 92) to limit non-root-user file and directory access.

3.8 Required RHEL OS packages for NSP container elements

3.8.1 OS packages for NSP deployer host or cluster member

The OS for an NSP deployer host or a member node in an NSP cluster requires the RHEL OS package set listed in Table 3-1, “Required OS packages, NSP container element” (p. 75). A listed package is available from the RHEL BaseOS repository, RHEL AppStream repository, or the RHEL ISO disk image.

To facilitate the package installation, you can paste the following command block in a CLI:

Note: Specific versions of some packages are required, as described in 3.12 “Special OS requirements” (p. 86).

```
dnf -y install @base aide.x86_64 autofs.x86_64 bpftool.x86_64 c-ares.x86_64
dnf -y install cloud-utils-growpart.noarch compat-openssl10.x86_64
dnf -y install container-selinux.noarch copy-jdk-configs.noarch conntrack-tools.x86_64
dnf -y install createrepo_c.x86_64 cups-client.x86_64 cups-libs.x86_64 dialog.x86_64
dnf -y install elfutils.x86_64 fio.x86_64 flac-libs.x86_64 ftp.x86_64 gc.x86_64
dnf -y install gtk2.x86_64 guile.x86_64 haproxy.x86_64 hdparm.x86_64 hyphen-en.noarch
dnf -y install ipvsadm.x86_64 irqbalance.x86_64 javapackages-tools.noarch
dnf -y install keepalived.x86_64 libkadm5.x86_64 libnetfilter_cthelper.x86_64
dnf -y install libnetfilter_cttimeout.x86_64 libnetfilter_queue.x86_64 libquadmath.x86_64
dnf -y install libselinux-devel.x86_64 libverto-libevent.x86_64 lksctp-tools.x86_64
dnf -y install lshw.x86_64 lsof.x86_64 man mcelog.x86_64 net-snmp.x86_64
dnf -y install net-snmp-utils.x86_64 network-scripts.x86_64 nfs-utils.x86_64
dnf -y install nspr.x86_64 nss-softokn.x86_64 nss-softokn-freebl.x86_64 nss-util.x86_64
dnf -y install ntpstat.noarch openssh.x86_64 openssh-askpass.x86_64
dnf -y install openssh-clients.x86_64 openssh-server.x86_64 policycoreutils.x86_64
dnf -y install pcsc-lite-libs.x86_64 procps python3 python3-babel.noarch
dnf -y install python3-jinja2.noarch python3-jmespath.noarch python3-jsonpatch.noarch
dnf -y install python3-jsonpointer.noarch python3-ldb.x86_64 python3-libselinux.x86_64
dnf -y install python3-markupsafe.x86_64 python3-netaddr.noarch python3-oauthlib.noarch
dnf -y install python3-prettytable.noarch python3-pytz.noarch python3-tdb.x86_64
dnf -y install python3-urllib3.noarch redhat-lsb-core.x86_64
dnf -y install redhat-lsb-submod-security.x86_64 rng-tools.x86_64 rsync.x86_64
dnf -y install selinux-policy-devel.noarch selinux-policy-doc.noarch
dnf -y install setroubleshoot-server.x86_64 setools-console.x86_64 sshpass.x86_64
dnf -y install socat.x86_64 tcpdump.x86_64 tzdata-java.noarch unzip.x86_64 which.x86_64
dnf -y install zip.x86_64
```

Table 3-1 Required OS packages, NSP container element

Package	Description
@base	Roles and playbooks to deploy FreeIPA servers, replicas and client
aide.x86_64	Intrusion detection environment
autofs.x86_64	Libraries for avahi run-time use
bpftool.x86_64	A 2D graphics library
c-ares.x86_64	A library that performs asynchronous DNS operations
cloud-utils-growpart.noarch	Script for growing a partition
compat-openssl10.x86_64	Compatibility version of the OpenSSL library
conntrack-tools.x86_64	Userspace tools for interacting with the Connection Tracking System
container-selinux.noarch	SELinux policies for container runtimes
copy-jdk-configs.noarch	JDKs configuration files copier
createrepo_c.x86_64	Creates a common metadata repository
cups-client.x86_64	CUPS printing system - client programs
cups-libs.x86_64	CUPS printing system - libraries
dialog.x86_64	A utility for creating TTY dialog boxes
elfutils.x86_64	A collection of utilities and DSOs to handle ELF files and DWARF data
fio.x86_64	Multithreaded IO generation tool
flac-libs.x86_64	Libraries for the Free Lossless Audio Codec
ftp.x86_64	The standard UNIX FTP client
gc.x86_64	A garbage collector for C and C++
gtk2.x86_64	GTK+ graphical user interface library
guile.x86_64	A GNU implementation of Scheme for application extensibility
haproxy.x86_64	HAProxy reverse proxy for high availability environments
hdparm.x86_64	A utility for displaying and/or setting hard disk parameters
hyphen-en.noarch	English hyphenation rules
ipvsadm.x86_64	Utility to administer the Linux Virtual Server
irqbalance.x86_64	IRQ balancing daemon
javapackages-tools.noarch	Macros and scripts for Java packaging support
keepalived.x86_64	High Availability monitor built upon LVS, VRRP and service pollers
libkadm5.x86_64	Kerberos 5 Administrative libraries
libnetfilter_cthelper.x86_64	User-space infrastructure for connection tracking helpers
libnetfilter_cttimeout.x86_64	Timeout policy tuning for Netfilter/conntrack Fedora Rawhide for x86_64

Table 3-1 Required OS packages, NSP container element (continued)

Package	Description
libnetfilter_queue.x86_64	Netfilter queue userspace library, Fedora Rawhide for x86_64
libquadmath.x86_64	GCC __float128 shared support library
libselinux-devel.x86_64	Header files and libraries used to build SELinux
libverto-libevent.x86_64	libevent module for libverto
lksctp-tools.x86_64	User-space access to Linux Kernel SCTP
lshw.x86_64	Hardware lister
lsof.x86_64	A utility that lists open files on a Linux/UNIX system
man	Linux kernel and C library user-space interface documentation
mcelog.x86_64	Tool to translate x86-64 CPU Machine Check Exception date
net-snmp.x86_64	A collection of SNMP protocol tools and libraries
net-snmp-utils.x86_64	Network management utilities using SNMP, from the NET-SNMP project
network-scripts.x86_64	Legacy scripts for manipulating of network devices
nfs-utils.x86_64	NFS utilities and supporting clients and daemons for the kernel NFS server
nspr.x86_64	Netscape Portable Runtime
nss-softokn.x86_64	Network Security Services Softoken Module
nss-softokn-freebl.x86_64	Freebl library for the Network Security Services
nss-util.x86_64	Network Security Services Utilities Library
ntpstat.noarch	Utility to print NTP synchronization status
openssh.x86_64	An open source implementation of SSH protocol version 2
openssh-askpass.x86_64	A passphrase dialog for OpenSSH and X
openssh-clients.x86_64	An open source SSH client application
openssh-server.x86_64	An open source SSH server daemon
policycoreutils.x86_64	SELinux policy core utilities
pcsc-lite-libs.x86_64	PC/SC Lite libraries
procps	System and process monitoring utilities
python3	Interpreter of the Python programming language
python3-babel.noarch	Library for internationalizing Python applications
python3-jinja2.noarch	General purpose template engine for Python 3
python3-jmespath.noarch	JSON Matching Expressions
python3-jsonpatch.noarch	Applying JSON Patches in Python 3
python3-jsonpointer.noarch	Resolve JSON Pointers in Python

Table 3-1 Required OS packages, NSP container element (continued)

Package	Description
python3-ldb.x86_64	Python bindings for the LDB library
python3-libselinux.x86_64	SELinux python 3 bindings for libselinux Fedora Rawhide for x86_64
python3-markupsafe.x86_64	Implements a XML/HTML/XHTML Markup safe string for Python 3
python3-netaddr.noarch	A pure Python network address representation and manipulation library
python3-oauthlib.noarch	An implementation of the OAuth request-signing login
python3-prettytable.noarch	Python library to display tabular data in tables
python3-pytz.noarch	World Timezone Definitions for Python
python3-tdb.x86_64	Python3 bindings for the Tdb library
python3-urllib3.noarch	Python3 HTTP module with connection pooling and file POST abilities.
redhat-lsb-core.x86_64	LSB Core module support
redhat-lsb-submod-security.x86_64	LSB Security sub-module support
rng-tools.x86_64	Random number generator related utilities
rsync.x86_64	A program for synchronizing files over a network
selinux-policy-devel.noarch	SELinux policy devel
selinux-policy-doc.noarch	SELinux policy documentation
setroubleshoot-server.x86_64	SELinux troubleshooting
setools-console.x86_64	Policy analysis command-line tools for SELinux
sshpass.x86_64	Non-interactive SSH authentication utility
socat.x86_64	Bidirectional data relay between two data channels 'netcat++’
tcpdump.x86_64	A network traffic monitoring tool
tzdata-java.noarch	Timezone data for Java
unzip.x86_64	A utility for unpacking zip files
which.x86_64	Displays where a particular program in your path is located
zip.x86_64	A file compression and packaging utility compatible with PKZIP

3.9 Required RHEL OS packages for ancillary NSP components

3.9.1 OS packages for components outside NSP cluster

For a system component that you deploy outside an NSP cluster, you must install the common RHEL OS package set listed in Table 3-2, “Required OS packages, ancillary component” (p. 79). A listed package is available from the RHEL BaseOS repository, RHEL AppStream repository, or the RHEL ISO disk image.

The components that require the package set are the following:

- NFM-P main and auxiliary servers and databases
- NSP Flow Collectors and Flow Collector Controllers
- NSP analytics servers

To facilitate the package installation, you can paste the following command block in a CLI:

Note: Specific versions of some packages are required, as described in 3.12 “Special OS requirements” (p. 86).

```
dnf -y install @base aide.x86_64 atk.i686 autofs.x86_64 avahi-libs.i686 bc.x86_64
dnf -y install binutils.x86_64 binutils-devel.i686 bpftool.x86_64 c-ares.x86_64 cairo.i686
dnf -y install cloud-utils-growpart.noarch compat-openssl10.x86_64
dnf -y install container-selinux.noarch copy-jdk-configs.noarch createrepo_c.x86_64
dnf -y install cups-client.x86_64 cups-libs.x86_64 cups-libs.i686 dbus-libs.i686
dnf -y install dialog.x86_64 elfutils.x86_64 elfutils-libelf-devel.x86_64
dnf -y install elfutils-libelf-devel.i686 elfutils-libelf.i686 fio.x86_64 flac-libs.x86_64
dnf -y install fontconfig-devel.x86_64 fontconfig-devel.i686 fribidi.i686 ftp.x86_64
dnf -y install gc.x86_64 gcc.x86_64 gcc-c++.x86_64 gcc-gfortran.x86_64 gdb.x86_64
dnf -y install gdb-headless.x86_64 gdk-pixbuf2-modules.i686 gdk-pixbuf2.i686 glib2.i686
dnf -y install glibc.x86_64 glibc-devel.x86_64 glibc-devel.i686 glibc.i686 gmp.i686
dnf -y install gnutls.i686 graphite2.i686 gtk2.x86_64 gtk2.i686 guile.x86_64
dnf -y install haproxy.x86_64 harfbuzz.i686 hdparm.x86_64 hyphen-en.noarch
dnf -y install irqbalance.x86_64 jasper-libs.i686 javapackages-tools.noarch
dnf -y install jbigkit-libs.i686 keepalived.x86_64 keyutils-libs-devel.x86_64
dnf -y install krb5-devel.x86_64 ksh.x86_64 libaio.x86_64 libaio-devel.x86_64
dnf -y install libaio-devel.i686 libaio.i686 libcom_err-devel.x86_64 libcurl-devel.x86_64
dnf -y install libffi-devel.x86_64 libgcc.x86_64 libgcc.i686 libgcrypt-devel.x86_64
dnf -y install libgfortran.x86_64 libgpg-error-devel.x86_64 libibverbs.x86_64
dnf -y install libibverbs.i686 libkadm5.x86_64 libnsl.i686 libnsl.x86_64
dnf -y install libquadmath.x86_64 libquadmath-devel.x86_64 librdmacm.i686
dnf -y install librdmacm.x86_64 libselinux-devel.x86_64 libsepol-devel.x86_64
dnf -y install libstdc++.x86_64 libstdc++-devel.x86_64 libstdc++-devel.i686 libstdc++.i686
dnf -y install libverto-devel.x86_64 libverto-libevent.x86_64 libX11.i686 libX11.x86_64
dnf -y install libXau.i686 libXau.x86_64 libxcb.i686 libxcb.x86_64 libXi.x86_64 libXi.i686
dnf -y install libxml2-devel.x86_64 libXrender.x86_64 libXrender.i686 libxslt-devel.x86_64
dnf -y install libXtst.x86_64 libXtst.i686 lksctp-tools.x86_64 lshw.x86_64 lsof.x86_64
dnf -y install make.x86_64 man mcelog.x86_64 net-snmp.x86_64 net-snmp-utils.x86_64
dnf -y install network-scripts.x86_64 nfs-utils.x86_64 nspr.x86_64 nss-softokn.x86_64
dnf -y install nss-softokn-freebl.x86_64 nss-softokn-freebl.i686 nss-util.x86_64
dnf -y install ntpstat.noarch numactl-devel.x86_64 numactl-devel.i686 numad.x86_64
dnf -y install openssh.x86_64 openssh-askpass.x86_64 openssh-clients.x86_64
dnf -y install openssh-server.x86_64 openssl-devel.x86_64 policycoreutils.x86_64
dnf -y install pcre-devel.x86_64 pcsc-lite-libs.x86_64 procps python3 python3-babel.noarch
dnf -y install python3-jinja2.noarch python3-markupsafe.x86_64 python3-pytz.noarch
dnf -y install python3-jmespath.noarch python3-netaddr.noarch python3-jsonpatch.noarch
dnf -y install python3-jsonpointer.noarch python3-ldb.x86_64 python3-oauthlib.noarch
dnf -y install python3-prettytable.noarch python3-tdb.x86_64 python3-urllib3.noarch
dnf -y install redhat-lsb-core.x86_64 redhat-lsb-submod-security.x86_64 rng-tools.x86_64
dnf -y install rsync.x86_64 selinux-policy-devel.noarch selinux-policy-doc.noarch
dnf -y install setroubleshoot-server.x86_64 setools-console.x86_64 sshpass.x86_64
dnf -y install smartmontools.x86_64 socat.x86_64 sysstat.x86_64 tcpdump.x86_64
dnf -y install tzdata-java.noarch unzip.x86_64 which.x86_64 xz-devel.x86_64 zip.x86_64
```

Table 3-2 Required OS packages, ancillary component

Package	Description
@base	Roles and playbooks to deploy FreeIPA servers, replicas and client
aide.x86_64	Intrusion detection environment
atk.i686	A tool for automatically mounting and unmounting file systems
autofs.x86_64	Libraries for avahi run-time use
avahi-libs.i686	GNU's bc numeric processing language and dc, a calculator
bc.x86_64	A GNU collection of binary utilities
binutils.x86_64	BFD and opcodes static and dynamic libraries and header files
binutils-devel.i686	Inspection and simple manipulation of eBPF programs and maps
bpftool.x86_64	A 2D graphics library
c-ares.x86_64	A library that performs asynchronous DNS operations
cairo.i686	A library that performs asynchronous DNS operations
cloud-utils-growpart.noarch	Script for growing a partition
compat-openssl10.x86_64	Compatibility version of the OpenSSL library
container-selinux.noarch	SELinux policies for container runtimes
copy-jdk-configs.noarch	JDKs configuration files copier
createrepo_c.x86_64	Creates a common metadata repository
cups-client.x86_64	CUPS printing system - client programs
cups-libs.x86_64	CUPS printing system - libraries
cups-libs.i686	CUPS printing system - libraries
dbus-libs.i686	Libraries for accessing D-BUS
dialog.x86_64	A utility for creating TTY dialog boxes
elfutils.x86_64	A collection of utilities and DSOs to handle ELF files and DWARF data
elfutils-libelf-devel.x86_64	Development support for libelf
elfutils-libelf-devel.i686	Development support for libelf
elfutils-libelf.i686	Library to read and write ELF files
fio.x86_64	Multithreaded IO generation tool
flac-libs.x86_64	Libraries for the Free Lossless Audio Codec
fontconfig-devel.x86_64	Font configuration and customization library
fontconfig-devel.i686	Font configuration and customization library

Table 3-2 Required OS packages, ancillary component (continued)

Package	Description
fribidi.i686	Library implementing the Unicode Bidirectional Algorithm
ftp.x86_64	The standard UNIX FTP client
gc.x86_64	A garbage collector for C and C++
gcc.x86_64	Various compilers (C, C++, Objective-C, etc.)
gcc-c++.x86_64	C++ support for GCC
gcc-gfortran.x86_64	Fortran support
gdb.x86_64	A stub package for GNU source-level debugger
gdb-headless.x86_64	A GNU source-level debugger for C, C++, Fortran, Go and other languages
gdk-pixbuf2-modules.i686	Additional image modules for gdk-pixbuf
gdk-pixbuf2.i686	An image loading library
glib2.i686	A library of handy utility functions
glibc.x86_64	The GNU libc libraries
glibc-devel.x86_64	Object files for development using standard C libraries
glibc-devel.i686	Object files for development using standard C libraries
glibc.i686	The GNU libc libraries
gmp.i686	A GNU arbitrary precision library
gnutls.i686	A TLS protocol implementation
graphite2.i686	Font rendering capabilities for complex non-Roman writing systems
gtk2.x86_64	GTK+ graphical user interface library
gtk2.i686	GTK+ graphical user interface library
guile.x86_64	A GNU implementation of Scheme for application extensibility
haproxy.x86_64	HAProxy reverse proxy for high availability environments
harfbuzz.i686	Text shaping library
hdparm.x86_64	A utility for displaying and/or setting hard disk parameters
hyphen-en.noarch	English hyphenation rules
irqbalance.x86_64	IRQ balancing daemon
jasper-libs.i686	Runtime libraries for jasper
javapackages-tools.noarch	Macros and scripts for Java packaging support
jbigkit-libs.i686	JBIG1 lossless image compression library
keepalived.x86_64	High Availability monitor built upon LVS, VRRP and service pollers
keyutils-libs-devel.x86_64	Development package for building Linux key management utilities

Table 3-2 Required OS packages, ancillary component (continued)

Package	Description
krb5-devel.x86_64	Development files needed to compile Kerberos 5 programs
ksh.x86_64	The Original ATT Korn Shell
libaio.x86_64	Linux-native asynchronous I/O access library
libaio-devel.x86_64	Development files for Linux-native asynchronous I/O access
libaio-devel.i686	Development files for Linux-native asynchronous I/O access
libaio.i686	Linux-native asynchronous I/O access library
libcom_err-devel.x86_64	Common error description library
libcurl-devel.x86_64	Files needed for building applications with libcurl
libffi-devel.x86_64	Development files for libffi
libgcc.x86_64	GCC version 8 shared support library
libgcc.i686	GCC version 8 shared support library
libgcrypt-devel.x86_64	Development files for the libgcrypt package
libgfortran.x86_64	Fortran runtime
libgpg-error-devel.x86_64	Development files for the libgpg-error package
libibverbs.x86_64	A library and drivers for direct userspace use of RDMA InfiniBand/iWARP/RoCE hardware
libibverbs.i686	A library and drivers for direct userspace use of RDMA InfiniBand/iWARP/RoCE hardware
libkadm5.x86_64	Kerberos 5 Administrative libraries
libnsl.i686	Legacy support library for NIS
libnsl.x86_64	Legacy support library for NIS
libquadmath.x86_64	GCC __float128 shared support library
libquadmath-devel.x86_64	GCC __float128 support
librdmacm.i686	Userspace RDMA Connection Manager
librdmacm.x86_64	Userspace RDMA Connection Manager
libselinux-devel.x86_64	Header files and libraries used to build SELinux
libsepol-devel.x86_64	Header files and libraries used to build policy manipulation tools
libstdc++.x86_64	GNU Standard C++ Library
libstdc++-devel.x86_64	Header files and libraries for C++ development
libstdc++-devel.i686	Header files and libraries for C++ development
libstdc++.i686	Header files and libraries for C++ development
libverto-devel.x86_64	Development files for libverto
libverto-libevent.x86_64	libevent module for libverto

Table 3-2 Required OS packages, ancillary component (continued)

Package	Description
libX11.i686	Core X11 protocol client library
libX11.x86_64	Core X11 protocol client library
libXau.i686	Sample Authorization Protocol for X
libXau.x86_64	Sample Authorization Protocol for X
libxcb.i686	A C binding to the X11 protocol
libxcb.x86_64	A C binding to the X11 protocol
libXi.x86_64	X.Org X11 libXi runtime library
libXi.i686	X.Org X11 libXi runtime library
libxml2-devel.x86_64	Libraries, includes, etc. to develop XML and HTML applications
libXrender.x86_64	X.Org X11 libXrender runtime library
libXrender.i686	X.Org X11 libXrender runtime library
libxslt-devel.x86_64	Development libraries and header files for libxslt
libXtst.x86_64	X.Org X11 libXtst runtime library
libXtst.i686	X.Org X11 libXtst runtime library
lksctp-tools.x86_64	User-space access to Linux Kernel SCTP
lshw.x86_64	Hardware lister
lsof.x86_64	A utility that lists open files on a Linux/UNIX system
make.x86_64	A GNU tool that simplifies the build process for users
man	Linux kernel and C library user-space interface documentation
mcelog.x86_64	Tool to translate x86-64 CPU Machine Check Exception date
net-snmp.x86_64	A collection of SNMP protocol tools and libraries
net-snmp-utils.x86_64	Network management utilities using SNMP, from the NET-SNMP project
network-scripts.x86_64	Legacy scripts for manipulating of network devices
nfs-utils.x86_64	NFS utilities and supporting clients and daemons for the kernel NFS server
nspr.x86_64	Netscape Portable Runtime
nss-softokn.x86_64	Network Security Services Softoken Module
nss-softokn-freebl.x86_64	Freebl library for the Network Security Services
nss-softokn-freebl.i686	Freebl library for the Network Security Services
nss-util.x86_64	Network Security Services Utilities Library
ntpstat.noarch	Utility to print NTP synchronization status
numactl-devel.x86_64	Development package for building Applications that use numa

Table 3-2 Required OS packages, ancillary component (continued)

Package	Description
numactl-devel.i686	Development package for building Applications that use numa
numad.x86_64	Userspace daemon that automatically binds workloads to NUMA nodes
openssh.x86_64	An open source implementation of SSH protocol version 2
openssh-askpass.x86_64	A passphrase dialog for OpenSSH and X
openssh-clients.x86_64	An open source SSH client application
openssh-server.x86_64	An open source SSH server daemon
openssl-devel.x86_64	Files for development of applications that use OpenSSL
policycoreutils.x86_64	SELinux policy core utilities
pcre-devel.x86_64	Development files for pcre
pcsc-lite-libs.x86_64	PC/SC Lite libraries
procps	System and process monitoring utilities
python3	Interpreter of the Python programming language
python3-babel.noarch	Library for internationalizing Python applications
python3-jinja2.noarch	General purpose template engine for Python 3
python3-markupsafe.x86_64	Implements a XML/HTML/XHTML Markup safe string for Python 3
python3-pytz.noarch	World Timezone Definitions for Python
python3-jmespath.noarch	JSON Matching Expressions
python3-netaddr.noarch	A pure Python network address representation and manipulation library
python3-jsonpatch.noarch	Applying JSON Patches in Python 3
python3-jsonpointer.noarch	Resolve JSON Pointers in Python
python3-ldb.x86_64	Python bindings for the LDB library
python3-oauthlib.noarch	An implementation of the OAuth request-signing login
python3-prettytable.noarch	Python library to display tabular data in tables
python3-tdb.x86_64	Python3 bindings for the Tdb library
python3-urllib3.noarch	Python3 HTTP module with connection pooling and file POST abilities.
redhat-lsb-core.x86_64	LSB Core module support
redhat-lsb-submod-security.x86_64	LSB Security sub-module support
rng-tools.x86_64	Random number generator related utilities
rsync.x86_64	A program for synchronizing files over a network
selinux-policy-devel.noarch	SELinux policy devel
selinux-policy-doc.noarch	SELinux policy documentation

Table 3-2 Required OS packages, ancillary component (continued)

Package	Description
setroubleshoot-server.x86_64	SELinux troubleshooting
setools-console.x86_64	Policy analysis command-line tools for SELinux
sshpass.x86_64	Non-interactive SSH authentication utility
smartmontools.x86_64	Tools for monitoring SMART capable hard disks
socat.x86_64	Bidirectional data relay between two data channels 'netcat++'
sysstat.x86_64	Collection of performance monitoring tools for Linux
tcpdump.x86_64	A network traffic monitoring tool
tzdata-java.noarch	Timezone data for Java
unzip.x86_64	A utility for unpacking zip files
which.x86_64	Displays where a particular program in your path is located
xz-devel.x86_64	Devel libraries & headers for liblzma
zip.x86_64	A file compression and packaging utility compatible with PKZIP

3.10 RHEL OS packages to remove from NSP container elements

3.10.1 OS packages to remove from NSP deployer host or cluster member

After you install the required RHEL base environment and OS packages for an NSP deployer host or a member node in an NSP cluster, you must remove the packages listed in Table 3-3, “RHEL packages to remove, NSP container element” (p. 84). The packages are installed by default, but not required by the NSP.

To facilitate the package removal, you can paste the following command block in a CLI:

```
dnf -y remove esmtp.x86_64 gnupg2-smime iwl6000-firmware
dnf -y remove libconfig.x86_64 libesmtp.x86_64
dnf -y remove liblockfile.x86_64 libstoragemgmt.x86_64
dnf -y remove nmap-ncat python3-beautifulsoup4.noarch
dnf -y remove python3-cssselect.noarch python3-html5lib
dnf -y remove python3-webencodings realmd timedatex trousers
dnf -y remove trousers-lib
```

Table 3-3 RHEL packages to remove, NSP container element

Package	Description
esmtp.x86_64	User-configurable send-only Mail Transfer Agent
gnupg2-smime	CMS encryption and signing tool and smart card support for GnuPG
iwl6000-firmware	Firmware for Intel(R) Wireless WiFi Link 6000 AGN Adapter
libconfig.x86_64	C/C++ configuration file library

Table 3-3 RHEL packages to remove, NSP container element (continued)

Package	Description
libesmtp.x86_64	SMTP client library
liblockfile.x86_64	This implements a number of functions found in -lmail on SysV system
libstoragemgmt.x86_64	Storage array management library Fedora Rawhide for aarch64
nmap-ncat	Nmap's Netcat replacement Fedora Rawhide for aarch64
python3-beautifulsoup4.noarch	HTML/XML parser for quick-turnaround applications like screen-scraping
python3-cssselect.noarch	Serializer for literal Python expressions
python3-html5lib	A python based HTML parser/tokenizer
python3-webencodings	Documentation for python-webencodings
realmd	Kerberos realm enrollment service Fedora Rawhide for aarch64
timedatex	D-Bus service for system clock and RTC settings CentOS 8-stream BaseOS for aarch64
trousers	TSS (TCG Software Stack) access daemon for a TPM chip OpenSuSE Leap 15.4 for aarch64
trousers-lib	TrouSerS libtspi library Fedora Rawhide for aarch64

3.11 RHEL OS packages to remove from ancillary components

3.11.1 OS packages to remove from components outside NSP cluster

After you install the required RHEL base environment and OS packages on a component that is deployed outside an NSP cluster, you must remove the packages listed in Table 3-4, “RHEL packages to remove, ancillary component” (p. 85). The packages are installed by default, but not required by the NSP.

To facilitate the package removal, you can paste the following command block in a CLI:

```
dnf -y remove gnupg2-smime iwl6000-firmware python3-webencodings python3-html5lib
dnf -y remove timedatex trousers trousers-lib libstoragemgmt.x86_64 nmap-ncat realmd
```

Table 3-4 RHEL packages to remove, ancillary component

Package	Description
gnupg2-smime	CMS encryption and signing tool and smart card support for GnuPG
iwl6000-firmware	Firmware for Intel(R) Wireless WiFi Link 6000 AGN Adapter
libstoragemgmt.x86_64	Storage array management library Fedora Rawhide for aarch64
nmap-ncat	Nmap's Netcat replacement Fedora Rawhide for aarch64
python3-webencodings	Documentation for python-webencodings
python3-html5lib	A python based HTML parser/tokenizer
realmd	Kerberos realm enrollment service Fedora Rawhide for aarch64

Table 3-4 RHEL packages to remove, ancillary component (continued)

Package	Description
timedatex	D-Bus service for system clock and RTC settings CentOS 8-stream BaseOS for aarch64
trousers	TSS (TCG Software Stack) access daemon for a TPM chip OpenSuSE Leap 15.4 for aarch64
trousers-lib	TrouSerS libtspi library Fedora Rawhide for aarch64

3.12 Special OS requirements

3.12.1 Required OS package versions

The NSP requires the minimum version or later of each RHEL package listed in Table 3-5, “Required RHEL OS package versions” (p. 86). If an installed package version is lower than the minimum, you must upgrade the package to at least the minimum,

You can use the following commands to check the current package versions:

```
# dnf list installed | grep container-selinux ↵
```

```
# dnf list installed | grep tzdata-java ↵
```

Note: If the minimum version is not installed, NSP component deployment may fail.

As required, use the following CLI commands to upgrade one or more packages:

```
dnf -y install container-selinux

dnf -y install tzdata-java
```

Table 3-5 Required RHEL OS package versions

Package	Minimum required version
container-selinux	2.191.0-1
tzdata-java	2023c

3.13 Required additional OS packages, NFM-P single-user client or client delegate server

3.13.1 Description

Table 3-6, “Required additional OS packages, NFM-P single-user client or client delegate server” (p. 87) lists the additional OS packages that an NFM-P RHEL single-user client or client delegate server requires.

Note: You must ensure that you remove the packages in 3.10 “RHEL OS packages to remove from NSP container elements” (p. 84) after you add the packages in the table below.

To facilitate the package installation, you can paste the following command block in a CLI:

```
dnf -y install @gnome-desktop @legacy-x @base-x firefox.x86_64
```

Table 3-6 Required additional OS packages, NFM-P single-user client or client delegate server

Package	Description
@gnome-desktop	Gnome package group
@legacy-x	Legacy X package group
@base-x	X11 package group
firefox.x86_64	Mozilla Firefox web browser

3.14 Optional RHEL OS packages

3.14.1 Optional RHEL OS packages

Table 3-7, “Optional RHEL OS packages” (p. 87) lists the packages that you can opt to install for any component without affecting NSP operation.

Note: The packages are not included in the NSP RHEL OS disk images.

To facilitate the package installation, you can paste the following command block in a CLI:

```
dnf -y install @gnome-desktop @legacy-x @base-x firefox.x86_64
dnf -y install tigervnc-server.x86_64
```

Table 3-7 Optional RHEL OS packages

Package	Description
@gnome-desktop	Gnome package group
@legacy-x	Legacy X package group
@base-x	X11 package group
firefox.x86_64	Mozilla Firefox web browser
tigervnc-server.x86_64	Server for the VNC remote display system

3.15 To verify the rngd service startup

3.15.1 Purpose

Perform this procedure to ensure that the RHEL rngd service is loaded and running on each NFM-P component.

Note: You must perform the steps on each NFM-P component station.

3.15.2 Steps

1

Log in as the root user.

2

Enter the following:

```
# systemctl status rngd.service ↵
```

The service status is displayed; if the status includes the following, the service is loaded and running:

```
   Loaded: loaded (/usr/lib/systemd/system/rngd.service; enabled;
vendor preset)
   Active: active (running) since timestamp; uptime
```

where

timestamp is the service startup time

uptime is the amount of time since the service startup

3

If the status output indicates that the service is not loaded and running, enter the following to start the service:

```
# systemctl enable rngd.service ↵
# systemctl start rngd.service ↵
```

The service starts.

End of steps

3.16 To enable the NSP crypto-policy function on a manually installed RHEL OS

3.16.1 Purpose

Perform this procedure to configure the minimum RSA cryptography key length for the RHEL crypto-policy function on a NSP OS instance.

Note: The crypto-policy function is not enabled on the OS until you perform the procedure.

Note: You must perform the procedure before you install any NSP software on the OS.

3.16.2 Steps

1

Log in as the root user on the station that hosts the OS.

2

Enter the following:

```
# cat /etc/crypto-policies/config ↵
```

The following crypto-policy setting is displayed:

```
DEFAULT
```

3

Create the following file using a plain-text editor such as vi:

/etc/crypto-policies/policies/modules/NSP_CUSTOM_RSA_SIZE.pmod

4

Edit the file to read as follows:

```
min_rsa_size = 2048
```

5

Save and close the file.

6

Enter the following:

```
# cat NSP_CUSTOM_RSA_SIZE.pmod ↵
```

The edited file is displayed.

7

Ensure that the file reads as follows:

```
min_rsa_size = 2048
```

8

Enter the following:

```
# update-crypto-policies --set FUTURE:NSP_CUSTOM_RSA_SIZE ↵
```

Messages like the following are displayed.

```
Setting system policy to FUTURE:NSP_CUSTOM_RSA_SIZE
Note: System-wide crypto policies are applied on application start-up.
It is recommended to restart the system for the change of policies to
fully take place.
```

If the output is as shown, the crypto-policy configuration is successful.

9

If the crypto-policy configuration succeeds, enter the following:

```
# systemctl reboot ↵
```

The station reboots.

10

Log in as the root user.

11

Open a console window.

12

Enter the following:

```
# cat /etc/crypto-policies/config ↵
```

The crypto-policy setting is displayed.

13

Verify that the crypto-policy setting reads as follows:

```
FUTURE:NSP_CUSTOM_RSA_SIZE
```

14

Close the console window.

END OF STEPS

3.17 To set the default Python version

3.17.1 Purpose

Perform the procedure to set the default version of the Python language that the NSP requires. The setting is required after a manual RHEL OS installation for an NSP component, and before any NSP software is installed on the component station.

ℹ **Note:** You must perform the procedure on each station in an NSP deployment that has a manually installed RHEL OS.

ℹ **Note:** You do not need to perform the procedure on a RHEL OS deployed using the NSP qcow2 OS image, as the OS image includes the setting.

3.17.2 Steps

1

Log in as the root user on the station.

2

Enter the following:

```
# alternatives --set python /usr/bin/python3 ↵
```

The setting is applied.

3

Close the console window.

End of steps

3.18 To create the nsp user on a manually installed NSP cluster RHEL OS

3.18.1 Purpose

Perform the procedure to create the Linux nsp user as the owner of files and processes on a station that are otherwise associated by default with user ID 1000.

The procedure applies only to a manually installed RHEL OS on the following:

- NSP deployer host
- NSP cluster node

You must perform the procedure on each such NSP station after a manual RHEL OS installation, and before any NSP software is installed on the station.

Note: You do not need to perform the procedure on a RHEL OS deployed using the NSP qcow2 OS image, as the OS image includes the setting.

3.18.2 Steps

1

Log in as the root user on the station.

2

Enter the following:

```
# useradd --shell /sbin/nologin --no-create-home --uid 1000
--user-group nsp ↵
```

The nsp user account is created in the nsp user group.

3

Close the console window.

End of steps

3.19 To disable the RHEL firewalld service

3.19.1 Purpose

You must stop and disable the RHEL firewalld service on each station in an NSP deployment before you attempt to install an NSP component on a station.

Perform this procedure to disable firewalld on an NSP component station.

3.19.2 Steps

1

Log in as the root user on the station.

2

Open a console window.

3

Enter the following:

```
# systemctl stop firewalld ↵
```

The firewalld service stops.

4

Enter the following:

```
# systemctl disable firewalld ↵
```

The firewalld service is disabled.

5

Close the console window.

END OF STEPS

3.20 To set the default umask to 0027

3.20.1 Purpose

To align with OS-hardening best practices, as defined by the Center for Information Security, or CIS, you can change the default login umask on an NSP component station to restrict file and directory access for non-root users.

Perform this procedure to set the default login umask on an NSP station to 0027.

3.20.2 Steps

1

Log in as the root user on the station.

2

Back up the following files to a secure location on a station outside the management network for safekeeping:

- /etc/bashrc

- /etc/profile
- /etc/login.defs

3

Enter the following:

```
# sed -i 's/^\([[:space:]]*\)\(umask\|UMASK\)[[:space:]][[:space:]]*
[0-9][0-9][0-9]/\1\2 027/'  /etc/bashrc /etc/profile /etc/login.defs ↵
```

4

Log out.

5

Log in as the root user.

6

Enter the following:

```
# umask ↵
```

The current umask value is displayed.

7

Verify that the umask value is 0027.

8

Close the console window.

End of steps

4 Configuring NSP security

4.1 Overview

4.1.1 Purpose

This chapter describes fundamental NSP system security elements, and includes important information that you must consider as you deploy an NSP system or component.

For additional NSP security information such as post-deployment configuration, see the *NSP Security Hardening Guide* or the *NSP System Administrator Guide*.

4.1.2 Contents

NSP security introduction

4.2 NSP user accounts

4.2.1 NSP RHEL user

An NSP component installation creates a local ‘nsp’ RHEL user group and an ‘nsp’ user in the group that owns the local NSP component processes. The nsp user has administrative control over NSP maintenance and deployment functions.

The nsp user home directory is the NSP installation base directory, /opt/nsp. The initial nsp password is randomly generated, and must be changed by the root user during the initial login attempt.

Note: NSP software uninstallation does not remove the nsp user account, user group, or home directory.

Note: root-user privileges are required only for low-level operations such as deployment functions and support intervention.

4.2.2 NSP system administrator

A new NSP system has one user account for NSP access. The ‘admin’ user has full NSP UI and system administration privileges, and access to all NSP functions.

Note: Only the admin user, or a user with equivalent administrative privileges, has access to NSP administrative functions.

4.3 HTTPS Strict-Transport Security (HSTS)

4.3.1 Enabling HSTS for the NSP

CAUTION

Security Risk

Without HSTS, a browser that receives an invalid TLS certificate displays a warning that the user can circumvent. If HSTS is enabled, however, the browser blocks NSP access, and does not allow the user to circumvent the warning.

If HSTS is enabled, the system administrator must monitor and manage the TLS certificates carefully to ensure that, for example, a certificate is not expired, self-signed, or signed by an unknown CA.

HSTS is a mechanism that returns a header with specific instructions for any browser that attempts to connect using HTTP. The HSTS header instructs the browser to access the site using HTTPS instead of HTTP for all subsequent connections to the site or any child domain.

When HSTS is enabled, all NSP web interfaces are protected.

Note: HSTS is disabled by default in an NSP system, and can be enabled only during system installation; you cannot enable HSTS in a deployed NSP system.

4.3.2 HSTS TLS certificate management

In addition to ensuring that the current TLS certificate recognized by HSTS is not expired or nearing expiry, the same level of security must be applied to a certificate that replaces an expired certificate.

For example, if HSTS is enabled in the NSP, and you then change from a trusted root-CA-signed certificate to a self-signed certificate, browsers that attempt to connect to the NSP may prevent access because the new certificate is not trusted.

4.3.3 Configuring HSTS

You can enable HSTS during NSP system installation in the **hsts** section of the NSP configuration file.

Note: HSTS is disabled by default.

NFM-P HSTS configuration

You can enable HSTS during NFM-P installation using the samconfig utility on a main server.

NSP user authentication

4.4 Introduction

4.4.1 NSP user authentication modes

The NSP supports local user authentication, and authentication using external authentication agents such as RADIUS, LDAP/S, and TACACS+ servers. Windows Active Directory is also supported.

The NSP can be deployed in one of the following user authentication modes:

- 4.5 “OAUTH2 mode” (p. 100)—default; based on Keycloak open-source identity and access management, uses OAuth 2.0 protocol
- 4.6 “CAS mode” (p. 101)—deprecated; based on Central Authentication Service SSO solution and identity provider

An NSP system in either mode includes configurable mechanisms that guard against unwanted system access by maintaining strict control over repeated login attempts. See 4.5.2 “OAUTH2 login protection” (p. 101) and 4.6.2 “CAS login protection” (p. 102) for information.

OAUTH2 mode also supports the forwarding of user activity log events, as described in 4.5.3 “OAUTH2 user activity logging” (p. 101).

See 6.4 “Configuring Single-Sign-On (SSO)” (p. 175) for specific OAUTH2 and CAS configuration information.

i **Note:** You must use CAS authentication if the NSP deployment includes the WS-NOC.

Migrating from CAS to OAUTH2

Because CAS authentication is to be removed in a future NSP release, if you currently use CAS, it is strongly recommended that you migrate from CAS to OAUTH2. See 10.6 “To migrate from CAS to OAUTH2 NSP user authentication” (p. 317) for information.

4.4.2 Kafka user authentication

The NSP Kafka subsystem reports events to internal clients and systems, for example, the NFM-P, and to external clients, such as OSS subscribers. The internal and external Kafka communication is secured using TLS.

Kafka authentication for internal and external clients is configurable in the **nsp**—**modules**—**nspos**—**kafka** section of the NSP configuration file.

External Kafka client user authentication

If an NSP system is in OAUTH2 mode and uses separate interfaces for client and internal communication, you can enable NSP OAUTH2 user authentication for the external Kafka clients.

Internal Kafka client authentication

Kafka authentication for internal clients is based on two-way mTLS, rather than NSP user credentials.

An NFM-P shared-mode system supports internal Kafka client authentication. The authentication is configured using the samconfig utility on a main server, as described in the NFM-P deployment procedures. See “NFM-P installation” (p. 431) for mTLS configuration information.

4.5 OAUTH2 mode

4.5.1 NSP OAUTH2 user authentication

OAUTH2 authentication supports local and remote user management. The NSP Users and Security function is the interface for local user creation and administration.

NSP OAUTH2 mode does not use the NFM-P as an authentication source. In order to be authenticated by OAUTH2, the NFM-P users must undergo a migration to the NSP, as described in “Migrating from CAS to OAUTH2” (p. 99).

ℹ **Note:** Because CAS mode is deprecated, migrating from CAS to OAUTH2 is strongly recommended.

ℹ **Note:** The WS-NOC supports CAS, but does not support OAUTH2.

OAUTH2 username convention

To be valid for NSP access via OAUTH2, a local or remote authentication source username must consist of only lowercase characters, for example, johndoe. The convention is enforced as follows:

- You cannot create a local username that includes an uppercase character.
- OAUTH2 cannot authenticate a remote authentication username that includes uppercase characters; during NSP login, the username is converted to lowercase before authentication is attempted.

OAUTH2 and remote authentication

OAUTH2 supports the use of multiple LDAP, RADIUS, and TACACS+ remote authentication sources. OAUTH2 first attempts to verify a set of user credentials against the local user database. If the user account is not found, or lacks the correct credentials, OAUTH2 then tries to verify the credentials against the remote authentication sources that are configured.

ℹ **Note:** During a remote user login attempt, if the remote authentication source returns a user group that does not exist in the NSP:

- An LDAP user is granted restricted access to the NSP.
- A RADIUS or TACACS+ user is denied NSP access.

ℹ **Note:** OAUTH2 supports remote authentication servers that communicate using IPv4 or IPv6.

NSP OAUTH2 remote authentication has the following characteristics.

- You can define multiple servers for each type of remote authentication source, for example, two LDAP servers.
- RADIUS and TACACS+ authentication sources cannot be used in the same OAUTH2 deployment.

- LDAP immediately follows local user authentication in priority, and is always above RADIUS or TACACS+.
- RADIUS or TACACS+ is always the last authentication source to be tried.

4.5.2 OAUTH2 login protection

OAUTH2 provides functions for temporarily or permanently locking out users for login failures. Login failure management is configured during NSP deployment.

You cannot enable both temporary and permanent user lockout. If user lockout is to be enforced, only one mechanism can be active at any time.

Note: Temporary user lockout is enabled by default.

User login failures and permanent lockout

OAUTH2 can automatically lock out a user after a specified number of consecutive login failures. The user is prevented from logging in until an administrator unsuspends the user account. The user lockout applies only to local NSP users, and not to users defined in external authentication sources.

User login throttling and temporary lockout

A user that reaches a specified number of consecutive failed login attempts can be temporarily disabled for a specified wait interval. During the wait interval, further login attempts by the user are not processed. After the wait interval, OAUTH2 processes new login attempts by the user. If the user login attempts continue to fail, the login attempts are subsequently disabled for incrementally longer periods, up to a configurable maximum.

Note: Temporary lockout applies to local and external authentication source users.

4.5.3 OAUTH2 user activity logging

The NSP logs OAUTH2 activity for events such as user login, user logout, and system configuration changes, and can forward the log entries to a third-party processing system.

The log forwarding requires the following to be enabled in the NSP configuration file:

- "NSP Platform - Logging and Monitoring" installation option
- one option in the **nsp**—**modules**—**logging**—**forwarding**—**applicationLogs** section:
  - openSearch
  - splunk
  - syslog

4.6 CAS mode

4.6.1 NSP CAS user authentication

In an NSP system that uses CAS and includes the NFM-P, the NFM-P provides local user authentication and management. An NSP system that uses CAS can also delegate to one or more external authentication sources.

Note: CAS mode is deprecated, and is to be removed in a future NSP release. Migrating to OAUTH2 mode as described in 10.6 “To migrate from CAS to OAUTH2 NSP user authentication” (p. 317) is strongly recommended.

Note: The WS-NOC uses only CAS authentication.

CAS and remote authentication

In CAS mode, it is recommended to configure the NSP to delegate directly to one or more external authentication sources, rather than to an NFM-P system that in turn delegates to an external source.

Note: An NSP deployment that uses CAS and does not include the NFM-P requires the configuration of a remote authentication source such as LDAP, RADIUS, or TACACS+, or the NSP software deployment fails.

Note: In CAS mode, it is not recommended to configure external authentication sources in the NSP and also in the NFM-P, as redundant authentication requests may be sent and result in longer login times.

Table 4-1, “CAS authentication source comparison” (p. 101) describes the advantages and disadvantages of using various authentication sources with CAS.

Table 4-1 CAS authentication source comparison

Source	Advantages	Disadvantages
External source such as LDAP, RADIUS, TACACS+	The NSP continues to authenticate users in the event that the NFM-P is unavailable. NSP users can continue to access NSP functions while the NFM-P is unavailable.	You cannot configure an order of precedence for the authentication sources; the NSP determines the order during initialization.
NFM-P, using local user database or external authentication source	You can configure the order in which the NFM-P tries the external authentication sources.	If the NFM-P is down, the NSP is unable to authenticate any users.
	The NFM-P can assign a user to a default user group if an authentication source does not return a group name.	

4.6.2 CAS login protection

An NSP system deployed with CAS or OAUTH2 authentication provides mechanisms to guard against unwanted system access by maintaining strict control over repeated login attempts. The following CAS login authentication mechanisms are available.

User login failures

During NSP deployment, you can specify whether, and for how long, to lock out users that exceed a specified number of consecutive login failures.

User login throttling

User login throttling limits the number of failed login attempts, based on a username and client source IP address combination, to discourage password guessing and other unauthorized login attempts. Login throttling is enabled by default. You can configure the login failure rate and a lockout period for login attempts that exceed the failure rate.

After a failed login attempt, subsequent login attempts by the same user from the same source IP address during the login threshold period are blocked for the duration of the specified lockout period.

The login threshold period is defined by two parameters: The rate_seconds parameter defines a time interval, in seconds, and the rate_threshold parameter defines the number of allowed login attempts during the time interval.

The lockout_period parameter specifies the number of seconds to block login attempts by a user from the same address that exceeds the login threshold.

NSP Transport Layer Security (TLS)

4.7 Implementation and requirements

4.7.1 Introduction

The NSP uses Transport Layer Security, or TLS, to secure communication among system components, and for communication with clients and external systems. The TLS setting, whether enabled or disabled, must be the same on all NSP components.

The NSP supports the use of a custom TLS certificate that you provide, as described in 4.8.1 “Using a custom TLS certificate” (p. 105), or a certificate signed by a public root certification authority (CA). The NSP installation software includes a tool for automated TLS artifact generation and distribution, as described in 4.8.2 “Using a PKI server” (p. 105).

ℹ **Note:** If you intend to enable or disable TLS in an existing NSP system, you must stop, configure, and start the components in a specific order. To reduce the maintenance period and associated NSP system outage duration, see “Workflow: stop and start DR NSP clusters” in the *NSP System Administrator Guide*. The workflow describes how to perform a “graceful” shutdown and startup of DR NSP clusters and the ancillary NSP components in each data center.

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

ℹ **Note:** Auxiliary database security is independent of general NSP cluster or NFM-P internal system security, as described in 4.7.4 “Auxiliary database TLS” (p. 105).

4.7.2 NSP system TLS requirements

The private key and certificate files used in an NSP deployment must be in unencrypted PEM format.

If the NSP system uses advertised hostnames, the SAN field of the TLS certificate must include the hostnames advertised on the client and internal interfaces of the NSP cluster.

If an integrated NFM-P system uses hostnames, the NSP must use only DNS to resolve the hostnames.

See “NSP TLS configuration” (p. 108) for information about how to deploy TLS in an NSP system.

4.7.3 NFM-P TLS requirements

Custom certificate deployment is supported for an integrated NFM-P system that uses external IP addresses or hostnames.

If an NFM-P main server uses a hostname for communication with other components, the hostname specified using samconfig must be the hostname of the main server station, and must be the hostname that you include in the SAN field of the TLS certificate.

ℹ **Note:** A short hostname is valid only if DNS can resolve the hostname.

4.7.4 Auxiliary database TLS

The NSP and NFM-P system configurations each include a section specific to auxiliary database security that you must configure in advance of configuring TLS on an auxiliary database.

Note: The auxiliary database security setting in the NSP cluster, NFM-P main server, and auxiliary database configurations must match.

4.8 Configuring TLS for the NSP

4.8.1 Using a custom TLS certificate

You can generate and use a custom TLS certificate in an NSP deployment, as described in 4.9 “To generate custom TLS certificate files for the NSP” (p. 108).

A custom TLS certificate that you provide must meet the following criteria:

- be CA-signed
- be a 2048-bit RSA key
- include serverAuth in the ExtendedKeyUsages field

Note: After you redeploy an NSP cluster that uses a custom TLS certificate and has deleteOnUndeploy set to false in the nsp-config.yml file, you must reset the OpenSearch security configuration, as described in 4.12 “To reset the OpenSearch security configuration” (p. 119).

4.8.2 Using a PKI server

To reduce the complexity of configuring TLS in a new NSP system, or adding components to an existing system, you can use the Public Key Infrastructure server. A PKI server can create and sign certificates, if required, and distribute certificates to NSP components that are configured as requestors.

Note: The NSP messaging subsystems require a separate TLS certificate that is used internally. The certificate is generated and distributed automatically by the PKI server, which runs automatically during an NSP installation or upgrade. The separate internal certificate is required regardless of the external TLS configuration or deployment method.

In addition to simplifying TLS deployment, the benefits of using a PKI server include:

- no downtime when adding components, or during operations such as system conversion to DR
- configuration simplicity
- no need for operator knowledge of component interface addresses
- compatibility with current and future NSP releases
- ability to can generate a certificate, use an existing certificate, or use a certificate from a previous PKI-server instance, for example, if the original PKI server is no longer available

See 4.10 “To configure and enable a PKI server” (p. 113) for information about using a PKI server to deploy TLS.

Functional description

A PKI server is a standalone utility that implements TLS certificate signing requests (CSRs) from requesting NSP components. A PKI server is available on a station to which you extract an NSP software bundle.

Note: Only one PKI server instance is required for automated TLS deployment throughout an entire NSP system.

Note: Nokia recommends that you run the PKI server from the default installation location; optionally, you can run a copy of the utility on any host that is reachable by each requestor.

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

After receiving a CSR from a requestor, a PKI server uses the local 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 component that is not deployed in an NSP cluster, you must enable the PKI server in the component configuration. 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.
- but no keystore and truststore passwords are specified, the default password, which is available from technical support, is used.

4.8.3 Using intermediate signing certificates

A PKI server can act as an intermediate CA. The supported intermediate key type is a 4096-bit RSA key.

The required and recommended key extensions are the following:

- Required:
  - CA:TRUE
  - certificate sign key usage
  - chained pem file in which the NSP Intermediate cert is first in the chain, followed by the intermediate certificates, and ending with the root certificate
- Recommended:
  - path length = 0, which signifies that the PKI server can sign end-entity certificates only

For example:

Note: Required restrictions are in **boldface** type:

X509v3 Basic Constraints: critical

CA:TRUE, pathlen:0

X509v3 Key Usage: critical

Digital Signature, **Certificate Sign**, CRL Sign

4.8.4 TLS version and cipher support

By default, only TLS 1.2 is enabled. However, external systems such as OSS clients may use deprecated TLS versions. For NSP compatibility with such systems, you can enable older TLS versions.

Note: You must enable support for the deprecated TLS versions in a shared-mode NSP system that includes a Release 20 WS-NOC, if the **secure** parameter in the **nspos** section of the NSP configuration file is set to true.

The following parameter in the NSP configuration file enables or disables the support for the deprecated TLS versions:

- tlsv1ProtocolsEnabled

NFM-P 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.

NSP TLS configuration

4.9 To generate custom TLS certificate files for the NSP

4.9.1 Purpose

A TLS keystore and truststore are security artifacts that are required in order to enable TLS in an NSP system. This procedure describes how to manually generate a set of files that contain custom TLS artifacts for use in an NSP deployment.

Note: After you redeploy an NSP cluster that uses a custom TLS certificate and has deleteOnUndeploy set to false in the nsp-config.yml file, you must reset the OpenSearch security configuration, as described in 4.12 “To reset the OpenSearch security configuration” (p. 119).

The locations of the custom TLS files that the procedure generates are specified in the **tls** section of the nsp-config.yml file, as shown below:

```
tls
  customKey: private_server_key_location
  customCert: public_server_key_location
  customCaCert: public_CA_key_location
```

When you configure the NSP deployment, you must set the file locations in the **tls** section using the following values:

customKey—location of server private key file from Step 9

customCert—location of server.pem file from Step 7, or server-chained.pem from Step 10, if using intermediate CA

customCaCert—location of CA.pem file from Step 7

Note: An NSP keystore must be in JKS, or Java Key Store format.

Note: The NSP TLS artifacts are an OpenSSL RSA key and certificate. The NFM-P artifacts are JKS keystore and truststore files.
If you use self-signed TLS certificates, you must do one of the following:

- Submit separate NSP and NFMP CSRs with the appropriate artifacts
- Convert the CSR-signed artifacts to the appropriate format.

The Java keytool utility is included in each Java Development Kit, or JDK, and Java Runtime Environment, or JRE.

The keytool utility that you use must be from the Java version that the NSP uses. After an NSP component installation, the keytool utility is defined in the server PATH variable, so can be run from any location on an NSP cluster VM. If the NSP is not yet installed, ensure that the keytool utility on an alternative station that you use is from the supported Java version specified in the *NSP Planning Guide*.

Note: You require root user privileges.

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.

4.9.2 Steps

Generate TLS certificate

1

Log in as the root user on the NSP or NFM-P VM, or alternative station, as required.

2

Open a console window.

3

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

Note: If the NSP includes one or more NSP analytics servers, each analytics server must be represented in the certificate, as shown in this step.

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.

Note: You must enclose a password that contains a special character in single quotation marks; for example:

```
-keypass 'Mypa$$word' -storepass 'Mypa$$word'
```

```
# 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=DNS:DNS_name↵
```

where

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 common name or hostname of the server

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

DNS_name is the DNS-resolvable server hostname or FQDN

Note: Multiple server SAN entries are separated using semicolons; for example: san=DNS:*DNS_name_1*;DNS:*DNS_name_2*

4

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

5

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

Note: You must enclose a password that contains a special character in single quotation marks; for example:

```
-storepass 'Mypa$$word'
```

```
# 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

6

Generate a certificate signing request, or CSR.

1. Enter the following:

   ```
   # path/keytool -certreq -alias alias -keystore keystore_file -file
   CSR_file -storetype JKS -ext san=DNS:DNS_name -ext
   ExtendedKeyUsage=serverAuth,clientAuth ↵
   ```

   where

   alias is the keystore alias

   keystore_file is the keystore file generated in Step 3

   CSR_file is the name of the CSR file to generate

   DNS_name is the DNS-resolvable server hostname or FQDN

   Note: Multiple server SAN entries are separated using semicolons; for example,

   san=DNS:*DNS_name_1*;DNS:*DNS_name_2*

   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 a CSR file.

7

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

- server.pem—public server key
- CA.pem—public CA key

Generate NSP cluster TLS artifacts

8

Enter the following to convert the keystore to PKCS12 format:

```
# keytool -importkeystore -noprompt -srckeystore keystore_file
-destkeystore file_name.pkcs12 -deststoretype PKCS12 -deststorepass
storepass -destkeypass keypass -srcstorepass storepass -srckeypass
keypass -alias alias ↵
```

where

alias is the keystore alias

keystore_file is the keystore file generated in Step 3

file_name is the name of the new keystore file in PKCS12 format

keypass is the keystore password

storepass is the truststore password

9

Enter the following to extract the private key from the PKCS12 keystore to a file:

```
# openssl pkcs12 -in file_name.pkcs12 -passin pass:keypass -nodes
-nocerts -descert -out private_key.key ↵
```

where

file_name is the name of the keystore file in PKCS12 format

private_key is the name to assign to the private key file

10

If you are using an intermediate CA, enter the following to generate the chained server .pem file:

```
# cat server.pem ca-chained.pem > server-chained.pem ↵
```

Note: The certificate order is important; the server certificate must be first in the chain of certificates in the file in order for the NSP installer to read the certificates correctly.

11

If the NSP deployment does not include the NFM-P, go to Step 15.

Generate NFM-P TLS artifacts

12

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.

Note: You must enclose a password that contains a special character in single quotation marks; for example:

```
-storepass 'Mypa$$word'
```

```
# 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

13

Enter the following to import the certificate 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.

Note: You must enclose a password that contains a special character in single quotation marks; for example:

```
-storepass 'Mypa$$word'
```

```
# 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 keystore password

14

Perform the required TLS configuration described in “NFM-P TLS configuration” (p. 122).

15

Close the console window.

End of steps

4.10 To configure and enable a PKI server

4.10.1 Purpose

The following procedure describes:

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

A PKI server that you configure and start does the following.

1. Creates a local private root CA service.
2. Does one of the following:
   - imports a certificate from a file that you provide
   - generates a TLS certificate signed by the CA service
3. Polls for certificate requests
4. Distributes the certificate to requestors

Note: You require root user privileges to use the PKI server.

Note: *release-ID* in a file path has the following format:
R.r.p-rel.*version*
where
R.r.p is the NSP release, in the form *MAJOR.minor.patch*
version is a numeric value

4.10.2 Steps

1

By default, the PKI server utility is installed in the following location on an NSP deployer host:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/tools/pki

Note: You can run a PKI server from the default location, or from another station that is reachable by all requestors, as may be required when integrating a system such as the NFM-P or WS-NOC. To run the utility from a non-default location, you must first copy the pki-server file from the pki directory to the new location.

2

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

3

Open a console window.

4

If you need to use a backed-up PKI-server private key and public certificate from a previous PKI-server instance, copy the files to the directory that contains the pki-server utility. 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 utility, and the user that invokes the PKI server requires read access to the files.

5

Perform one of the following to start the PKI server.

a. Enter the following to use the default PKI server port:

```
# ./pki-server ↵
```

b. Enter the following to specify a port other than the default:

Note: If you specify a port other than the default, you must specify the non-default port number when you configure each requestor to use the PKI server.

```
# ./pki-server -port port ↵
```

where *port* is the port to use for receiving and responding to requests

6

If you are using files from a previous PKI-server instance, as described in Step 4, or have previously configured the root CA parameters for the PKI server, go to Step 19.

7

If this is the first time that the PKI server is run on the station, the following message and prompt are displayed:

```
********************************************************************************

No External Root CA detected on the filesystem.

********************************************************************************

Create new External Root CA Identity [y/n]?
```

8

Enter y ↵. The following prompt is displayed:

```
Organization Name (eg, company) []:
```

9

Enter your company name.

The following prompt is displayed:

```
Country Name (2 letter code) []:
```

10

Enter the two-letter ISO alpha-2 code for your country.

The following prompt is displayed:

```
State or Province Name (full name) []:
```

11

Enter your state or province name.

The following prompt is displayed:

```
Validity (days) [3650]:
```

12

Enter the length of time, in days, for which the TLS certificate is valid, or press ↵ to accept the default.

The following messages are displayed as the PKI server creates a local TLS root CA and begins to poll for TLS certificate requests:

```
date time Root CA generated successfully.
```

13

If this is the first time that the PKI server is run on the station, the following message and prompt are displayed. Otherwise, go to Step 19.

```
********************************************************************************
No Internal Root CA detected on the filesystem.
********************************************************************************
Creating new Internal Root CA Identity.
Organization Name (eg, company) []:
```

14

Enter your company name.

The following prompt is displayed:

```
Country Name (2 letter code) []:
```

15

Enter the two-letter ISO alpha-2 code for your country.

The following prompt is displayed:

```
State or Province Name (full name) []:
```

16

Enter your state or province name.

The following prompt is displayed:

```
Validity (days) [3650]:
```

17

Enter the length of time, in days, for which the TLS certificate is valid, or press ↵ to accept the default.

The following messages are displayed as the PKI server creates a local TLS root CA and begins to poll for TLS certificate requests:

```
date time Root CA generated successfully.
```

```
date time Using Root CA from disk, and serving requests on port port
```

18

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

19

When the PKI server receives a certificate request, 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]
```

20

The PKI server log is the pki-server.log file in the current directory. View the log to determine when the PKI server has distributed a certificate to each requestor.

21

When the PKI server has distributed a certificate to each requestor, enter Ctrl+C to stop the PKI server.

Note: The PKI server must continue to run until the installation of all products and NSP components that use the PKI server is complete. For example, if you are also installing the NFM-P, the PKI server must continue to run until the NFM-P configuration is complete.

22

Close the console window.

END OF STEPS

4.11 To migrate to a PKI server

4.11.1 Purpose

Use this procedure to migrate from manual TLS configuration to using a PKI server if the deprecated ROOT CA method, which involves generating ca.jks and ca-cert.pem files, has previously been used.

Note: This procedure is to be used if all components in the existing deployment were configured using the deprecated ROOT CA method.

Note: *release-ID* in a file path has the following format:

R.r.p-rel.*version*

where

R.r.p is the NSP release, in the form *MAJOR.minor.patch*

version is a numeric value

4.11.2 Steps

1

Copy over the existing ca.jks file, which is the ROOT CA keystore, and the ca-cert.pem file, which is the ROOT CA certificate.

2

Use the existing ca.jks file to create a new ca.key file. Execute the following commands:

Note: You must enclose a password that contains a special character in single quotation marks; for example:

```
-srcstorepass 'MyPa$$word' -deststorepass 'Mypa$$word'
```

```
path/keytool -importkeystore -srckeystore ca.jks -destkeystore
keystore.p12 -srcstorepass storePassword -deststorepass storePassword
-deststoretype PKCS12
```

```
openssl pkcs12 -in keystore.p12 -passin pass:keyPassword -nocerts
-nodes -out ca.key
```

where

path is the path to the keytool utility

storePassword is the password to access the contents of the keystore

keyPassword is the password that is used to access the private key stored within the keystore

3

Move the new ca.key file to the PKI server location. By default, this is the *NSP_installer_directory*/tools/pki directory, where *NSP_installer_directory* is the directory where the NSP software bundle was extracted.

4

Copy the existing ca-cert.pem file to the PKI server location.

5

Rename the ca-cert.pem file to ca.pem.

6

Perform one of the following.

a. Enter the following to use the default PKI server port:

```
# ./pki-server ↵
```

b. Enter the following to specify a port other than the default:

```
# ./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 to use the PKI server.

7

If this is the first time that the PKI server is run on the station, the following message and prompt are displayed. Otherwise, go to Step 12.

```
********************************************************************************
No Internal Root CA detected on the filesystem.
********************************************************************************
Creating new Internal Root CA Identity.
Organization Name (eg, company) []:
```

8

Enter your company name.

The following prompt is displayed:

```
Country Name (2 letter code) []:
```

9

Enter the two-letter ISO alpha-2 code for your country.

The following prompt is displayed:

```
State or Province Name (full name) []:
```

10

Enter your state or province name.

The following prompt is displayed:

```
Validity (days) [3650]:
```

11

Enter the length of time, in days, for which the TLS certificate is valid, or press ↵ to accept the default.

The following messages are displayed as the PKI server creates a local TLS root CA and begins to poll for TLS certificate requests:

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

The required ca.pem and ca.key files are created in the current working directory.

12

Copy the ca.pem and ca.key files to the following directory on the NSP cluster host:

/opt/nsp/NSP-CN-*release-ID*/tools/pki

13

Close the console window.

End of steps

4.12 To reset the OpenSearch security configuration

4.12.1 Purpose

If all of the following are true in an NSP cluster, you must reset the OpenSearch security configuration used by Log Viewer in the cluster.

- A custom TLS certificate is used.
- The deleteOnUndeploy parameter in the nsp-config.yml file is set to false.
- You have undeployed, and then redeployed, the NSP cluster.

4.12.2 Steps

1

Log in as the root user on the NSP cluster host.

2

Open a console window.

3

Enter the following:

```
# kubectl exec -it opensearch-cluster-master-0 -n nsp-psa-restricted
bash ↵
```

4

Enter the following:

```
# /usr/share/opensearch/plugins/opensearch-security/tools/securityadmin.sh -cacert /usr/share/opensearch/config/root-ca.pem -cert /usr/share/opensearch/config/kirk.pem -key /usr/share/opensearch/config/kirk-key.pem -cd /usr/share/opensearch/config/opensearch-security/ ↵
```

The OpenSearch security configuration is reset.

5

Close the console window.

End of steps

4.13 To enable TLS communication with the NFM-P using the NFM-P certificate

4.13.1 Purpose

Use this procedure to enable TLS communication with an NFM-P system that uses a non-custom TLS certificate.

4.13.2 Steps

1

Log in as the root user on an NFM-P main server station.

2

Enter the following:

```
# cd /opt/nsp/nfmp/server/nms/config/tls/keystore/samserver.keystore ↵
```

3

Enter the following to export the CA certificate from the NFM-P TLS keystore:

```
# /opt/nsp/os/jre/bin/keytool -exportcert -keystore samserver.keystore -alias alias -storepass password -rfc -file nfmp.pem ↵
```

where

alias is the certificate alias

password is the TLS keystore password

4

Copy the generated nfmp.pem file to a secure location for use in the NSP deployment.

END OF STEPS

4.14 To suppress security warnings in NSP browser sessions

4.14.1 Purpose

The following steps describe how to prevent the repeated display of security warnings in a browser that connects to the NSP 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 trusted by default.

4.14.2 Steps

1

Perform one of the following.

a. If you deployed TLS using the PKI server, transfer the ca.pem certificate file from the PKI server to each client host 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 host 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 OS.

Note: This method suppresses the display of NSP-related security warnings for all client browsers.

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 NSP opens without the display of security warnings.

END OF STEPS

NFM-P TLS configuration

4.15 To configure an NFM-P main server to request a PKI-server TLS certificate

4.15.1 Purpose

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.

4.15.2 Steps

1

Ensure that the PKI server is configured and running; see 4.10 “To configure and enable a PKI server” (p. 113).

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

2. Enter the following:

   ```
   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.

4. Enter the following to switch to the root user:

```
bash$ su ↵
```

5. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to display the nspOS service status:

```
# nspdctl status ↵
```

Information like the following is displayed.

```
Mode:      redundancy_mode
Role:      redundancy_role
DC-Role:   dc_role
DC-Name:   dc_name
Registry:  IP_address:port
State:     stopped
Uptime:    0s
SERVICE            STATUS
service_a          inactive
service_b          inactive
service_c          inactive
```

You must not proceed to the next step until all NSP services are stopped; if the State is not ‘stopped’, or the STATUS indicator of each listed service is not ‘inactive’, repeat this substep.

5

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

6

Enter the following:

```
<main> configure tls ↵
```

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

7

Enter the following:

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

8

Enter the following:

```
<main 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:

```
<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

10

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

11

Enter the following:

```
<main configure tls> alias alias ↵
```

where *alias* is the keystore alias to assign

12

Enter the following:

```
<main configure tls> pki-server server ↵
```

where *server* is the PKI server IP address or hostname

13

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

14

Enter the following:

```
<main configure tls> exit ↵
```

The prompt changes to `<main>`.

15

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

16

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

17

Enter the following to return to the nsp user:

```
# exit ↵
```

18

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.

19

Close the console window.

END OF STEPS

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

4.16.1 Purpose

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.

4.16.2 Steps

1

Ensure that the PKI server is configured and running; see 4.10 “To configure and enable a PKI server” (p. 113).

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:

```
# 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

4.17 To enable or disable TLS on an auxiliary database

4.17.1 Purpose

CAUTION

Service Outage

A change to the auxiliary database security settings requires a restart of each NFM-P main server and each NSP cluster, so is service-affecting.

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

CAUTION

Data Loss

No data is written to an auxiliary database unless the auxiliary database setting that defines whether TLS is enabled or disabled matches the auxiliary database security setting in the NSP and NFM-P.

You must ensure that the security setting on the auxiliary database cluster, NSP cluster, and NFM-P main server match.

The following steps describe how to enable or disable TLS for auxiliary database communication.

Note: TLS must be enabled in the NSP and NFM-P configurations before you can enable TLS on an auxiliary database.

Note: You require root user privileges on each auxiliary database station, each NFM-P main server station, and each NSP deployer host.

Note: You also require nsp user privileges on each NFM-P main server station.

Note: *release-ID* in a file path has the following format:

R.r.p-rel.*version*

where

R.r.p is the NSP release, in the form *MAJOR.minor.patch*

version is a numeric value

4.17.2 Steps

1

Start the PKI server, if the server is not running; perform 4.10 “To configure and enable a PKI server” (p. 113).

Note: The PKI server is required for internal system configuration purposes.

2

Log in as the root user on an auxiliary database station.

Note: In a DR NSP deployment, you must log in on a station in the primary auxiliary database cluster.

3

If you are configuring a standalone auxiliary database, go to Step 6.

Verify DR cluster-copy

4

If you are upgrading the first auxiliary database cluster in a DR NSP deployment, you must verify the success of the most recent copy-cluster operation, which synchronizes the database data between the redundant clusters.

Note: You must not proceed to the next step until the copy-cluster operation is complete and successful.

Perform one of the following periodically to check the copy-cluster status.

a. If the NFM-P is in a shared-mode NSP deployment, issue the following REST API call:

Note: In order to issue a REST API call, you require a REST token; see this tutorial on the Network Developer Portal for information.

```
GET https://address:8545/restconf/data/auxdb:/auxdb-agent
```

where *address* is the advertised address of the primary NSP cluster

The call returns a status of SUCCESS, as shown below, for a successfully completed copy-cluster operation:

```
<HashMap>
      <auxdb-agent>
         <name>nspos-auxdb-agent</name>
         <application-mode>ACTIVE</application-mode>
         <copy-cluster>
            <source-cluster>cluster_M</source-cluster>
            <target-cluster>cluster_N</target-cluster>
            <time-started>timestamp</time-started>
            <status>SUCCESS</status>
         </copy-cluster>
      </auxdb-agent>
</HashMap>
```

b. If the NFM-P is not in a shared-mode NSP deployment, enter the following as the root user on the primary main server station:

```
# /opt/nsp/os/nspd/nspdctl auxdb agent-status ↵
```

The command returns output like the following for a successfully completed copy-cluster operation:

```
DC-ROLE HOST APPLICATION-MODE
active leader 203.0.113.101 ACTIVE
Copy Cluster Details
SOURCE TARGET TIME-STARTED STATUS
cluster_1 cluster_2 2022-03-14T15:09:26.535Z SUCCESS
```

Stop database proxies

5

Perform the following steps on each auxiliary database station in each auxiliary database cluster to stop the database proxy.

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following:

   ```
   # systemctl stop nspos-auxdbproxy.service ↵
   ```
4. Enter the following:

   ```
   # systemctl status nspos-auxdbproxy ↵
   ```

   The proxy status is displayed; the proxy is stopped if the status includes the following:

   ```
   Active: inactive
   ```
5. You must ensure that the proxy is stopped.

   If the proxy is not stopped, repeat substep 4.

Configure TLS, standalone or primary cluster

6

Open the following file using a plain-text editor such as vi:

/opt/nsp/nfmp/auxdb/install/config/install.config

7

CAUTION

Service disruption

Changing a parameter in the auxiliary database install.config file can have serious consequences that include service disruption.

Do not change any parameter in the install.config file, other than the parameters described in the step, without guidance from technical support.

Edit the following lines in the file to read as shown below:

ℹ **Note:** TLS must be enabled in the NSP and NFM-P configurations before you can enable TLS on an auxiliary database.

```
secure=value
pki_server=server
pki_server_port=port
```

where

value is true or false, and indicates whether TLS is enabled

server is the PKI server IP address or hostname

port is the PKI server port number

8

Save and close the install.config file.

9

Enter the following:

```
# /opt/nsp/nfmp/auxdb/install/bin/auxdbAdmin.sh configureTLS ↵
```

The script prompts for the auxiliary database dba password.

10

Enter the required password.

The script configures TLS on the station.

11

Perform the following steps on each auxiliary database station in the cluster.

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following:

   ```
   # systemctl stop nspos-auxdbproxy.service ↵
   ```

4. Enter the following:

   ```
   # systemctl start nspos-auxdbproxy.service ↵
   ```

12

If you are configuring a standalone auxiliary database, go to Step 24.

Configure TLS, standby cluster

13

Log in as the root user on an auxiliary database station in the standby auxiliary database cluster.

14

Perform the following steps on each auxiliary database station in the cluster.

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following:

```
# systemctl stop nspos-auxdbproxy.service ↵
```

4. Enter the following:

```
# systemctl start nspos-auxdbproxy.service ↵
```

15

Enter the following:

```
# ./auxdbAdmin.sh start ↵
```

The auxiliary database cluster starts.

16

Open the following file using a plain-text editor such as vi:

/opt/nsp/nfmp/auxdb/install/config/install.config

17

CAUTION

Service disruption

Changing a parameter in the auxiliary database install.config file can have serious consequences that include service disruption.

Do not change any parameter in the install.config file, other than the parameters described in the step, without guidance from technical support.

Edit the following lines in the file to read as shown below:

```
secure=value
pki_server=server
pki_server_port=port
```

where

value is true or false, and indicates whether TLS is enabled

server is the PKI server IP address or hostname *port* is the PKI server port number

18

Save and close the install.config file.

19

Enter the following:

```
# /opt/nsp/nfmp/auxdb/install/bin/auxdbAdmin.sh configureTLS ↵
```

The script sequentially prompts for the root user password of each auxiliary database station.

20

Enter the required password at each prompt. The script configures TLS on the station.

21

Enter the following:

```
# ./auxdbAdmin.sh stop ↵
```

The auxiliary database cluster stops.

22

Perform the following steps on each auxiliary database station in the cluster.

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following:

   ```
   # systemctl stop nspos-auxdbproxy.service ↵
   ```

4. Enter the following:

   ```
   # systemctl start nspos-auxdbproxy.service ↵
   ```

Start database proxies

23

Perform the following steps on each auxiliary database station in each auxiliary database cluster to start the database proxy.

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following:

   ```
   # systemctl start nspos-auxdbproxy.service ↵
   ```

   The proxy starts.
4. Enter the following to verify that the proxy is started:

   ```
   # systemctl status nspos-auxdbproxy ↵
   ```

   The proxy status is displayed; the proxy is started if the status includes the following:

```
Active: active
```

Configure NFM-P

24

Perform Step 25 to Step 27 on each main server.

25

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.
6. Enter the following to switch to the root user:

   ```
   bash$ su ↵
   ```
7. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to display the nspOS service status:

   ```
   # nspdctl status ↵
   ```

   Information like the following is displayed.

   ```
   Mode:      redundancy_mode
   Role:      redundancy_role
   DC-Role:   dc_role
   DC-Name:   dc_name
   Registry:  IP_address:port
   State:     stopped
   Uptime:    0s
   SERVICE          STATUS
   service_a        inactive
   service_b        inactive
   service_c        inactive
   ```

You must not proceed to the next step until all NSP services are stopped; if the State is not ‘stopped’, or the STATUS indicator of each listed service is not ‘inactive’, repeat this substep.

26

When the main server is stopped, enable secure auxiliary database communication on the main server.

1. Enter the following:

   ```
   # samconfig -m main ↲
   ```

   The following is displayed:

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

2. Enter the following:

   ```
   <main> configure auxdb secure ↲
   ```

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

3. Enter the following:

   ```
   <main configure auxdb> exit ↲
   ```

   The prompt changes to `<main>`.

4. Enter the following:

   ```
   <main> apply ↲
   ```

   The configuration is applied.

5. Enter the following:

   ```
   <main> exit ↲
   ```

   The samconfig utility closes.

27

Start the main server.

1. Enter the following to switch back to the nsp user:

   ```
   # su ↲
   ```

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.

6. Close the console window.

Configure NSP clusters

28

If the NFM-P is not part of a shared-mode deployment that includes an NSP cluster, go to Step 37.

29

Log in as the root user on the NSP deployer host in the standalone or primary NSP cluster.

30

Open the following file using a plain-text editor such as vi:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

31

Locate the following section:

```
auxDb:
  secure: "value"
  ipList: "local_cluster_IPs"
  standbyIpList: "peer_cluster_IPs"
```

where *value* is true or false, and specifies whether TLS is enabled

32

Set the secure parameter to true or false, as required.

33

Save and close the nsp-config.yml file.

34

Enter the following to start the NSP cluster:

```
# /opt/nsp/NSP-CN-DEP-release-ID/bin/nspdeployerctl install --config
--deploy ↵
```

The NSP cluster starts, and the TLS configuration update is put into effect.

35

If the NSP is a DR deployment, perform Step 29 to Step 34 on the standby NSP cluster.

36

If no other components are to be deployed, stop the PKI server by entering Ctrl+C in the console window.

37

Close the open console windows.

End of steps

4.18 To disable TLS for NFM-P XML API clients

4.18.1 Purpose

The following steps describe how to disable TLS for all XML API clients in order to support OSS clients 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 access.

Note: Disabling TLS on the XML API disables the REST API, which can operate only when secured using TLS.

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

4.18.2 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 ↵
   ```
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.
5. Enter the following to switch to the root user:

   ```
   bash$ su ↵
   ```
6. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to display the nspOS service status:

   ```
   # nspdctl status ↵
   ```

   Information like the following is displayed.

   ```
   Mode:      redundancy_mode
   Role:      redundancy_role
   DC-Role:   dc_role
   DC-Name:   dc_name
   Registry:  IP_address:port
   State:     stopped
   Uptime:    0s
   SERVICE            STATUS
   service_a          inactive
   service_b          inactive
   service_c          inactive
   ```

   You must not proceed to the next step until all NSP services are stopped; if the State is not ‘stopped’, or the STATUS indicator of each listed service is not ‘inactive’, repeat this substep.

2

When the main servers are stopped, perform the following on each main server station.

1. Enter the following:

   ```
   # samconfig -m main ↵
   ```

   The following is displayed:

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

2. Enter the following:

   ```
   <main> configure oss no secure back ↵
   ```

   The prompt changes to `<main configure>`.

3. Enter the following:

   ```
   <main configure> back ↵
   ```

   The prompt changes to `<main>`.

4. Enter the following:

   ```
   <main> apply ↵
   ```

   The configuration is applied.

5. Enter the following:

   ```
   <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 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

Close the console window.

5

On each XML API client station, modify the URL that the client uses to reach the main server.

1. Change https: to http:.
2. Change the URL port value from 8443 to 8080.

END OF STEPS

4.19 To enable TLS for NFM-P XML API clients

4.19.1 Purpose

The following steps describe how to enable TLS for all XML API client communication with the NFM-P.

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

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

4.19.2 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.

5. Enter the following to switch to the root user:

   ```
   bash$ su ↵
   ```

6. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to display the nspOS service status:

   ```
   # nspdctl status ↵
   ```

   Information like the following is displayed.

   ```
   Mode:     redundancy_mode
   Role:     redundancy_role
   DC-Role:  dc_role
   DC-Name:  dc_name
   Registry: IP_address:port
   State:    stopped
   Uptime:   0s
   SERVICE           STATUS
   service_a         inactive
   service_b         inactive
   service_c         inactive
   ```

   You must not proceed to the next step until all NSP services are stopped; if the State is not ‘stopped’, or the STATUS indicator of each listed service is not ‘inactive’, repeat this substep.

2

When the main servers are stopped, perform the following on each main server station.

1. Enter the following:

   ```
   # samconfig -m main ↵
   ```

   The following is displayed:

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

2. Enter the following:

```
<main> configure oss secure back ↵
```

The prompt changes to `<main configure>`.

3. Enter the following:

```
<main configure> back ↵
```

The prompt changes to `<main>`.

4. Enter the following:

```
<main> apply ↵
```

The configuration is applied.

5. Enter the following:

```
<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 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 a 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

Part II: NSP system deployment

Overview

Purpose

This part of the *NSP Installation and Upgrade Guide* describes the NSP deployment environment, and provides information about performing various NSP system deployment operations.

For information about deploying additional NSP components, see Part III: “NSP component deployment”.

Contents

5 NSP deployment basics

5.1 Overview

5.1.1 Purpose

This chapter describes the container-based NSP environment and fundamental NSP deployment considerations. Also included is information about upgrading the deployment environment.

The following contain important information about the initial platform setup in advance of deploying the NSP container environment:

- *NSP Planning Guide*—platform hardware recommendations and deployment scaling guidelines
- Part I: "Getting started"—platform configuration, for example, preparing disk partitions, installing the RHEL OS, and implementing platform security

5.1.2 Contents

NSP system elements

5.2 Introduction

5.2.1 nspOS resource base

The nspOS, which is the common resource base of an NSP system, is deployed in an NSP cluster of one or more VMs in the Kubernetes container environment. A disaster-recovery, or DR, deployment, consists of matching NSP clusters in geographically separate data centers. A DR deployment is also called a geo-redundant deployment.

Some NSP components are not deployed in the NSP cluster, as described in Part III: “NSP component deployment”.

5.2.2 Time synchronization

CAUTION

Service Degradation

Some components, for example, members of an etcd cluster, fail to trust data integrity in the presence of a time difference. Failing to closely synchronize the system clocks among components complicates troubleshooting and may cause a service outage.

Ensure that you use only the time service described in this section to synchronize the NSP components.

The system clocks of the NSP components must always be closely synchronized. The RHEL chronyd service is the mandatory time-synchronization mechanism that you must engage on each NSP component during deployment.

Note: Only one time-synchronization mechanism can be active in an NSP system. Before you enable chronyd on an NSP component, you must ensure that no other time-synchronization mechanism, for example, the VMware Tools synchronization utility, is enabled.

5.3 Containerized NSP cluster

5.3.1 Introduction

The system elements described in the following topics are common to all NSP deployments.

You can use a disk image to instantiate NSP components and functions as VMs, as described in 2.2.2 “NSP disk-image deployment” (p. 28).

Note: The NSP RHEL OS image deployment steps in a procedure are specific to a RHEL KVM environment; however, alternative virtualization environments are supported, as described in the *NSP Planning Guide*.

To deploy an NSP RHEL OS image in an environment other than KVM, you must observe the *NSP Planning Guide* requirements for the environment, and perform the deployment as directed in the virtualization product documentation.

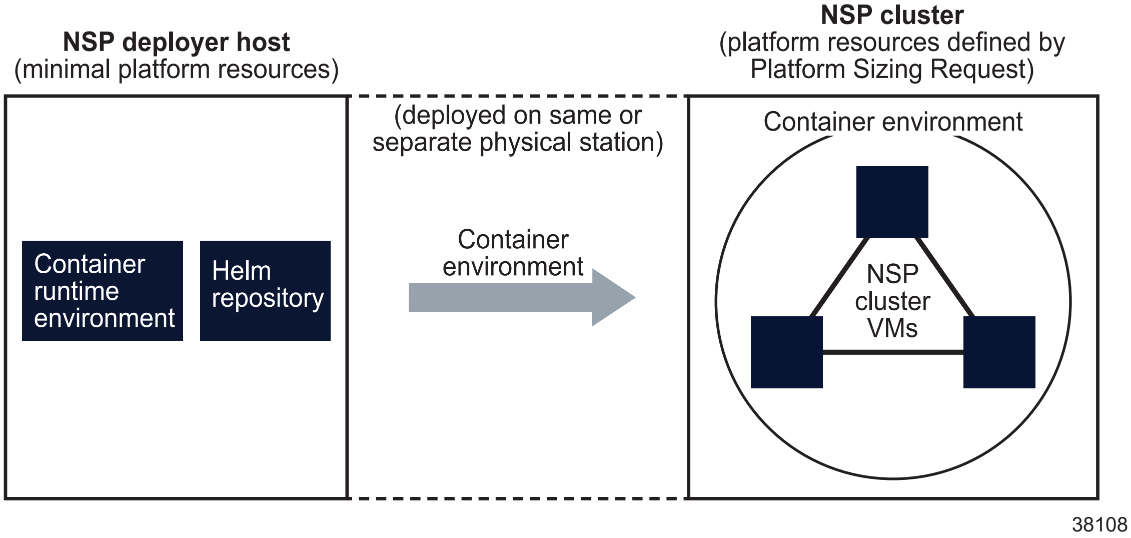
The main elements of an NSP system are the following:

- NSP deployer host—small; deploys containerization environment for NSP cluster; one NSP deployer host is required in each data center of a DR deployment
- NSP cluster VMs—large; host the main NSP functions, and components such as MDM

The NSP deployer host and NSP cluster VMs can be hosted on one physical station, or on separate stations. Figure 5-1, “NSP deployer host and NSP cluster” (p. 149) shows a standalone deployment on one physical station that hosts the NSP deployer host and NSP cluster VMs. An actual deployment may require multiple host stations.

Note: Communication between the NSP deployer host and the NSP cluster VMs is IPv4-only.

Figure 5-1 NSP deployer host and NSP cluster


NSP deployer host
(minimal platform resources)
NSP cluster
(platform resources defined by Platform Sizing Request)
(deployed on same or separate physical station)
Container runtime environment
Helm repository
Container environment
Container environment
NSP cluster VMs
38108

Resource allocation

The host stations in an NSP deployment require sufficient resources to support the specifications in your NSP Platform Sizing Request. The response to your Platform Sizing Request specifies the minimum platform resources to support your deployment.

See the *NSP Planning Guide* for information about platform sizing and the required resources for your deployment.

Note: In a DR NSP deployment, each NSP cluster must have the same number of NSP cluster VMs, and the same number of MDM instances.

5.3.2 NSP host station

An NSP host station hosts one or more NSP VMs. For example, an NSP deployer host and the NSP cluster can be installed on one NSP host station, or on separate stations.

5.3.3 NSP deployer host

CAUTION

Service degradation risk

The NSP deployer host is a crucial element of an NSP cluster deployment that must remain reachable by each NSP cluster VM after the initial deployment; otherwise, cluster recovery in the event of a failure may be compromised.

You must ensure that the NSP deployer host remains operational and reachable by the NSP cluster VMs at all times.

The NSP deployer host holds the required container image repository and Helm repository, and pushes a containerization environment for the NSP cluster.

The NSP deployer host requires the following resources; see the *NSP Planning Guide* for more information:

- CPUs—4
- RAM—8 GBytes
- disk capacity—250 GBytes

5.3.4 NSP cluster VMs

The NSP software runs on the NSP cluster VMs, and is load-balanced among the VMs, depending on the deployment configuration.

The resources required for the NSP cluster VMs are defined in the response to your Platform Sizing Request.

Note: The storage assigned to the NSP cluster VMs requires a specific minimum read/write throughput; see the *NSP Planning Guide* for the minimum required IOPS throughput for trial and live deployments.

If the NSP cluster includes more VMs than are named in the label profile, you must create a label for each additional VM before you can deploy the NSP cluster.

Note: You can deploy one MDM instance per NSP cluster VM. For example, a three-node NSP cluster can have up to three MDM instances. Warm -standby replica pods provide fault tolerance.

NSP cluster host

The NSP cluster host is a specific NSP cluster VM from which NSP configuration operations are performed. The VM requires direct network access to the NSP deployer host.

Note: The NSP cluster host is functionally no different from the other VMs in an NSP cluster; the VM is merely the designated cluster member for performing cluster and software management actions. The designation helps to prevent operator confusion, and simplifies the logging of maintenance actions.

NSP deployment infrastructure

5.4 Kubernetes deployment environment

5.4.1 Introduction

The NSP software can be deployed only in a supported version of Kubernetes environment. An NSP software bundle includes the latest supported version as of the NSP release date; an NSP system installation uses the bundled Kubernetes version.

An NSP system may be compatible with a Kubernetes version that is released after the NSP deployment. In such a case, you can upgrade the Kubernetes deployment environment without upgrading the NSP software, as described in 5.4.2 “Upgrading Kubernetes” (p. 152).

5.4.2 Upgrading Kubernetes

An NSP system upgrade typically includes an upgrade of the Kubernetes deployment environment. Each NSP system upgrade procedure has a link to 5.5 “To upgrade the NSP Kubernetes environment” (p. 153), which describes the upgrade process for a standalone or DR NSP deployment.

Supported upgrade schemes

A Kubernetes upgrade must be version-sequential, which means that you cannot upgrade directly from version A to version C and skip version B; you must first upgrade from version A to version B, and only then can you upgrade to version C.

Rather than performing a series of sequential Kubernetes upgrades, you can choose to uninstall your current Kubernetes environment and then install the new version.

Note: Performing a series of sequential upgrades preserves the NSP cluster data in the Kubernetes etcd database, while uninstalling Kubernetes deletes the etcd data.

Off-cycle upgrades

After an NSP installation or upgrade, if a new Kubernetes version is made available, you can choose to perform an “off-cycle” Kubenetes upgrade to the new version without upgrading the NSP software, if the NSP release supports the new Kubernetes version. See the *Host Environment Compatibility Reference for NSP and CLM* for information about the supported Kubernetes versions for various NSP releases.

See 5.5 “To upgrade the NSP Kubernetes environment” (p. 153) for the upgrade steps.

Time estimates

A Kubernetes upgrade and a Kubernetes re-installation take different amounts of time to complete, as shown below; the values are based on a four-node NSP cluster:

- upgrade—40 minutes
- re-installation—30 minutes

The time estimates show that re-installation may save considerable time if multiple sequential upgrades are required, especially in a DR deployment.

5.5 To upgrade the NSP Kubernetes environment

5.5.1 Purpose

Perform this procedure to upgrade the Kubernetes deployment environment in an NSP system. The procedure upgrades only the deployment infrastructure, and not the NSP software.

Note: You must upgrade Kubenetes in each NSP cluster of a DR deployment, as described in the procedure.

Note: *release-ID* in a file path has the following format:

R.*r*.*p*-rel.*version*

where

R.*r*.*p* is the NSP release, in the form *MAJOR*.*minor*.*patch*

version is a numeric value

5.5.2 Steps

Download Kubernetes upgrade bundle

1

Download the following from the NSP downloads page on the Nokia Support portal to a local station that is not part of the NSP deployment:

Note: The download takes considerable time; while the download is in progress, you may proceed to Step 2.

- NSP_K8S_DEPLOYER_*R*_*r*.tar.gz—software bundle for installing the registry and deploying the container environment
- associated .cksum file

where

*R*_*r* is the NSP release ID, in the form *Major*_*minor*

Verify NSP cluster readiness

2

Perform the following steps on each NSP cluster to verify that the cluster is fully operational.

1. Log in as the root user on the NSP cluster host.
2. Open a console window.
3. Enter the following to display the status of the NSP cluster nodes:

   ```
   # kubectl get nodes -A ↵
   ```

   The status of each cluster node is displayed.

   The NSP cluster is fully operational if the status of each node is Ready.

4. If any node is not in the Ready state, you must correct the condition; contact technical support for assistance, if required.

   Do not proceed to the next step until the issue is resolved.

5. Enter the following to display the NSP pod status:

   ```
   # kubectl get pods -A ↵
   ```

   The status of each pod is displayed.

   The NSP cluster is operational if the status of each pod is Running or Completed.

6. If any pod is not in the Running or Completed state, you must correct the condition; see the *NSP Troubleshooting Guide* for information about troubleshooting an errored pod.

Back up NSP databases

3

On the standalone NSP cluster, or the primary cluster in a DR deployment, perform “How do I back up the NSP cluster databases?” in the *NSP System Administrator Guide*.

ℹ **Note:** The backup takes considerable time; while the backup is in progress, you may proceed to Step 4.

Back up system configuration files

4

Perform the following on the NSP deployer host in each data center.

ℹ **Note:** In a DR deployment, you must clearly identify the source cluster of each set of backup files.

1. Back up the following Kubernetes registry certificate files in the following directory:

   /opt/nsp/nsp-registry/tls

   - nokia-nsp-registry.crt
   - nokia-nsp-registry.key

2. Back up the Kubernetes deployer configuration file:

   /opt/nsp/nsp-k8s-deployer-*release-ID*/config/k8s-deployer.yml

3. Back up the NSP deployer configuration file:

   /opt/nsp/NSP-CN-DEP-*release-ID*/config/nsp-deployer.yml

4. Back up the NSP configuration file:

   /opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/appliedConfigs/nspConfiguratorConfigs.zip

5. Copy the backed-up files to a separate station that is not part of the NSP deployment.

Verify checksum of downloaded file

5

It is strongly recommended that you verify the message digest of each NSP file that you download from the Nokia Support portal. The downloaded .cksum file contains checksums for comparison with the output of the RHEL md5sum, sha256sum, or sha512sum commands.

When the file download is complete, verify the file checksum.

1. Enter the following:

   ```
   # command file ↵
   ```

   where

   command is md5sum, sha256sum, or sha512sum

   file is the name of the downloaded file

   A file checksum is displayed.
2. Compare the checksum and the associated value in the .cksum file.
3. If the values do not match, the file download has failed. Retry the download, and then repeat Step 5.

Upgrade NSP registry

6

Perform Step 7 to Step 16 on the NSP deployer host in each data center, and then go to Step 17.

Note: In a DR deployment, you must perform the steps first on the NSP deployer host in the primary data center.

7

If the NSP deployer host is deployed in a VM created using an NSP RHEL OS disk image, perform 3.4 “To apply a RHEL update to an NSP image-based OS” (p. 67).

8

Copy the downloaded NSP_K8S_DEPLOYER_*R*_*r*.tar.gz file to the /opt/nsp directory.

9

Expand the software bundle file.

1. Enter the following:

   ```
   # cd /opt/nsp ↵
   ```
2. Enter the following:

   ```
   # tar -zxvf NSP_K8S_DEPLOYER_R_r.tar.gz ↵
   ```

   The bundle file is expanded, and the following directories are created:

   - /opt/nsp/nsp-registry-*new-release-ID*

- /opt/nsp/nsp-k8s-deployer-*new-release-ID*

3. After the file expansion completes successfully, enter the following to remove the bundle file, which is no longer required:

```
# rm -f NSP_K8S_DEPLOYER_R_r.tar.gz ↵
```

10

If you are not upgrading Kubernetes from the immediately previous version supported by the NSP, but from an earlier version, you must uninstall the Kubernetes software; otherwise, you can skip this step. See the *Host Environment Compatibility Guide for NSP and CLM* for information about Kubernetes version support.

Enter the following:

```
# /opt/nsp/nsp-registry-old-release-ID/bin/nspregistryctl uninstall ↵
```

The Kubernetes software is uninstalled.

11

Enter the following:

```
# cd /opt/nsp/nsp-registry-new-release-ID/bin ↵
```

12

Enter the following to perform the registry upgrade:

Note: During the registry upgrade, the registry may be temporarily unavailable. During such a period, an NSP pod that restarts on a new cluster node, or a pod that starts. is in the ImagePullBackOff state until the registry upgrade completes. Any such pods recover automatically after the upgrade, and no user intervention is required.

```
# ./nspregistryctl install ↵
```

13

If you did not perform Step 10 to uninstall Kubernetes, go to Step 16.

14

Enter the following to import the original Kubernetes images.

```
# /opt/nsp/NSP-CN-DEP-base_load/bin/nspdeployerctl import ↵
```

where *base_load* is the initially deployed version of the installed NSP release

15

If you have applied any NSP service pack since the original deployment of the installed release, you must import the Kubernetes images from the latest applied service pack.

Enter the following to import the Kubernetes images from the latest applied service pack.

```
# /opt/nsp/NSP-CN-DEP-latest_load/bin/nspdeployerctl import ↵
```

where *latest_load* is the version of the latest applied NSP service pack

Verify NSP cluster initialization

16

When the registry upgrade is complete, verify the cluster initialization.

1. Enter the following:

   ```
   # kubectl get nodes ↵
   ```

   NSP deployer node status information like the following is displayed:

   ```
   NAME         STATUS     ROLES                        AGE       VERSION
   node_name    status     control-plane,master         xxdnnh     version
   ```

2. Verify that *status* is Ready; do not proceed to the next step otherwise.
3. Enter the following periodically to monitor the NSP cluster initialization:

   ```
   # kubectl get pods -A ↵
   ```

   The status of each pod is displayed.

   The NSP cluster is fully operational when the status of each pod is Running or Completed.
4. If any pod fails to enter the Running or Completed state, correct the condition; see the *NSP Troubleshooting Guide* for information about troubleshooting an errored pod.

Prepare to upgrade NSP Kubernetes deployer

17

Perform Step 18 to Step 23 on the NSP deployer host in each cluster. and then go to Step 24.

Note: In a DR deployment, you can perform the steps on each NSP deployer host concurrently; the order is unimportant.

18

Copy the k8s-deployer.yml file backed up in Step 4 to the following directory:

/opt/nsp/nsp-k8s-deployer-*new-release-ID*/config

19

Enter the following:

```
# cd /opt/nsp/nsp-k8s-deployer-new-release-ID/bin ↵
```

20

Enter the following to create the new hosts.yml file:

```
# ./nspk8sctl config -c ↵
```

21

Enter the following to list the node entries in the new hosts.yml file:

```
# ./nspk8sctl config -l ↵
```

Output like the following example for a four-node cluster is displayed:

Note: If NAT is used in the cluster:

- The *access_ip* value is the public IP address of the cluster node.
- The *ip* value is the private IP address of the cluster node.
- The *ansible_host* value is the same value as *access_ip*

Note: If NAT is not used in the cluster:

- The *access_ip* value is the IP address of the cluster node.
- The *ip* value matches the *access_ip* value.
- The *ansible_host* value is the same value as *access_ip*

```
Existing cluster hosts configuration is:
all:
hosts:
node1:
ansible_host: 203.0.113.11
ip: ip
access_ip: access_ip
node2:
ansible_host: 203.0.113.12
ip: ip
access_ip: access_ip
node3:
ansible_host: 203.0.113.13
ip: ip
access_ip: access_ip
node4:
ansible_host: 203.0.113.14
ip: ip
access_ip: access_ip
```

22

Verify the IP addresses.

23

Enter the following to import the Kubernetes images to the repository:

```
.# ./nspk8sctl import ↵
```

The images are imported.

Stop and undeploy NSP cluster

24

Perform Step 25 to Step 27 on each NSP cluster, and then go to Step 28.

Note: In a DR deployment, you must perform the steps first on the standby cluster.

25

Perform the following steps on the NSP deployer host to preserve the existing cluster data.

1. Open the following file using a plain-text editor such as vi:

   /opt/nsp/NSP-CN-DEP-*old-release-ID*/NSP-CN-*old-release-ID*/config/nsp-config.yml
2. Edit the following line in the **platform** section, **kubernetes** subsection to read:

   ```
   deleteOnUndeploy:false
   ```
3. Save and close the file.

26

Enter the following on the NSP deployer host to undeploy the NSP cluster:

Note: If you are upgrading a standalone NSP system, or the primary NSP cluster in a DR deployment, this step marks the beginning of the network management outage associated with the upgrade.

Note: If the NSP cluster members do not have the required SSH key, you must include the --ask-pass argument in the command, as shown in the following example, and are subsequently prompted for the common root password of each cluster member:
nspdeployerctl --ask-pass --*option* --*option* ↵

```
# /opt/nsp/NSP-CN-DEP-old-release-ID/bin/nspdeployerctl uninstall
--undeploy --clean ↵
```

The NSP cluster is undeployed.

27

On the NSP cluster host, enter the following periodically to display the status of the Kubernetes system pods:

Note: You must not proceed to the next step until the output lists only the following:

- pods in kube-system namespace
- nsp-backup-storage pod

```
# kubectl get pods -A ↵
```

The pods are listed.

Deploy new NSP Kubernetes software

28

Perform Step 29 to the end of the procedure on each NSP cluster.

Note: In a DR deployment, you must perform the steps first on the primary cluster.

29

Perform one of the following.

a. Upgrade the Kubernetes software, which is recommended if the new version is only one version later than your current version.

   Note: The installation takes considerable time; during the process, each cluster node is cordoned, drained, upgraded, and uncordoned, one node at a time. The operation on each node may take 15 minutes or more.

   Enter the following on the NSP deployer host:

   ```
   # /opt/nsp/nsp-k8s-deployer-new-release-ID/bin/nspk8sctl install ↵
   ```

   The upgraded NSP Kubernetes environment is deployed.

b. Replace the current Kubernetes software with the new version.

   Note: Replacement is the recommended option if the new Kubernetes version is more than one version later than your current version.

   Note: The replacement takes approximately 30 minutes per cluster.

   1. Enter the following on the NSP deployer host:

      ```
      # cd /opt/nsp/nsp-k8s-deployer-old-release-ID/bin ↵
      ```

   2. Enter the following:

      ```
      # ./nspk8sctl uninstall ↵
      ```

      The existing Kubernetes software is uninstalled.

   3. Enter the following:

      ```
      # cd /opt/nsp/nsp-k8s-deployer-new-release-ID/bin ↵
      ```

   4. Enter the following:

      ```
      # ./nspk8sctl install ↵
      ```

   The new NSP Kubernetes environment is deployed.

30

Enter the following on the NSP cluster host periodically to display the status of the Kubernetes system pods:

Note: You must not proceed to the next step until each pod STATUS reads Running or Completed.

```
# kubectl get pods -A ↵
```

The pods are listed.

31

Enter the following periodically on the NSP cluster host to display the status of the NSP cluster nodes:

Note: You must not proceed to the next step until each node STATUS reads Ready.

```
# kubectl get nodes -o wide ↵
```

The NSP cluster nodes are listed, as shown in the following three-node cluster example:

```
NAME    STATUS   ROLES    AGE   VERSION    INTERNAL-IP   EXTERNAL-IP
node1   Ready    master   nd     version    int_IP    ext_IP
node2   Ready    master   nd    version    int_IP    ext_IP
node3   Ready    <none>   nd    version    int_IP        ext_IP
```

32

Update the NSP deployer configuration file.

1. Open the following file using a plain-text editor such as vi:

   /opt/nsp/NSP-CN-DEP-*old-release-ID*/config/nsp-deployer.yml
2. Edit the following line to read:

   ```
   hosts: "/opt/nsp/nsp-k8s-deployer-new-release-ID/config/hosts.yml"
   ```
3. Save and close the file.

Disable pod security policy

33

If your NSP deployment is at Release 23.4 and has a Kubernetes version newer than the version initially shipped with NSP Release 23.4, you must disable the pod security policy.

1. Open the following file on the NSP deployer host using a plain-text editor such as vi:

   /opt/nsp/NSP-CN-DEP-*latest_load*/NSP-CN-*latest_load*/config/nsp-config.yml

   where *latest_load* is the ID of the latest applied NSP service pack
2. Edit the following line in the **nsp** section, **podSecurityPolicies** subsection to read:

   ```
       enabled: false
   ```
3. Save and close the file.

Redeploy NSP software

34

Enter the following on the NSP deployer host:

```
# cd /opt/nsp/NSP-CN-DEP-new-release-ID/bin ↵
```

35

Enter the following:

```
# ./nspdeployerctl install --config --deploy ↵
```

The NSP starts.

Verify NSP initialization

36

On the NSP cluster host, monitor and validate the NSP cluster initialization.

ℹ **Note:** You must not proceed to the next step until each NSP pod is operational.

1. Enter the following every few minutes:

   ```
   # kubectl get pods -A ↵
   ```

   The status of each NSP cluster pod is listed; all pods are running when the displayed STATUS value is Running or Completed.

   The nsp deployer log file is /var/log/nspdeployerctl.log.

2. If the Network Operations Analytics - Baseline Analytics installation option is enabled, ensure that the following pods are listed; otherwise, see the *NSP Troubleshooting Guide* for information about troubleshooting an errored pod:

   Note: The output for a non-HA deployment is shown below; an HA cluster has three sets of three baseline pods, three rta-ignite pods, and two spark-operator pods.

   - analytics-rtanalytics-tomcat
   - baseline-anomaly-detector-*n*-exec-1
   - baseline-trainer-*n*-exec-1
   - baseline-window-evaluator-*n*-exec-1
   - rta-anomaly-detector-app-driver
   - rta-ignite-0
   - rta-trainer-app-driver
   - rta-windower-app-driver
   - spark-operator-*m*-*n*

3. If any pod fails to enter the Running or Completed state, see the *NSP Troubleshooting Guide* for information about troubleshooting an errored pod.

37

Enter the following on the NSP cluster host to display the status of the NSP cluster members:

ℹ **Note:** You must not proceed to the next step until each node is operational.

```
# kubectl get nodes ↵
```

The status of each node is listed; all nodes are operational when the displayed STATUS value is Ready.

The NSP Kubernetes deployer log file is /var/log/nspk8sctl.log.

Verify upgraded NSP cluster operation

38

Use a browser to open the NSP cluster URL.

39

Verify the following.

- In a DR deployment, if you specify the standby cluster address, the browser is redirected to the primary cluster address.
- The NSP sign-in page opens.
- The NSP UI opens after you sign in.

40

As required, use the NSP to monitor device discovery and to check network management functions.

Note: You do not need to perform the step on the standby NSP cluster.

Note: If you are upgrading Kubenetes in a standalone NSP cluster, or the primary NSP cluster in a DR deployment, the completed NSP cluster initialization marks the end of the network management outage.

Purge Kubernetes image files

41

Note: You must perform this and the following step only after you verify that the NSP system is operationally stable and that an upgrade rollback is not required.

Enter the following on the NSP deployer host:

```
# cd /opt/nsp/nsp-k8s-deployer-new-release-ID/bin ↵
```

42

Enter the following on the NSP deployer host:

```
# ./nspk8sctl purge-registry -e ↵
```

The images are purged.

43

Close the open console windows.

End of steps

IP version support

5.6 Introduction

5.6.1 Using IPv4 and IPv6

The NSP supports IPv4 or IPv6 communication with external clients, and internally among NSP components, in single- and multiple-interface deployments. The managed NEs can communicate with the NSP using IPv4, IPv6, or both concurrently.

Some restrictions may apply in a multi-interface deployment; see 5.8.4 “NSP cluster multi-interface configuration” (p. 165) for information.

i **Note:** The use of compressed IPv6 addresses, for example, 2001:E7A3::6502:0DA8, is fully supported.

5.7 Addressing requirements

5.7.1 Client and internal addressing

The client and internal networks must be in the same IP family: IPv4 or IPv6. NSP functions communicate internally and externally using only one protocol version.

i **Note:** Only IPv4 is supported for communication between an NSP deployer host and an NSP cluster.

5.7.2 Mediation addressing

Concurrent IPv4 and IPv6 NE mediation is supported using separate interfaces, or using one interface that supports both protocols.

5.7.3 IP addressing in shared-mode deployments

The IP version support in a shared-mode deployment varies, depending on which components or products are integrated, as described below.

NFM-P

The NFM-P fully supports IPv6 for mediation and client communication; integration with an IPv6 NSP system has no special requirements.

WS-NOC

The WS-NOC supports only IPv4 communication, so can be integrated only with an NSP system that uses IPv4 in the client and internal networks.

Using multiple NSP interfaces

5.8 Multi-interface configuration

5.8.1 Introduction

For greater security, you can configure multiple network interfaces to segregate the different types of NSP traffic.

When the NSP uses only one network for all communication, the NSP client traffic shares the same network as the NE mediation traffic and the internal communication between NSP components. Such a configuration may pose a considerable security risk.

You can segregate the NSP client, mediation, and internal traffic by configuring the NSP to use interfaces in separate networks for each traffic type.

Note: If you are deploying the NSP using multiple interfaces, the NSP deployer host must connect to the NSP cluster using the internal interface address specified in the NSP configuration file.

5.8.2 Traffic isolation

The multi-interface implementation isolates different traffic types to one or more of the following networks:

- client—for GUI, OSS, and other such northbound clients; for example, browser-based clients, REST clients, and Kafka subscribers.
- mediation—for direct communication with managed NEs
- internal—for communication such as the following:
  - traffic between NSP cluster members
  - communication with other NSP components or systems such as the VSR-NRC, NFM-P, and NSP analytics servers
  - traffic related to NSP DR functions such as data replication and keepalive messaging between data centers

Using separate networks enables you to apply additional security policies. For example, the NSP PostgreSQL service is an internal service only, and the only legitimate clients are NSP components, and not northbound browser or API clients. To help secure the PostgreSQL service from unintended access, you could apply a firewall rule to block the PostgreSQL port on the northbound client interface.

5.8.3 System conversion to multi-interface

You can convert an existing NSP system from a single-interface deployment to a multi-interface deployment, as described in 10.7 “Workflow for NSP system conversion to multi-interface” (p. 323).

5.8.4 NSP cluster multi-interface configuration

The **platform** section of the NSP configuration file has the following parameters for configuring multiple interfaces; see the descriptive text in the configuration file for more information:

Note: You must specify the *client_address* value, which is used as the default for any optional address parameter that you do not configure.

Note: If the client network uses IPv6, you must specify the NSP cluster hostname as the *client_address* value.

```
advertisedAddress: "client_address"

clusterHost: “cluster_host_address”

mediationAdvertisedAddress: "IPv4_mediation_address"

mediationAdvertisedAddressIpv6: "IPv6_mediation_address"

internalAdvertisedAddress: "internal_cluster_address"
```

where

client_address is the public IPv4 address or hostname that is advertised to clients

cluster_host_address is the IPv4 address of a host with access to the Kubernetes cluster for management operations; typically cluster node1

internal_cluster_address is the optional IPv4 or IPv6 address for internal NSP communication

IPv4_mediation_address is the optional IPv4 address for NE management traffic

IPv6_mediation_addressIpv6 is the optional IPv6 address for NE management traffic

5.8.5 Multi-interface configuration for RPM-based components

If an NSP cluster is configured to use a separate internal interface, you must specify the internal interface address as the NSP cluster address in the configuration of other NSP components.

Note: The WS-NOC is an exception; you must specify the NSP client address as the NSP cluster address in the WS-NOC configuration, regardless of whether the internal interface is used by other components.

Centralized logging

5.9 Introduction

5.9.1 NSP logging functions

The NSP includes centralized functions for logging NSP application and user activity. By default, the following are enabled:

- NSP and NFM-P user-activity log forwarding to the Kafka messaging subsystem
- NSP application-log forwarding to OpenSearch

“NSP logging and monitoring” in the *NSP System Administrator Guide* describes using OpenSearch and NSP Logviewer.

In order to enable one or more NSP centralized logging functions, the following NSP Installation Option must be enabled:

NSP Platform - Logging and Monitoring

Additional logging options

You can also configure the NSP to forward the following:

- application log records to Splunk servers
- NSP and NFM-P user-activity records to a remote syslog server
- NSP application logs and NFM-P server logs to a remote syslog server
- NSP application logs to a remote Elasticsearch server

ℹ **Note:** You can specify separate syslog servers for application and user activity log forwarding, as described in 5.13.1 “Description” (p. 169) and 5.16 “User activity log forwarding to syslog servers” (p. 170).

ℹ **Note:** The forwarding of NSP application logs and NFM-P server logs to a syslog server is supported over a TLS-secured or non-secure connection.

5.10 NSP application log forwarding to OpenSearch

5.10.1 Description

By default, the NSP is configured to forward NSP application logs to the internal OpenSearch engine, which makes the information available in an OpenSearch Dashboards view available from the NSP Log Viewer.

NSP application log forwarding to OpenSearch is configurable in the **nsp**—**modules**—**logging**—**forwarding**—**applicationLogs**—**opensearch** section of the NSP configuration file.

ℹ **Note:** If OAUTH2 user authentication is enabled, access to the NSP OpenSearch-Dashboards requires NSP user credentials.

5.11 NSP application log forwarding to Elasticsearch

5.11.1 Description

NSP application log forwarding to a remote Elasticsearch server is disabled by default. To enable NSP application-log forwarding to an Elasticsearch server, you configure the parameters in the **nsp**—**modules**—**logging**—**forwarding**—**applicationLogs**—**elasticsearch** section of the NSP configuration file.

5.11.2 Activation and security

In order to activate Elasticsearch application-log forwarding, you must copy the required TLS certificate files from the Elasticsearch server to the following location on the NSP deployer host:

/opt/nsp/NSP-CN-DEP-*release*-I*D*/NSP-CN-*release-ID*/tls/fluent

If mTLS is enabled on the internal NSP interface, the following TLS files are required for the mutual authentication:

- root CA certificate
- client certificate
- client key

If basic TLS is enabled on the internal NSP interface, the root CA certificate file is mandatory, and the client files are optional.

The files transferred to the NSP deployer host must be named as follows:

- root CA certificate file—ca_cert.pem
- client certificate file—client_cert.pem
- client key file—client.key

During initialization, the NSP imports the required TLS certificates to the local trust store.

5.12 NSP application log forwarding to Splunk

5.12.1 Description

An NSP cluster can forward application logs to a remote Splunk server using the Splunk HEC, or HTTP Event Collector. During NSP deployment, you can enable the log forwarding by configuring the Splunk forwarding parameters in the **nsp**—**modules**—**logging**—**forwarding**—**applicationLogs**—**splunk** section of the NSP configuration file.

When log forwarding to Splunk is enabled, the advertisedAddress parameter in the NSP cluster configuration file serves as a Splunk query criterion for the NSP application logs.

For example:

index="*k8s_log*" and nspHost="*cluster_address*"

where

cluster_address is the advertisedAddress in the NSP configuration file *k8s_log* is the Splunk HEC index

For information about setting up Splunk HEC, see the Splunk documentation.

5.13 NSP application log forwarding to syslog servers

5.13.1 Description

To enable NSP application-log forwarding to a syslog server, you must configure the parameters in the **nsp**—**modules**—**logging**—**forwarding**—**applicationLogs**—**syslog** section of the NSP configuration file.

Note: A syslog server address can be an IPv4 or IPv6 address, or a hostname or FQDN that the local NSP cluster and the NFM-P can resolve.

To secure the application-log forwarding, you must generate a TLS certificate on the syslog server and transfer the certificate to the **caCertPath** location that you specify in the **applicationLogs** section of the NSP configuration file. During initialization, the NSP imports the certificate to the local trust store.

“What is the syslog record format for NSP application log forwarding?” in the *NSP System Administrator Guide* describes the NSP application log record format.

5.14 NFM-P server log forwarding to syslog servers

5.14.1 Description

You can configure the NFM-P to forward the NFM-P server log entries in the EmsServer.log file to a remote syslog server.

To enable NFM-P server log forwarding to a remote syslog server, you must configure the **server-logs-to-remote-syslog** parameters using samconfig on each NFM-P main server.

Note: A syslog server address can be an IPv4 or IPv6 address, or a hostname or FQDN that the local NSP cluster and the NFM-P can resolve.

To secure the server log forwarding, you must generate a TLS certificate on the syslog server and transfer the certificate to the **ca-cert-path** location that you specify in the **server-logs-to-remote-syslog** section of samconfig. You must also set the **secure** parameter in the section to true. During initialization, the NFM-P imports the certificate to the local trust store.

“What is the syslog record format for NSP application log forwarding?” in the *NSP System Administrator Guide* describes the NFM-P server log record format.

Fault tolerance

Only a standalone or primary NFM-P main server can forward server logs. When the standby main server in a redundant deployment assumes the primary role after a main server activity switch or switchover, the new primary main server forwards the logs to the syslog server specified in the local main server configuration.

The greatest fault tolerance in a redundant deployment is achieved if you specify a different syslog server in each main server configuration.

5.15 NFM-P server log forwarding to OpenSearch

5.15.1 Description

In an NSP deployment that includes the NFM-P, you can configure the NFM-P to forward the NFM-P server log entries from the EmsServer.log and server_console.log files to the NSP OpenSearch instance.

i **Note:** The forwarding function is not available in an NFM-P system that is not integrated with an NSP cluster.

You can view the collected log entries in the Logviewer view of the NSP Opensearch Dashboards.

To enable NFM-P server log forwarding to NSP OpenSearch, you must configure the **server-logs-to-opensearch** parameters using samconfig on each NFM-P main server. Subsequently, the log entries from each NFM-P main server are pushed to the OpenSearch instance in each NSP cluster.

5.16 User activity log forwarding to syslog servers

5.16.1 Description

You enable the forwarding of NSP user activity logs to a remote syslog server by specifying the syslog server parameters in the **nsp**—**modules**—**logging**—**forwarding**—**activityLogs**—**syslog** section of the NSP configuration file.

i **Note:** A syslog server address can be an IPv4 or IPv6 address, or a hostname or FQDN that the local NSP cluster and the NFM-P can resolve.

In order to secure the forwarding of logs to a syslog server, you must generate a TLS certificate on the syslog server, and transfer the certificate to the **caCertPath** location that you specify in the **activityLogs** section of the NSP configuration file. During initialization, the NSP imports the certificate to the local TLS truststore.

NFM-P

To enable NFM-P user activity log forwarding, you must configure the **remote-syslog** parameters using samconfig on each NFM-P main server. In the section, you specify the server address and port, and the local path to the syslog TLS certificate, if the transfer is to be secure.

See “What is user activity log forwarding?” in the *NSP System Administrator Guide* for information about the NSP user activity syslog record format.

NFM-P fault tolerance

Only the standalone or primary NFM-P main server forwards NFM-P user activity logs; a main server in the role of standby does not forward logs to a syslog server. When the standby assumes the primary role after a main server activity switch or switchover, the new primary main server forwards the logs to the syslog server specified in the local main server configuration.

Note: The greatest fault tolerance in a redundant deployment is achieved if you specify a different syslog server in each main server configuration.

6 NSP software configuration

6.1 NSP configuration file

6.1.1 nsp-config.yml file format

CAUTION

Password Exposure

The NSP cluster configuration may include text-based truststore and keystore passwords that can be exposed.

To avoid exposing a password, you are strongly encouraged to store the NSP configuration file in a secure location outside the NSP management network.

In order to deploy an NSP cluster, you must specify system parameters, installation options, and additional components in the following NSP configuration file on the NSP deployer host:

/opt/nsp/NSP-CN--DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

The nsp-config.yml file has the following main sections:

- **platform**—defines the following for the mandatory *platform-baseServices* installation option:
  - deployment type, for example, standalone or DR
  - NSP IP addressing scheme
  - container environment
- **nsp**—defines the NSP deployment; includes the following subsections:
  - **deployment**—system scale, license, DR, backup configuration
  - **installationOptions**—NSP installation options to include in the deployment
  - **modules**—internal nspOs functions such as security and health monitoring, optional system functions
  - **integrations**—other systems to integrate, for example, NFM-P or WS-NOC
  - **sso**—SSO configuration for single sign-on system access

A section begins with a header and section label, followed by descriptive text and one or more parameter lines. An example section layout is shown below.

```
################################################################
## platform - Platform specific configs                       ##
################################################################
platform:
   ## parameter_1     - This is the parameter 1 description.
   ## parameter_2     - This is the parameter 2 description.
   ## parameter_3     - This is the parameter 3 description.
```

```
# parameter_1=
# parameter_2=
 parameter_3=true
```

To enable a parameter, delete the leading # symbol from the parameter line. In the example, only *parameter_3* is enabled and configured.

Note: You must preserve the lead spacing of each line. Ensure that you delete only the # symbol, and no spaces, from a parameter line.

Note: In the event of a discrepancy between information in a configuration file and the NSP documentation, or if the documentation fails to adequately describe a specific configuration, the configuration file information is to be followed and considered correct. Also, the *NSP Release Notice* describes configuration updates and corrections that are not captured in the core documentation.

6.1.2 Enabling installation options

The **installationOptions** section lists all available installation options. You enable the deployment of an option by removing the leading # character from the name and id lines of the option.

Note: *NSP Platform - Base Services* is mandatory and enabled by default.

In the example below, the following are enabled, and *NSP Platform - Pluggable Network Adaptation* is disabled:

- NSP Platform - Base Services (mandatory)
- NSP Platform - Logging and Monitoring
- Network Infrastructure Management - Basic Management

```
  installationOptions:
    - name: "NSP Platform - Base Services"
      id: platform-baseServices
    - name: "NSP Platform - Logging and Monitoring"
      id: platform-loggingMonitoring
#    - name: "NSP Platform - Pluggable Network Adaptation"
#      id: platform-pluggableNetworkAdaptation
    - name: "Network Infrastructure Management - Basic Management"
      id: networkInfrastructureManagement-basicManagement
```

6.2 Configuring database backups

6.2.1 Description

It is strongly recommended that you configure a database backup storage location that is not local to the NSP cluster. To do so, you must configure NFS using the following parameters in the **backups** section of the nsp-config.yml file:

```
nfs:
   server: "server"
   path: "path"
```

where

server is the NFS server IP address

path is the local path of the exported file system

6.3 Configuring nspOS security

6.3.1 Description

CAUTION

Service disruption

It is strongly recommended that the **secure** *parameter in the* **nspos** *section of nsp-config.yml is set to "true". Some features require a secure connection to function correctly.*

```
nspos:
   secure: true
```

Do not set the secure parameter to "false" unless you are certain that doing so is safe for your deployment.

Many NSP features including policies, alarms, NSP performance, database functions and system stability either require or are improved by a secure NSP.

6.4 Configuring Single-Sign-On (SSO)

6.4.1 Introduction

The NSP supports Single-Sign-On, or SSO access using CAS or OAUTH2 authentication, as described in 4.4.1 "NSP user authentication modes" (p. 99). Each supports multiple authentication sources of the same type or different types.

Note: In order to deploy an NSP system that uses CAS authentication, you must specify the NFM-P or another external authentication source in the NSP cluster configuration. If the primary_ip parameter in the **nfmp** section of the configuration specifies an NFM-P system, the

NFM-P system is used as an authentication source. If the primary_ip parameter is not configured, another external authentication source must be specified.

ℹ **Note:** You must configure only the parameters for the authentication mode that you specify using the authMode parameter.

ℹ **Note:** The descriptive text in the nsp-config.yml file may include additional configuration information.

ℹ **Note:** The following REST-session parameters in the **nsp** section of the nsp-config.yml file apply only to an NSP system that uses the CAS authentication mode, and are not to be configured otherwise:

- ttlInMins
- maxNumber

Configuring LDAPS or secure AD

TLS certificates for LDAPS communication must be copied to the /tls/ldap directory below the NSP installation directory.

CAS authentication does not require that an LDAPS certificate contains an IP address or hostname in the certificate SAN field. However, if a certificate does have an IP address or hostname, the same IP address or hostname must be specified in the nsp-config.yml file.

OAUTH2 requires that an LDAPS certificate contains the IP or hostname of the LDAP server in the certificate SAN field, and that the same IP or hostname is specified in the nsp-config.yml.

6.4.2 NSP SSO configuration parameters

Table 6-1, “SSO parameters, NSP configuration file” (p. 176) lists and describes the configuration parameters in the **sso** subsection of the **nsp** section. Some parameters are specific to CAS or OAUTH2, as indicated in the table.

The table also includes parameters for managing repeated failed login attempts, such as in brute-force attacks; see 4.6.2 “CAS login protection” (p. 102) or 4.5.2 “OAUTH2 login protection” (p. 101) for information about login protection.

See Appendix B, “NSP Single Sign-On configuration examples” for OAUTH2 and CAS remote authentication configuration examples.

Table 6-1 SSO parameters, NSP configuration file

Section and parameters	Description
The following parameters are common to CAS and OAUTH2 authentication.	
authMode	Authentication mode, which is one of the following: • oauth2—OAUTH2 user authentication • cas—CAS user authentication (deprecated) Default: oauth2

Table 6-1 SSO parameters, NSP configuration file (continued)

Section and parameters	Description
hsts	Whether to enable HSTS headers that tell client browsers to use only HTTPS and a valid CA certificate Default: false
session — CAS authentication parameters (deprecated) **Note: The parameters in this block are specific to CAS authentication, and are absent from the nsp-config.yml file in a new or upgraded deployment.**	
concurrentLimitsEnabled	Whether a maximum concurrent session limit is enabled Values: true/false
maxSessionsPerUser	Maximum number of concurrent sessions per user - does not apply to admin group Default: 10
maxSessionsForAdmin	Maximum number of concurrent sessions for users in admin group Default: 10
The following parameters are specific to OAUTH2 authentication. **Note: The sessionIdleTimeout value must be equal to or higher than the accessTokenLifeSpan value, or NSP client access may be compromised. The NSP verifies the parameter settings during deployment; however, the sessionIdleTimeout value is configurable after installation using NSP Users and Security, so care must be taken to set the value appropriately.**	
sessionIdleTimeout	Number of minutes after which to terminate an idle GUI-client session Default: 60
accessTokenLifespan	Client access-token validity duration, in minutes Default: 60
bruteForceDetection parameters **The parameters in this block are specific to OAUTH2 authentication.**	

Table 6-1 SSO parameters, NSP configuration file (continued)

Section and parameters		Description
	enabled	Whether to enable brute-force protection Default: true
	permanentLockout	Whether to enable permanent user lockout after the maxLoginFailures number of login failures Default: false
	maxLoginFailures	Number of allowed login failures before temporary or permanent lockout Default: 5
	waitIncrement	Temporary lockout time, in seconds, after maxLoginFailures failed login attempts reached Default: 60
	quickCheck	Number of milliseconds during which two consecutive login failures enable lockout period defined by minQuickWait parameter Default: 1000
	minQuickWait	Lockout duration, in seconds, triggered by quickCheck violation Default = 60
	maxWait	Maximum temporary lockout duration, in minutes Default: 15
	failureResetTime	Number of hours after which to reset the login-failure counts Default: 12
nfmp — NFM-P authentication parameters **The parameters in this block are common to CAS and OAUTH2 authentication.**		
enabled		Whether NFM-P is to perform user authentication Default: true if using CAS and deployment includes NFM-P; false otherwise
realms		NFM-P realm list **Note:** The realm parameters are defunct , and are not to be configured.
	realm	NFM-P authentication realm name; first realm must be named “sam” Default: sam
	display_name	Realm name to display in NSP UI Default: NFM-P 1
ldap — CAS LDAP parameters **The parameters in this block are specific to CAS authentication.**		
enabled		Whether LDAP is to be used for authentication Default: false
servers		List of LDAP servers; specify a server using the parameters below

Table 6-1 SSO parameters, NSP configuration file (continued)

Section and parameters		Description	
	type	LDAP server type; valid values are: • AD • ANONYMOUS • AUTHENTICATED **Note:** The AD and ANONYMOUS types do not allow the use of group search filters, so a user must belong to only the group specified by groupBaseDn. The AUTHENTICATED type requires bind credentials for LDAP querying, and allows the use of groupSearch filters.	
	url	LDAP server URL with IP address or hostname and port Default: none	
	security	Type of LDAP server security Values: SSL/STARTTLS/NONE	
	timeout	Timeout period, in seconds, for receiving an authentication response Default: 10	
	userBaseDn	User base dn value	
	userFilter	Filter criteria for username	
	groupBaseDn	The DN that contains the applicable NSP groups. **Note:** Used for further refining the groups returned by the server	
	groupSearch	Custom group search options **Note:** Can also be used for custom searches or further group filtering	
		filter	Group search filter criteria; ,must resolve to only one group for NSP authorization Default: none
		attributeId	Group attribute that identifies the NSP group name Default: none **Note:** In most cases, CN is adequate
	bind	LDAP bind credentials for authenticated access only	
		dn	User with authority to bind to LDAP server Default: none
		credential	Password of bind user **Note:** The password must be enclosed in double quotation marks. Default: none

Table 6-1 SSO parameters, NSP configuration file (continued)

Section and parameters		Description
minPoolSize		Minimum pool size Default: 0
maxPoolSize		Maximum pool size Default: 10
useEntryResolver		Whether an entry resolver is to be used for extracting additional user information Default: false
principalAtrributes		
	username	Optional username attribute
	first_name	Optional username attribute
	last_name	Optional username attribute
	email	Optional username attribute
ldap — OAUTH2 LDAP parameters **The parameters in this block are specific to OAUTH2 authentication.**		
enabled		Whether LDAP is to be used for authentication Default: false
servers		List of LDAP servers; specify a server using the parameters below

Table 6-1 SSO parameters, NSP configuration file (continued)

Section and parameters		Description	
	type	LDAP server type; valid values are: • AD • AUTHENTICATED	
	name	LDAP server name; text string	
	url	LDAP server URL with IP address or hostname and port, for example: ldap://203.0.113.172:389 Default: none	
	priority	LDAP server priority, 0 is highest Default: 0	
	usernameLdapAttribute	LDAP attribute to map to OAUTH2 username	
	rdnLdapAttribute	LDAP attribute to use as rdn for typical user dn, typically cn	
	uuidLdapAttribute	LDAP attribute that uniquely identifies LDAP objects	
	userObjectClasses	Comma-separated list of user objectClasses	
	customUserLdapFilter	Additional filter for user searches	
	searchScope	Scope of user search in userDn, typically 1	
	security	LDAP server security type; valid values are: • SSL • None	
	timeout	Timeout period for receiving LDAP server response, in milliseconds Default: 5000	
	userDn	DN of LDAP tree in which to find users	
	userFilter	User filter criteria	
	groupDn	DN of LDAP tree in which to find groups	
	groupNameLdapAttribute	LDAP attribute to map to user group	
	groupsLdapFilter	Groups filter criteria	
	groupObjectClasses	Comma-separated list of objectClasses for groups	
	groupMembershipLdapAttribute	Group attribute for user search	
	groupMembershipUserLdapAttribute	Username attribute in group membership	
	groupMemberOfLdapAttribute	User attribute that indicates group membership, usually memberOf	
	bind	LDAP bind credentials; for AUTHENTICATED server type only	
		dn	Bind user DN
		credential	Bind user credential

Table 6-1 SSO parameters, NSP configuration file (continued)

Section and parameters	Description
radius — RADIUS parameters **The parameters in this block are common to CAS and OAUTH2 authentication, with noted exceptions.**	
enabled	Whether RADIUS is to be used for authentication Default: none
address	**CAS**—comma-separated list of RADIUS-server IP addresses or hostnames **OAUTH2**—comma-separated list of colon-separated RADIUS-server IP addresses or hostnames and ports; for example: 203.0.113.150:1812,radius-server-a:1812 Default: none
secret	**CAS**—comma-separated list of shared server secrets enclosed in double quotation marks; for example: "*secret1*,*secret2*" CAS requires a separate secret entry for each RADIUS server in the configuration **OAUTH2**—one shared server secret, used for each RADIUS server in the configuration Default: none
protocol	Protocol to use—PAP or CHAP Default: none
retries	Maximum number of attempts to reach server Default: 3
timeout	**CAS**—timeout, in seconds, for RADIUS-server connection attempts Default: 60 **OAUTH2**—timeout, in milliseconds, for RADIUS-server connection attempts Default: 5000
failoverOnException (**CAS only**)	Whether second server is tried if first server fails with exception Default: none
failoverOnRejection (**CAS only**)	Whether second server is tried if first server fails with rejection Default: none
authenticationPort (**CAS only**)	RADIUS port Default: 1812
vendorId	Vendor ID for VSA search Default: 123
roleVsaId	VSA ID used to identify group Default: 3

Table 6-1 SSO parameters, NSP configuration file (continued)

Section and parameters	Description
mfa (**CAS only**)	Whether multi-factor authentication, or MFA, is enabled **Note:** MFA is always enabled in OAUTH2 RADIUS. Default: false
nasId	ID of the RADIUS Network Access Server (optional)
nasIp	IP address of the RADIUS Network Access Server (optional)
nasIpv6	IPv6 address of the RADIUS Network Access Server (optional)
tacacs — TACACS+ parameters **The parameters in this block are common to CAS and OAUTH2 authentication, with noted exceptions.**	
enabled	Whether TACACS+ authentication is to be used Default: none
address	**CAS**—comma-separated list of TACACS+-server IP addresses or hostnames **OAUTH2**—comma-separated list of colon-separated TACACS+-server IP addresses or hostnames and ports; for example: 203.0.113.167:1812,tacacs-server-a:1812 Default: none
secret	**CAS**—comma-separated list of shared server secrets enclosed in double quotation marks; for example: "*secret1*,*secret2*" CAS requires a separate secret entry for each TACACS+ server in the configuration **OAUTH2**—one shared server secret, used for each TACACS+ server in the configuration Default: none
protocol	Protocol to use Default: PAP
timeout	**CAS**—timeout, in seconds, for TACACS+-server connection attempts Default: 7 **OAUTH2**—timeout, in milliseconds, for TACACS+-server connection attempts Default: 7000
failoverOnException (**CAS only**)	Whether second server is tried if first server fails with exception Default: none
failoverOnRejection (**CAS only**)	Whether second server is tried if first server fails with rejection Default: none
authenticationPort (**CAS only**)	TACACS+ port Default: 49

Table 6-1 SSO parameters, NSP configuration file (continued)

Section and parameters	Description
defaultGroup	Default group to assign if no group is defined on remote server for user The group is assigned to a TACACS+ user if the vsaEnabled parameter is set to false. Default: none
vsaEnabled	Whether VSA search is enabled If set to true, a user group attribute is expected in the user authentication response/ Default: true
roleVsaId	Role used for VSA search Default: sam-security-group
vsaServiceId	VSA search service identifier Default: sam-app
throttling — user login throttling parameters **Note: The parameters in this block are specific to CAS authentication, and are absent from the nsp-config.yml file in a new or upgraded deployment.**	
enabled	Whether to enable login throttling Values: true/false
rateThreshold	Login failure threshold used for calculating login failure rate; see rate_seconds parameter Default: 3
rateSeconds	Number of seconds used for calculating login failure rate; exceeded if login attempt comes within rate_seconds/rate_ threshold seconds of a previous failed login attempt Default: 9
lockoutPeriod	Number of seconds after throttling threshold exceeded to wait before attempting to authenticate the same user and source address combination Default: 5
login_failure — user login failure parameters **Note: The parameters in this block are specific to CAS authentication, and are absent from the nsp-config.yml file in a new or upgraded deployment.**	
enabled	Whether to lock out users who have more consecutive login failures than specified by the threshold parameter Values: true/false
threshold	Maximum number of consecutive login failures before user lockout Default: 3
lockoutMinutes	Number of minutes to lock the user out after the threshold parameter value is exceeded Default: 1

6.5 Configuring LLDP link discovery

6.5.1 Description

The **nim**, or Network Infrastructure Management section specifies the method by which LLDP link discovery is accomplished.

In the MDM framework, NSP supports the LLDP-based discovery of physical links in the network topology. This discovery mechanism uses the MDM to read the LLDP neighbor information. NSP then adds the discovered links to the common store so that all applicable functions can access the link information. This process is controlled by the NSP network infrastructure management component by default, however, Original Service Fulfillment can be made to assume control by changing the value of the linkDiscovery parameter from “nim” to “sdn”.

Note: This function is supported only for the physical links with the Nearest Bridge transmission scope.

```
## nim                    - Network Infrastructure Management

     #    lldp                 - LLDP configuration

     #      linkDiscovery      - Link discovery type.  Valid values are:

     #                             "sdn" - indicates link discovery is
based on LLDP AMI v1

     #                             "nim" - indicates link discovery is
based on LLDP AMI v2 and onwards (default)
```

If upgrading from an NSP release earlier than 22.6, the linkDiscovery parameter is set to “sdn” by default. In order to change the value to “nim”, the following commands must be executed only when the lldpv2 adaptors are available or deployed for all managed devices:

```
./nspdeployerctl install --config

./nspdeployerctl install --deploy

kubectl delete pods `kubectl get pods -A | grep lldp-app | awk '{ print
$2 }'` -n $(kubectl get pods -A | awk '/lldp-app/ {print$1;exit}')`
```

6.6 Configuring SROS

6.6.1 Description

The SROS section of the NSP configuration file is used to integrate a containerized NSP system and an SROS VM such as the VSR-NRC in order to use the NSP PCE functions.

sros — required when integrating NSP with an SROS VM	
enabled	Whether path computation using SROS VM is enabled Default: false **Note:** When set to true, the SROS block of the hosts file must be configured.

partialSync		Whether partial sync functionality is enabled Default: true
ip		IP address of SROS VM
router_id		SROS VM router ID
matePort		The port used by SROS VM to communicate with other SROS VM in HA configuration Default: 4199
global		Whether global is enabled
pcep		Whether PCEP is enabled Default: false
rom		Whether rom is enabled
bgpls		Whether BGP LS is enabled Default: false
vms	ip	IP address of SROS VM
	router_id	SROS VM router ID
	v_id	SROS VM virtual ID; must be an integer value **NOTE:** The value must be the same for redundant VMs.
	mateAddress	The address used by SROS VM to communicate with other SROS VM in HA configuration Default: the IP of the other SROS VM within the same vId cluster
	matePort	The port used by SROS VM to communicate with other SROS VM in HA configuration Default: 4199
	global	Whether global is enabled
	pcep	Whether PCEP is enabled Default: false
	rom	Whether rom is enabled
	bgpls	Whether BGP LS is enabled Default: false

6.6.2 Parameters affecting Original Service Fulfillment

When modifying the nsp-config.yml file, special attention should be paid to the following parameters if Original Service Fulfillment is to be part of your deployment:

- in the NFM-P block of the file, setting the selectiveSync enabled parameter to 'true' will effectively disable Original Service Fulfillment. It is strongly recommended, however, that this parameter be set to 'true' if the path control function is part of your deployment. The parameter is set to 'false' by default.

- In the NFM-P block of the file, the deployOriginalServiceFulfillment parameter can be set to ‘false’ in order to disable Original Service Fulfillment's sam plugin. This parameter is set to 'true' by default.

7 NSP system installation

7.1 Supported installation scenarios

7.1.1 Introduction

CAUTION

Service Disruption

An NSP system installation requires a thorough understanding of NSP system administration and platform requirements, and is supported only under the conditions described in this guide, the NSP Planning Guide, and the NSP 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 NSP professional services to assess the requirements of your NSP deployment, and for information about the upgrade service, which you are strongly recommended to engage for any type of deployment.

The following scenarios are supported for the deployment of a new NSP system:

- typical standalone or DR system installation described in 7.1.2 “Completely new system installation” (p. 189)
- migration of functions from a legacy system during NSP system installation; see 7.1.3 “Legacy nspOS migration” (p. 190)

7.1.2 Completely new system installation

7.2 “Workflow for NSP system installation” (p. 190) provides a comprehensive view of the installation activities for advance planning purposes, and includes links to NSP system installation procedures.

Licensing

Your NSP system requires a license. It is recommended that you contact Nokia early in the planning process to obtain the required license for your deployment.

DR system installation

7.4 “To install the NSP” (p. 193) describes the installation of one NSP cluster. To install a DR NSP system, you must perform the procedure once in each data center, as described in 7.2 “Workflow for NSP system installation” (p. 190).

Note: In a DR deployment, the first data center in which you perform 7.4 “To install the NSP” (p. 193) is designated the primary data center and hosts the active nspOs instance.

7.1.3 Legacy nspOS migration

As part of a new NSP system installation, you can transfer the nspOS functions of a traditional RPM-based NSP system, or an independent NFM-P system, to the new NSP system. See 7.6 “To migrate from an independent NFM-P system to the NSP” (p. 217) for information.

7.2 Workflow for NSP system installation

7.2.1 Purpose

The following is the sequence of high-level actions that you must perform in order to install a standalone or DR NSP system.

7.2.2 Stages

1

Submit an NSP Platform Sizing Request to Nokia; if the NSP deployer host and cluster VMs are to be deployed on one station, ensure that you include the deployer host resources in your request.

2

If using physical hosts for the VMs, perform 7.3 “To provision the network bridge for NSP VMs” (p. 191) on each physical host to create a network bridge for KVM access to the guest VMs.

3

Commission the required stations for the NSP VMs according to the specifications in the response to your Platform Sizing Request.

4

Ensure that the RHEL chronyd time-synchronization service is running on each component, and that chronyd is actively tracking a central time source. See the RHEL documentation for information about using the chronyc command to view the chronyd synchronization status.

Note: NSP deployment is blocked if the chronyd service is not active.

5

Contact Nokia to obtain the required license for your deployment.

6

If you are using a custom TLS certificate for the deployment, perform 4.9 “To generate custom TLS certificate files for the NSP” (p. 108) to generate the required TLS files.

7

Install the NSP in the standalone or primary data center; perform 7.4 “To install the NSP” (p. 193).

8

In a DR deployment, install the NSP in the standby data center; perform 7.4 “To install the NSP” (p. 193).

9

If you are adding the NFM-P to the NSP system, perform 11.3 “To integrate the NSP and NFM-P” (p. 327).

7.3 To provision the network bridge for NSP VMs

7.3.1 Purpose

Perform the following steps on a physical host to create a network bridge for communication with the guest VMs.

Note: There is no requirement for the VM host station to be at the same RHEL OS release as the guest NSP VMs, which use RHEL 8. The configuration commands in the procedure are specific to RHEL 7, the predominantly deployed RHEL version in data centers that have not yet migrated to RHEL 8.

Note: It is strongly recommended that you perform the procedure using the local console or ILO interface. Using a local session ensures that the session remains active in the event that a misconfiguration or network disruption isolates the station.

Note: You require root user privileges on the station.

Note: Command lines use the # symbol to represent the RHEL CLI prompt for the root user. Do not type the leading # symbol when you enter a command.

7.3.2 Steps

1

Ensure that the RHEL firewalld, iptables, and netfilter configurations allow traffic to and from the network bridge; see the RHEL documentation for information.

2

If you are configuring the network bridge on a RHEL 8 station, perform the following steps.

1. See the RHEL 8 documentation for information about configuring a network bridge and assigning an interface to the bridge.
2. Go to Step 16.

3

Log in as the root user on the station.

4

Open a console window.

5

Enter the following sequence of commands:

```
chkconfig NetworkManager off
chkconfig network on
systemctl stop NetworkManager
systemctl start network
```

6

Open the following file using a plain-text editor such as vi:

/etc/sysconfig/network-scripts/ifcfg-*interface*

where *interface* is the physical network interface that the host is to use for connectivity as a bridge member, for example, eno1

7

Add the following line:

```
BRIDGE=bridge_name
```

where *bridge_name* is the name to assign to the bridge

8

Record the *bridge_name* value.

9

Save and close the file.

10

Create the following file using a plain-text editor such as vi:

/etc/sysconfig/network-scripts/ifcfg-*bridge_name*

where *bridge_name* is the network bridge name specified in Step 7

11

Enter the following as the file content:

```
TYPE=Bridge
BOOTPROTO=static
DEFROUTE=yes
DEVICE=bridge_name
ONBOOT=yes
IPADDR=n.n.n.n
```

```
PREFIX=mm
GATEWAY=g.g.g.g
DNS1=d.d.d.d
DOMAIN=domain
```

where

bridge_name is the network bridge name specified in Step 7

n.n.n.n is the IP address of *interface* specified in Step 6

mm is the *interface* subnet mask

g.g.g.g is the gateway IP address

d.d.d.d is a DNS IP address

domain is the DNS server FQDN

12

Save and close the ifcfg-*bridge_name* file.

13

Enter the following to instantiate the network bridge:

```
# brctl addbr bridge_name ↵
```

where *bridge_name* is the network bridge name

14

Enter the following to restart the network service:

```
# systemctl restart network ↵
```

15

Close the console window.

16

After you create the required VMs for the NSP deployment, verify the bridge connectivity between the host and the guest VMs.

END OF STEPS

7.4 To install the NSP

7.4.1 Purpose

Perform this procedure to deploy a new standalone or DR NSP system.

Note: To create a DR deployment, you must perform the procedure on the NSP cluster in each data center. The NSP cluster on which you first perform the procedure initializes as the primary cluster.

Note: You require root user privileges on the NSP deployer host, and on each VM that you create.

Note: *release-ID* in a file path has the following format:

R.r.p-rel.*version*

where

R.r.p is the NSP release, in the form *MAJOR.minor.patch*

version is a numeric value

Note: Command lines use the # symbol to represent the RHEL CLI prompt for the root user. Do not type the leading # symbol when you enter a command.

7.4.2 Steps

Create NSP deployer host VM

1

Download the following from the NSP downloads page on the Nokia Support portal:

Note: You must also download the .cksum file associated with each.

- NSP_K8S_DEPLOYER_*R_r*.tar.gz—bundle for installing the registry and deploying the container environment
- one of the following RHEL OS images for creating the NSP deployer host and NSP cluster VMs:
  - NSP_K8S_PLATFORM_RHEL8_*yy_mm*.qcow2
  - NSP_K8S_PLATFORM_RHEL8_*yy_mm*.ova
- NSP_DEPLOYER_*R_r*.tar.gz—bundle for installing the NSP application software

where

R_r is the NSP release ID, in the form *Major_minor*

yy_mm represents the year and month of issue

2

It is strongly recommended that you verify the message digest of each NSP image file or software bundle that you download from the Nokia Support portal. The download page includes checksums for comparison with the output of the RHEL md5sum, sha256sum, or sha512sum command.

To verify a file checksum, perform the following steps.

1. Enter the following:

   ```
   # command file ↵
   ```

   where

   command is md5sum, sha256sum, or sha512sum

   file is the name of the file to check

A file checksum is displayed.

2. Compare the checksum value and the value in the .cksum file.
3. If the values do not match, the file download has failed. Download a new copy of the file, and then repeat this step.

3

Log in as the root user on the station designated for the NSP deployer host VM.

4

Open a console window.

5

Perform one of the following to create the NSP deployer host VM.

Note: The NSP deployer host VM requires a hostname; you must change the default of ‘localhost’ to an actual hostname.

a. Deploy the downloaded NSP_K8S_PLATFORM_RHEL8_*yy_mm*.qcow2 disk image; perform Step 6 to Step 16 of 2.3 “To deploy an NSP RHEL qcow2 disk image” (p. 30).

b. Deploy the NSP_K8S_PLATFORM_RHEL8_*yy_mm*.ova disk image; see the documentation for your virtualization environment for information.

Note: For OVA-image deployment, it is strongly recommended that you mount the /opt directory on a separate hard disk that has sufficient capacity to allow for future expansion.

c. Manually install the RHEL OS and configure the disk partitions, as described in “Manual NSP RHEL OS installation” (p. 70) and Chapter 2, “NSP disk setup and partitioning”.

Configure NSP deployer host networking

6

Enter the following to open a console session on the NSP deployer host:

```
# virsh console deployer_host ↵
```

You are prompted for credentials.

7

Enter the following credentials:

- username—root
- password—*available from technical support*

A virtual serial console session opens on the deployer host VM.

8

Enter the following:

```
# ip a ↵
```

The available network interfaces are listed; information like the following is displayed for each:

```
if_n: if_name: LESSTHANBROADCAST,MULTICAST,UP,LOWER_UPGTRTHAN mtu 1500
qdisc mq state UP group default qlen 1000
    link/ether MAC_address
    inet IPv4_address/v4_netmask brd broadcast_address scope global
noprefixroute if_name
       valid_lft forever preferred_lft forever
    inet6 IPv6_address/v6_netmask scope link
       valid_lft forever preferred_lft forever
```

9

Record the *if_name* and *MAC_address* values of the interface that you intend to use.

10

Enter the following:

```
# nmcli con add con-name con_name ifname if_name type ethernet mac
MAC_address ↵
```

where

con_name is a connection name that you assign to the interface for ease of identification

if_name is the interface name recorded in Step 9

MAC_address is the MAC address recorded in Step 9

11

Enter the following:

```
# nmcli con mod con_name ipv4.addresses IP_address/netmask ↵
```

where

con_name is the connection name assigned in Step 10

IP_address is the IP address to assign to the interface

netmask is the subnet mask to assign

12

Enter the following:

```
# nmcli con mod con_name ipv4.method static ↵
```

13

Enter the following:

```
# nmcli con mod con_name ipv4.gateway gateway_IP ↵
```

gateway_IP is the gateway IP address to assign

14

Enter the following:

Note: You must specify a DNS name server. If DNS is not deployed, you must use a non-routable IP address as a nameserver entry.

Note: Any hostnames used in an NSP deployment must be resolved by a DNS server.

Note: An NSP deployment that uses IPv6 networking for client communication must use a hostname configuration.

```
# nmcli con mod con_name ipv4.dns nameserver_1,nameserver_2...
nameserver_n ↵
```

where *nameserver_1* to *nameserver_n* are the available DNS name servers

15

To optionally specify one or more DNS search domains, enter the following:

```
# nmcli con mod con_name ipv4.dns-search search_domains ↵
```

where *search_domains* is a comma-separated list of DNS search domains

16

Enter the following to reboot the VM:

```
# systemctl reboot ↵
```

Install NSP Kubernetes registry

17

Enter the following on the deployer host VM:

```
# mkdir /opt/nsp ↵
```

18

Copy the downloaded NSP_K8S_DEPLOYER_R_r.tar.gz bundle file to the following directory:

/opt/nsp

19

Enter the following:

```
# cd /opt/nsp ↵
```

20

Enter the following:

```
# tar xvf NSP_K8S_DEPLOYER_R_r.tar.gz ↵
```

where *R_r* is the NSP release ID, in the form *Major_minor*

The bundle file is expanded, and the following directories are created:

- /opt/nsp/nsp-k8s-deployer-*release-ID*
- /opt/nsp/nsp-registry-*release-ID*

21

Remove the bundle file to save disk space; enter the following:

```
# rm -f NSP_K8S_DEPLOYER_R_r.tar.gz ↵
```

The file is deleted.

22

Enter the following:

```
# cd nsp-registry-release-ID/bin ↵
```

23

Enter the following:

```
# ./nspregistryctl install ↵
```

The following prompt is displayed.

```
Enter a registry admin password:
```

24

Create a registry administrator password, and enter the password.

The following prompt is displayed.

```
Confirm the registry admin password:
```

25

Re-enter the password.

The registry installation begins, and messages like the following are displayed.

```
✔ New installation detected.
✔ Initialize system.
date time Copy container images ...
date time Install/update package [container-selinux] ...
✔ Installation of container-selinux has completed.
date time Install/update package [k3s-selinux] ...
✔ Installation of k3s-selinux has completed.
date time Setup required tools ...
✔ Initialization has completed.
date time Install k3s ...
date time Waiting for up to 10 minutes for k3s initialization ...
..............................................
✔ Installation of k3s has completed.
```

```
➜ Generate self-signed key and cert.
date time Registry TLS key file:
/opt/nsp/nsp-registry/tls/nokia-nsp-registry.key
date time Registry TLS cert file:
/opt/nsp/nsp-registry/tls/nokia-nsp-registry.crt
date time Install registry apps ...
date time Waiting for up to 10 minutes for registry services to be
ready ...
..........
✓ Registry apps installation is completed.
date time Generate artifacts ...
date time Apply artifacts ...
date time Setup registry.nsp.nokia.local certs ...
date time Setup a default project [nsp] ...
date time Setup a cron to regenerate the k3s certificate [nsp] ...
✓ Post configuration is completed.
✓ Installation has completed.
```

26

Enter the following periodically to display the status of the Kubernetes system pods:

ℹ **Note:** You must not proceed to the next step until each pod STATUS reads Running or Completed.

```
# kubectl get pods -A ↵
```

The pods are listed.

Create NSP cluster VMs

27

For each required NSP cluster VM, perform one of the following to create the VM.

ℹ **Note:** Each NSP cluster VM requires a hostname; you must change the default of 'localhost' to an actual hostname.

a. Deploy the downloaded NSP_K8S_PLATFORM_RHEL8_*yy_mm*.qcow2 disk image; perform Step 6 to Step 16 of 2.3 “To deploy an NSP RHEL qcow2 disk image” (p. 30).

b. Deploy the NSP_K8S_PLATFORM_RHEL8_*yy_mm*.ova disk image; see the documentation for your virtualization environment for information.

ℹ **Note:** For OVA-image deployment, it is strongly recommended that you mount the /opt directory on a separate hard disk that has sufficient capacity to allow for future expansion.

c. Manually install the RHEL OS and configure the disk partitions, as described in "Manual NSP RHEL OS installation" (p. 70) and Chapter 2, "NSP disk setup and partitioning".

28

Record the MAC address of each interface on each VM.

29

Perform Step 30 to Step 48 for each NSP cluster VM to configure the required interfaces.

Configure NSP cluster networking

30

Enter the following to open a console session on the VM:

```
# virsh console NSP_cluster_VM ↵
```

where *NSP_cluster_VM* is the VM name

You are prompted for credentials.

31

Enter the following credentials:

- username—root
- password—*available from technical support*

A virtual serial console session opens on the NSP cluster VM.

32

Enter the following:

```
# ip a ↵
```

The available network interfaces are listed; information like the following is displayed for each:

```
if_n: if_name: LESSTHANBROADCAST,MULTICAST,UP,LOWER_UPGTRTHAN mtu 1500
qdisc mq state UP group default qlen 1000
    link/ether MAC_address
    inet IPv4_address/v4_netmask brd broadcast_address scope global
noprefixroute if_name
       valid_lft forever preferred_lft forever
    inet6 IPv6_address/v6_netmask scope link
       valid_lft forever preferred_lft forever
```

33

Record the *if_name* and *MAC_address* values of the interfaces that you intend to use.

34

Enter the following for each interface:

```
# nmcli con add con-name con_name ifname if_name type ethernet mac
MAC_address ↵
```

where

con_name is a connection name that you assign to the interface for ease of identification; for example, ClientInterface or MediationInterface

if_name is the interface name recorded in Step 33

MAC_address is the MAC address recorded in Step 33

35

Enter the following for each interface:

```
# nmcli con mod con_name ipv4.addresses IP_address/netmask ↵
```

where

con_name is the connection name assigned in Step 34

IP_address is the IP address to assign to the interface

netmask is the subnet mask to assign

36

Enter the following for each interface:

```
# nmcli con mod con_name ipv4.method static ↵
```

37

Enter the following for each interface:

```
# nmcli con mod con_name ipv4.gateway gateway_IP ↵
```

gateway_IP is the gateway IP address to assign

Note: This command sets the default gateway on the primary interface and the gateways for all secondary interfaces.

38

Enter the following for all secondary interfaces:

```
# nmcli con mod con_name ipv4.never-default yes ↵
```

39

Enter the following for each interface:

Note: You must specify a DNS name server. If DNS is not deployed, you must use a non-routable IP address as a nameserver entry.

Note: Any hostnames used in an NSP deployment must be resolved by a DNS server.

Note: An NSP deployment that uses IPv6 networking for client communication must use a hostname configuration.

```
# nmcli con mod con_name ipv4.dns nameserver_1,nameserver_2...
nameserver_n ↵
```

where *nameserver_1* to *nameserver_n* are the available DNS name servers

40

To optionally specify one or more DNS search domains, enter the following for each interface:

```
# nmcli con mod con_name ipv4.dns-search search_domains ↵
```

where *search_domains* is a comma-separated list of DNS search domains

41

Open the following file with a plain-text editor such as vi:

/etc/sysctl.conf

42

Locate the following line:

```
vm.max_map_count=value
```

43

Edit the line to read as follows; if the line is not present, add the line to the end of the file:

```
vm.max_map_count=262144
```

44

Save and close the file.

45

If you are installing in a KVM environment, enter the following:

```
# mkdir /opt/nsp ↵
```

46

It is essential that the disk I/O on each VM in the NSP cluster meets the NSP specifications.

On each NSP cluster VM, perform the tests described in “Disk performance tests” in the *NSP Troubleshooting Guide*.

If any test fails, contact technical support for assistance.

47

Enter the following to reboot the NSP cluster VM:

```
# systemctl reboot ↵
```

48

Close the console session by pressing Ctrl+] (right bracket).

Deploy Kubernetes environment

49

Enter the following on the NSP deployer host

```
# cd /opt/nsp/nsp-k8s-deployer-release-ID/config ↵
```

50

Open the following file using a plain-text editor such as vi:

k8s-deployer.yml

51

Configure the parameters shown below for each NSP cluster VM; see the descriptive text at the head of the file for parameter information, and 13.9.2 “Hostname configuration requirements” (p. 379) for general configuration information.

Note: The nodeName value:

- can contain only ASCII alphanumeric and hyphen characters
- cannot include an uppercase character
- cannot begin or end with a hyphen
- cannot begin with a number
- cannot include an underscore
- must end with a number

```
- nodeName: node1
  nodeIp: 192.168.98.196
  accessIp: 135.228.8.196
```

52

Configure the following parameter, which specifies whether dual-stack NE management is enabled:

Note: Dual-stack NE management can function only when the network environment is appropriately configured, for example:

- Only valid, non-link-local static or DHCPv6-assigned addresses are used.
- A physical or virtual IPv6 subnet is configured for IPv6 communication with the NEs.

```
enable_dual_stack_networks: value
```

where *value* must be set to true if the cluster VMs support both IPv4 and IPv6 addressing

53

Save and close the file.

54

Create a backup copy of the updated k8s-deployer.yml file, and transfer the backup copy to a station that is separate from the NSP system, and preferably in a remote facility.

Note: The backup file is crucial in the event of an NSP deployer host failure, and must be copied to a separate station.

55

Enter the following:

```
# cd /opt/nsp/nsp-k8s-deployer-release-ID/bin ↵
```

56

Enter the following to create the cluster configuration:

```
# ./nspk8sctl config -c ↵
```

The following is displayed when the creation is complete:

```
✓ Cluster hosts configuration is created at:
/opt/nsp/nsp-k8s-deployer-release-ID/config/hosts.yml
```

57

Enter the following to import the Kubenetes container images to the registry:

```
# ./nspk8sctl import ↵
```

Messages like the following are displayed as the import proceeds:

```
✓ Pushing artifacts to registry (it takes a while) ...

date time Load container image from
[/opt/nsp/nsp-k8s-deployer-release-ID/artifact/nsp-k8s-R.r.0-rel.tar.
gz] ...

date time Push image [image_name] to registry.nsp.nokia.local/library
...

date time Push image [image_name] to registry.nsp.nokia.local/library
...

.

.

.

date time Push image [image_name] to registry.nsp.nokia.local/library
...
```

58

You must generate an SSH key for password-free NSP deployer host access to each NSP cluster VM.

Enter the following:

```
# ssh-keygen -N "" -f ~/.ssh/id_rsa -t rsa ↵
```

59

Enter the following for each NSP cluster VM to distribute the SSH key to the VM.

```
# ssh-copy-id -i ~/.ssh/id_rsa.pub root@address ↵
```

where *address* is the NSP cluster VM IP address

60

Enter the following:

```
.# ./nspk8sctl install ↵
```

The NSP Kubernetes environment is deployed.

61

The NSP cluster member named node1 is designated the NSP cluster host for future configuration activities; record the NSP cluster host IP address for future reference.

Check NSP cluster status

62

Open a console window on the NSP cluster host.

63

Enter the following periodically to display the status of the Kubernetes system pods:

Note: You must not proceed to the next step until each pod STATUS reads Running or Completed.

```
# kubectl get pods -A ↵
```

The pods are listed.

64

Enter the following periodically to display the status of the NSP cluster nodes:

Note: You must not proceed to the next step until each node STATUS reads Ready.

```
# kubectl get nodes -o wide ↵
```

The NSP cluster nodes are listed, as shown in the following three-node cluster example:

```
NAME    STATUS   ROLES    AGE   VERSION   INTERNAL-IP   EXTERNAL-IP
node1   Ready    master   nd     version   int_IP   ext_IP
node2   Ready    master   nd    version   int_IP   ext_IP
node3   Ready    <none>   nd    version   int_IP        ext_IP
```

Configure NSP software

65

Open a console window on the NSP deployer host.

66

Enter the following:

```
# cd /opt/nsp ↵
```

67

Enter the following:

```
# tar xvf NSP_DEPLOYER_R_r.tar.gz ↵
```

where *R_r* is the NSP release ID, in the form *Major_minor*

The bundle file is expanded, and the following directory is created:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*

68

Enter the following:

```
# rm -f NSP_DEPLOYER_R_r.tar.gz ↵
```

The bundle file is deleted.

69

Open the following file using a plain-text editor such as vi to specify the system parameters and enable the required installation options:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

Note: See 6.1.1 “nsp-config.yml file format” (p. 173) for configuration information.

Note: You must preserve the lead spacing of each line.

Note: The following REST-session parameters in the **nsp** section of the nsp-config.yml file apply only to an NSP system that uses CAS authentication, and are not to be configured otherwise:

- ttlInMins
- maxNumber

70

Configure the cluster addressing parameters in the **platform** section as shown below; you must specify the *client_address* value, which is used as the default for any optional address parameter that you do not configure:

ⓘ **Note:** If the client network uses IPv6, you must specify the NSP cluster hostname as the *client_address* value.

```
advertisedAddress: "client_address"
mediationAdvertisedAddress: "IPv4_mediation_address"
mediationAdvertisedAddressIpv6: "IPv6_mediation_address"
internalAdvertisedAddress: "internal_cluster_address"
clusterHost: "cluster_host_address"
```

where

client_address is the public IPv4 address or hostname that is advertised to clients

IPv4_mediation_address is the optional address for IPv4 NE management traffic

IPv6_mediation_address is the optional address for IPv6 NE management traffic

internal_cluster_address is the optional IPv4 or IPv6 address for internal NSP communication

cluster_host_address is the address of NSP cluster member node1, which is subsequently used for cluster management operations

71

Configure the remaining parameters in the **platform** section as shown below:

platform section, **docker** subsection:

```
repo: "registry.nsp.nokia.local/nsp/images"
pullPolicy: "IfNotPresent"
```

platform section, **helm** subsection:

```
repo: "oci://registry.nsp.nokia.local/nsp/charts"
timeout: "300"
```

72

If you are creating a multi-node cluster, perform the following steps.

1. Configure the following parameters in the **platform** section, **elb** subsection as shown below:

   ```
   elb:
     deploy: true
     virtualIpAddress: "client_VIP"
      mediationVirtualIpAddress: "IPv4_mediation_VIP"
      mediationVirtualIpAddressIpv6: "IPv6_mediation_VIP"
      internalVirtualIpAddress: "internal_VIP"
   ```

   where

   client_VIP is the virtual cluster address for client access

   IPv4_mediation_VIP is the virtual cluster address for IPv4 network mediation

   IPv6_mediation_VIP is the virtual cluster address for IPv6 network mediation *internal_VIP* is the virtual cluster address for internal communication

2. For each NSP cluster VM, add the following group of lines to the **elb** subsection under **hosts**:

```
- hostAddress: "client_IP"
  mediationHostAddress: "IPv4_mediation_IP"
  mediationHostAddressIpv6: "IPv6_mediation_IP"
  internalHostAddress: "internal_address"
```

where

client_IP is the address of the VM interface to the client network

IPv4_mediation_IP is the address of the VM interface to the IPv4 mediation network

IPv6_mediation_IP is the address of the VM interface to the IPv6 mediation network

internal_IP is the address of the VM interface to the internal network

ℹ **Note:** The deployer host requires access to the client network.

73

Configure the **type** parameter in the **deployment** section as shown below:

```
deployment:
    type: "deployment_type"
```

where *deployment_type* is one of the parameter options listed in the section

74

Configure the **tls** parameters in the **deployment** section as shown below:

ℹ **Note:** The customKey, customCert, and customCaCert parameters are required only if you are using custom TLS certificates.
See 4.9 “To generate custom TLS certificate files for the NSP” (p. 108) for information about configuring custom TLS certificates.

```
tls:
  truststorePass: "truststore_password"
  keystorePass: "keystore_password"
  customKey: private_server_key_location
  customCert: public_server_key_location
  customCaCert: public_CA_key_location
```

75

If the NSP deployment includes an auxiliary database and you are enabling TLS, set the **secure** parameter in the **auxdb** section to true.

76

If the NSP system is a DR deployment, configure the parameters in the **dr** section as shown below:

```
dr:
   dcName: "data_center"
   mode: "deployment_mode"
   peer: "peer_address"
   internalPeer: "peer_internal_address"
   peerDCName: "peer_data_center"
```

where

data_center is the unique alphanumeric name to assign to the cluster

deployment_mode is the case-sensitive deployment type, dr or standalone

peer_address is the address at which the peer data center is reachable over the client network

peer_internal_address is the address at which the peer data center is reachable over the internal network

peer_data_center is the unique alphanumeric name of the peer cluster

77

If you are integrating one or more existing systems or components with the NSP, configure the required parameters in the **integrations** section.

For example:

To integrate a standalone NFM-P system, you must configure the **nfmp** parameters in the section as shown below:

Note: When the section includes an NFM-P IP address, the NSP UI is accessible only when the NFM-P is operational.

Note: In the **client** section of samconfig on the NFM-P main servers, if the address for client access is set using the **hostname** parameter, the **primaryIp** and **standbyIp** values in the **nfmp** section of the NSP configuration file, nsp-config.yml, must be set to hostnames.
Likewise, if the **public-ip** parameter in the **client** section is configured on the main servefr, the **primaryIp** and **standbyIp** values in the nsp-config.yml file must be set to IP addresses.

```
integrations:
   nfmp:
     primaryIp: "main_server_address"
     standbyIp:
     tlsEnabled: true | false
```

78

If all of the following are true, configure the following parameters in the **integrations** section:

- You are integrating an NFM-P system with the NSP.
- You want the NFM-P to forward system metrics to the NSP cluster.
- The NFM-P main server and main database are on separate stations:

```
nfmpDB:
  primaryIp: ""
  standbyIp: ""
```

79

If both of the following are true, configure the following parameters in the **integrations** section:

- You are integrating an NFM-P system with the NSP.
- You want the NFM-P to forward system metrics to the NSP cluster.
- The NFM-P system includes one or more auxiliary servers:

```
auxServer:
  primaryIpList: ""
  standbyIpList: ""
```

80

If the NSP deployment includes one or more Release 22.11 or earlier analytics servers that are to remain at the earlier release, you must enable NSP and analytics compatibility; otherwise, you can skip this step.

Set the **legacyPortEnabled** parameter in the **analyticsServer** subsection of the **integrations** section to true as shown below:

```
analyticsServer:
  legacyPortEnabled: true
```

81

If the NSP deployment includes an auxiliary database, configure the required parameters.

Note: If the deployment includes the NFM-P, you must record the following values for addition to the local NFM-P main server configuration.

- ipList addresses, which must you must set as the *cluster_1* addresses in the local main server configuration
- standbyIpList addresses, which you must set as the *cluster_2* addresses local main server configuration

1. Locate the following section:

```
auxDb:
  secure: "value"
  ipList: ""
```

```
        standbyIpList: ""
```

2. Edit the section to read as follows:

   Note: The **secure** value must match the secure value in the NSP and NFM-P configurations.

   ```
   auxDb:
     secure: "value"
     ipList: "cluster_1_IP1,cluster_1_IP2...cluster_1_IPn"
     standbyIpList: "cluster_2_IP1,cluster_2_IP2...cluster_2_IPn"
   ```

   where

   cluster_1_IP1, *cluster_1_IP2*...*cluster_1_IPn* are the external IP addresses of the stations in the local cluster

   value is true or false, and specifies whether TLS is enabled

   cluster_2_IP1, *cluster_2_IP2*...*cluster_2_IPn* are the external IP addresses of the stations in the peer cluster; required only for geo-redundant deployment

82

If you are including VMs to host MDM instances in addition to a standard or enhanced NSP cluster deployment, configure the following **mdm** parameters in the **modules** section:

```
modules:
   mdm:
     clusterSize: members
     backupServers: n
```

where

members is the total number of VMs to host MDM instances

n is the total number of VMs to allocate as backup instances

83

Specify the user authorization mechanism in the **sso** section, as shown below.

```
  sso:
    authMode: "mode"
```

where *mode* is one of the following:

- oauth2—default; uses a local NSP user database, and can include remote authentication servers
- cas—deprecated; uses the NFM-P or remote authentication servers for authentication

84

If the **authMode** parameter is set to cas, special configuration is required; perform the following steps.

Note: The parameters apply only to an NSP system that uses CAS authentication.

1. Add the following to the **nsp**—**modules**—**nspos** section of the file:

```
    rest:
      session:
        ttlInMins: 60
        maxNumber: 50
```

2. Add the following to the end of the **nsp**—**sso** section:

```
  authMode: "cas"
  session:
    concurrentLimitsEnabled: false
    maxSessionsPerUser: 10
    maxSessionsForAdmin: 10
  throttling:
    enabled: true
    rateThreshold: 3
    rateSeconds: 9
    lockoutPeriod: 5
  loginFailure:
    enabled: false
    threshold: 3
    lockoutMinutes: 1
```

3. Configure the intended remote-authentication sources in the **nsp**—**sso** section.

85

Save and close the nsp-config.yml file.

86

Ensure that the location of your license.zip file, as indicated in the nsp-config.yml file, is in the correct location on the NSP deployer host.

87

If you are integrating an existing NFM-P system with the NSP, and the NFM-P TLS certificate is self-signed or root-CA-signed, you must use the NFM-P TLS artifacts in the NSP system.

Transfer the following TLS files from the NFM-P to the /opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/tls/ca directory:

- ca.pem
- ca.key
- ca_internal.pem
- ca_internal.key

88

If you are not including any dedicated MDM nodes in addition to the number of member nodes in a standard or enhanced NSP cluster, go to Step 95.

89

Log in as the root user on the NSP cluster host.

90

Open a console window.

91

Perform the following steps for each additional MDM node.

1. Enter the following to open an SSH session as the root user on the MDM node.

   Note: The root password for a VM created using the Nokia qcow2 image is available from technical support.

   ```
   # ssh root@MDM_node_IP_address ↵
   ```

2. Enter the following:

   ```
   # mkdir -p /opt/nsp/volumes/mdm-server ↵
   ```

3. Enter the following:

   ```
   # chown -R 1000:1000 /opt/nsp/volumes ↵
   ```

4. Enter the following:

   ```
   # exit ↵
   ```

92

Enter the following:

```
# kubectl get nodes -o wide ↵
```

A list of nodes like the following is displayed.

```
NAME     STATUS    ROLES     AGE    VERSION    INTERNAL-IP
EXTERNAL-IP
node1    Ready     master    nd    version    int_IP    ext_IP
node2    Ready     master    nd    version    int_IP    ext_IP
node3    Ready     <none>    nd    version    int_IP    ext_IP
```

93

Record the NAME value of each node whose INTERNAL-IP value is the IP address of a node that has been added to host an additional MDM instance.

94

For each node, enter the following sequence of commands:

```
# kubectl label node node mdm=true ↵
```

```
# kubectl cordon node ↵
```

where *node* is the recorded NAME value of the cordoned MDM node

Deploy NSP software

95

Log in as the root user on the NSP deployer host.

96

Open the following file with a plain-text editor such as vi:

/opt/nsp/NSP-CN-DEP-*release-ID*/config/nsp-deployer.yml

Configure the following parameters:

```
hosts: "hosts_file"
labelProfile: "../ansible/roles/apps/nspos-labels/vars/labels_file"
```

where

hosts_file is the absolute path of the hosts.yml file created in Step 56, typically /opt/nsp/nsp-k8s-deployer-*release-ID*/config/hosts.yml

labels_file is the file name below that corresponds to the cluster deployment type specified in Step 73:

- node-labels-basic-1node.yml
- node-labels-basic-sdn-2nodes.yml
- node-labels-enhanced-6nodes.yml
- node-labels-enhanced-sdn-9nodes.yml
- node-labels-standard-3nodes.yml
- node-labels-standard-4nodes.yml
- node-labels-standard-sdn-4nodes.yml
- node-labels-standard-sdn-5nodes.yml

97

Save and close the file.

98

Open a console window.

99

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

100

Enter the following to apply the node labels to the NSP cluster:

```
# ./nspdeployerctl config ↵
```

101

Enter the following to import the NSP images and Helm charts to the NSP Kubernetes registry

```
# ./nspdeployerctl import ↵
```

102

Enter the following to deploy the NSP software in the NSP cluster:

```
# ./nspdeployerctl install --config --deploy ↵
```

The specified NSP functions are installed and initialized.

Monitor NSP initialization

103

Monitor and validate the NSP cluster initialization.

Note: You must not proceed to the next step until each NSP pod is operational.

1. On the NSP cluster host, enter the following every few minutes:

   ```
   # kubectl get pods -A ↵
   ```

   The status of each NSP cluster pod is displayed; the NSP cluster is operational when the status of each pod is Running or Completed, with the following exception.

   - If you are including any MDM VMs in addition to a standard or enhanced NSP cluster deployment, the status of each mdm-server pod is shown as Pending, rather than Running or Completed.

2. If the Network Operations Analytics - Baseline Analytics installation option is enabled, ensure that the following pods are listed; otherwise, see the *NSP Troubleshooting Guide* for information about troubleshooting an errored pod:

   Note: The output for a non-HA deployment is shown below; an HA cluster has three sets of three baseline pods, three rta-ignite pods, and two spark-operator pods.

   - analytics-rtanalytics-tomcat
   - baseline-anomaly-detector-*n*-exec-1
   - baseline-trainer-*n*-exec-1
   - baseline-window-evaluator-*n*-exec-1
   - rta-anomaly-detector-app-driver
   - rta-ignite-0
   - rta-trainer-app-driver
   - rta-windower-app-driver
   - spark-operator-*m*-*n*

3. If any pod fails to enter the Running or Completed state, see the *NSP Troubleshooting Guide* for information about troubleshooting an errored pod.

104

If you are including any MDM VMs in addition to a standard or enhanced NSP cluster deployment, perform the following steps to uncordon the nodes cordoned in Step 94.

1. Enter the following:

   ```
   # kubectl get pods -A | grep Pending ↵
   ```

   The pods in the Pending state are listed; an mdm-server pod name has the format mdm-server-*ID*.

   Note: Some mdm-server pods may be in the Pending state because the manually labeled MDM nodes are cordoned in Step 94. You must not proceed to the next step if any pods other than the mdm-server pods are listed as Pending. If any other pod is shown, re-enter the command periodically until no pods, or only mdm-server pods, are listed.
2. Enter the following for each manually labeled and cordoned node:

   ```
   # kubectl uncordon node ↵
   ```

   where *node* is an MDM node name recorded in Step 94

   The MDM pods are deployed.

   Note: The deployment of all MDM pods may take a few minutes.
3. Enter the following periodically to display the MDM pod status:

   ```
   # kubectl get pods -A | grep mdm-server ↵
   ```
4. Ensure that the number of mdm-server-*ID* instances is the same as the **mdm** clusterSize value in nsp-config.yml, and that each pod is in the Running state. Otherwise, contact technical support for assistance.

105

Close the open console windows.

END OF STEPS

7.5 Workflow for independent NFM-P migration to the NSP

7.5.1 Description

The following is the sequence of high-level steps required to migrate from an NFM-P-only system to a shared-mode NSP deployment. Each cross-reference is a link to a section in procedure 7.6 “To migrate from an independent NFM-P system to the NSP” (p. 217).

7.5.2 Stages

1

Create the required NSP VMs in each data center, back up the NSP databases, and obtain the required security artifacts; see “Prepare for migration” (p. 218).

2

In each data center:

1. Deploy the NSP cluster; see “Deploy NSP clusters” (p. 219).
2. Restore the NSP Neo4j and PostgreSQL databases; see “Restore NSP databases” (p. 219).
3. Install the NSP software; see “Deploy NSP software” (p. 219).

3

Configure each NFM-P main server to use the nspOS instance in the new NSP cluster; see “Reconfigure NFM-P” (p. 220).

4

Synchronize the NFM-P and NSP system data; see “Synchronize system data” (p. 220).

5

If the NSP deployment includes NSP analytics servers, configure each analytics server to use the nspOS instance and PostgreSQL database in the NSP cluster; see “Reconfigure NSP analytics servers” (p. 221).

6

If the NSP system includes the WS-NOC, configure the WS-NOC to use the nspOS instance in the NSP cluster; see “Reconfigure WS-NOC” (p. 222).

7.6 To migrate from an independent NFM-P system to the NSP

7.6.1 Purpose

Perform this procedure to transfer the nspOS functions of an independent NFM-P system to a greenfield NSP deployment in order to create a shared-mode NSP deployment.

Note: When you migrate from an independent NFM-P to a shared-mode NSP system, the NFM-P Service Supervision groups are transferred to the NSP. The transfer may take hours, depending on the number of services. During this time, you must not auto-create any Service Supervision groups. You can use the Find Ungrouped members count in the Group Manager application to help determine when the upload is complete, after which you can auto-create groups.

Note: *release-ID* in a file path has the following format:

R.r.p-rel.*version*

where

R.r.p is the NSP release, in the form *MAJOR.minor.patch*

version is a numeric value

7.6.2 Steps

Prepare for migration

1

Perform Step 1 to Step 48 of 7.4 “To install the NSP” (p. 193) to do the following.

- Obtain the NSP software.
- Create the NSP deployer host.
- Create the NSP cluster VMs.

2

Using the specifications in the response to your Nokia Platform Sizing Request, create a VM for each additional RPM-based NSP component.

3

Perform the steps in the “To back up the main database from the client GUI” procedure in one of the following guides, depending on the installed NFM-P release:

- Release 22.9 or earlier—*NSP NFM-P Administrator Guide*
- Release 22.11 or later—*NSP System Administrator Guide*

4

Transfer the following TLS files from the current PKI-server station to a secure location on a station that is unaffected by the migration activity:

i **Note:** The PKI server address can be viewed using the samconfig utility on an NFM-P main server station.

- ca.pem
- ca.key
- ca_internal.pem
- ca_internal.key

5

Perform Step 7 to Step 12 on each NSP cluster.

i **Note:** In a DR deployment, you must perform the steps first on the NSP cluster that you want to be the primary cluster after the upgrade.

6

Go to Step 13.

Deploy NSP clusters

7

Perform Step 49 to Step 101 of 7.4 “To install the NSP” (p. 193) to deploy the NSP Kubernetes cluster and configure the NSP deployment parameters.

Restore NSP databases

8

Copy the following Neo4j and PostgreSQL database backup files created in Step 3 to an empty temporary directory on the NSP deployer host:

- nspos-neo4j_backup_*timestamp*.tar.gz
- nspos-postgresql_backup_*timestamp*.tar.gz

where *timestamp* is the backup creation time

9

Perform “How do I restore the NSP cluster databases?” in the *NSP System Administrator Guide* to restore only the following databases on the NSP cluster:

Note: Performing the procedure also starts the NSP.

- Neo4j database
- PostgreSQL database

Deploy NSP software

10

Monitor the NSP initialization; if the status of any pod is Error, you must correct the error; see the *NSP System Administrator Guide* for information about recovering an errored pod.

Note: You must not proceed to the next step until the cluster is operational and no pods are in error.

11

If you are configuring the standby NSP cluster in a DR deployment, obtain the SSH, TLS, and telemetry artifacts from the NSP cluster in the primary data center.

1. Open a console window on the NSP deployer host.
2. Enter the following:

```
# mkdir -p /opt/nsp/nsp-configurator/generated/ssh ↵
```

3. Enter the following:

```
# scp root@address:/opt/nsp/nsp-configurator/generated/ssh/*
/opt/nsp/nsp-configurator/generated/ssh/ ↵
```

4. Enter the following:

```
# scp root@address:
/opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tls/ca/*
/opt/nsp/NSP-CN-release-ID/tls/ca/ ↵
```

5. Enter the following:

```
# scp root@address:
/opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tls/telemetry/*
/opt/nsp/NSP-CN-release-ID/tls/telemetry/ ↵
```

where *address* is the address of the NSP cluster host in the primary cluster

12

In order for the IGP maps to function after the migration, you may need to change the IGP topology data source; see 13.20 “Configuring the IGP topology data source” (p. 397) for information.

Reconfigure NFM-P

13

Perform Step 1 to Step 15 of 11.3 “To integrate the NSP and NFM-P” (p. 327).

Synchronize system data

14

Verify that the NFM-P main server is fully initialized.

Note: You must not advance to the next step until the server is fully initialized.

1. Enter the following as the nsp user on the main server station.

```
# cd /opt/nsp/nfmp/nms/bin ↵
```

2.
```
# ./nmsserver.bash -s nms_status ↵
```

Output like the following is displayed:

```
Network Functions Manager - Packet: Main Server Information
-- Build Information
  -- NSP Version 23.11.MAIN.11098 - Built on Fri Nov 10 04:42:40
EST 2023
-- System Information
  -- Host/IP: 135.121.101.164
-- Server Information
  -- Server is a standalone system
  -- Server is server_state
  -- SSL Channel Disabled for OSS and GUI Clients
```

The server is fully initialized if the following is displayed:

```
  -- Server is Up
```

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

15

Log in as the root user on the NSP deployer host in the primary data center.

16

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/database ↵
```

17

Enter the following:

```
# ./nfmp-resync.sh ↵
```

The following time-stamped lines are displayed as the script synchronizes the NFM-P and NSP system data:

```
timestamp: Running with nsp-psa-restricted/nsp-platform-tomcat-pod_ID
timestamp: Resync triggered successfully
```

where *pod_ID* is an alphanumeric pod ID

Reconfigure NSP analytics servers

18

If the system from which you are migrating includes one or more analytics servers, perform the following steps on each NSP analytics server station.

1. Log in as the nsp user.
2. Enter the following:

   ```
   bash$ cd /opt/nsp/analytics/bin ↵
   ```

3. Enter the following to stop the server:

   ```
   bash$ ./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
   ```

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

4. Enter the following:

   ```
   bash$ ./AnalyticsAdmin.sh updateConfig ↵
   ```

   The script displays the following message and prompt:

   ```
   HIS ACTION UPDATES THE CONFIG FILE
   Please type 'YES' to continue
   ```

5. Enter YES.

The script displays the following, and the first in a series of prompts. At each prompt, you must enter a parameter value; to accept a default in brackets, press ↵.

```
Config file found.
```

6. Configure the following parameters as described below; see Table 14-2, “NSP analytics server parameters” (p. 419) for more information about a parameter.
   - Primary PostgreSQL Repository Database Host—standalone or primary NSP cluster VIP address
   - Secondary PostgreSQL Repository Database Host—standby NSP cluster VIP address; leave blank for a standalone NSP deployment
   - Zookeeper Connection String—the NSP cluster VIP addresses and ports, separated by a semicolon, for example:

     address_1:*port*;*address_2*:*port*
   - Use NFM-P-only mode—must be set to true

19

Enter the following:

```
bash$ ./AnalyticsAdmin.sh start ↵
```

The analytics server starts.

Reconfigure WS-NOC

20

If the deployment includes the WS-NOC, configure the WS-NOC to use the new nspOS instance by specifying the advertised address of the NSP cluster as the nspOS address.

END OF STEPS

8 NSP system upgrade from Release 22.6 or earlier

8.1 Upgrading from Release 22.6 or earlier

8.1.1 NSP system upgrade process

CAUTION

Service Disruption

An NSP system upgrade requires a thorough understanding of NSP system administration and platform requirements, and is supported only under the conditions described in this guide, the NSP Planning Guide, and the NSP 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 NSP professional services to assess the requirements of your NSP deployment, and for information about the upgrade service, which you are strongly recommended to engage for any type of deployment.

The following workflows provide comprehensive overviews of the required upgrade activities for advance planning purposes:

- 8.2 “Workflow for standalone NSP system upgrade from Release 22.6 or earlier” (p. 224)
- 8.3 “Workflow for DR NSP system upgrade from Release 22.6 or earlier” (p. 226)

Each workflow includes links to the required procedures and procedure sections for completing the upgrade.

Note: An NSP system that manages a large number of NEs may require several hours, or potentially a full day for a very large network, to resynchronize the network following an NSP upgrade. It is important to consider the resynchronization time when planning a maintenance window for NSP upgrade activity.

Licensing

Your NSP system may require a new or updated license, depending on your deployment and the NSP release from which you upgrade. It is recommended that you contact Nokia early in the planning process to obtain the required license for your upgraded deployment.

Migrating to RHEL 8

An NSP system upgrade from Release 22.6 or earlier involves a migration to version 8 of the RHEL OS on each NSP station, so is essentially a platform migration. If new stations are not to be used, the existing stations must be decommissioned and then recommissioned.

DR NSP system upgrade

In order to minimize the network visibility loss during a DR system upgrade, the primary NSP cluster remains active while a new standby cluster is deployed.

After a system database backup from the primary cluster is restored on the standby, the primary cluster is stopped, and the standby cluster is activated as a primary cluster. The former primary cluster is then upgraded, and subsequently assumes the standby role.

The loss of network visibility begins when the initial primary cluster is stopped, and ends when the NSP software initialization on the new primary cluster completes.

8.2 Workflow for standalone NSP system upgrade from Release 22.6 or earlier

8.2.1 Purpose

The following is the sequence of high-level actions involved in the upgrade of a standalone NSP system.

8.2.2 Stages

Prepare for upgrade

1

Perform 8.5 “To prepare for an NSP system upgrade from Release 22.6 or earlier” (p. 232) to do the following:

- back up the NSP system configuration, databases, and file service data
- download the NSP installation software
- verify the cluster readiness for the upgrade
- perform special upgrade preconfiguration

Upgrade NSP cluster

2

Perform the following phases of 8.6 “To upgrade a Release 22.6 or earlier NSP cluster” (p. 237). Each phase consists of a series of high-level action links that lead to step sections in the procedure.

1. **Disable existing cluster**—Step 1 to Step 8
    - “Stop and undeploy NSP cluster” (p. 238)—**marks the beginning of the network visibility loss associated with the upgrade**
    - “Uninstall IPRC, CDRC” (p. 239)
    - “Preserve NSP cluster configuration” (p. 240)
2. **Create new container environment**—Step 9 to Step 83
    - “Create NSP deployer host” (p. 240)
    - “Configure NSP deployer host network interface” (p. 241)
    - “Install NSP Kubernetes registry” (p. 244)
    - “Migrate legacy cluster parameters” (p. 246)
    - “Create NSP cluster VMs” (p. 248)

- “Configure NSP cluster interfaces” (p. 249)
- “Deploy container environment” (p. 251)

3. **Install and deploy NSP software**—Step 84 to Step 135 (end of procedure)
   - “Restore NSP system configuration” (p. 254)
   - “Label NSP cluster nodes” (p. 255)
   - “Configure NSP software” (p. 256)
   - “Restore dedicated MDM node labels” (p. 260)
   - “Deploy NSP cluster” (p. 261)
   - “Restore NSP data” (p. 262)
   - “Start NSP” (p. 262)
   - “Monitor NSP initialization” (p. 262)—**successful startup marks the end of the network visibility loss**
   - “Verify upgraded NSP cluster operation” (p. 264)
   - “Upgrade MDM adaptors” (p. 264)
   - “Synchronize auxiliary database password” (p. 265)
   - “Perform post-upgrade tasks” (p. 265)

Perform sanity check of upgraded system

3

Verify various NSP system functions by performing actions such as:

- comparing the benchmarks recorded before the upgrade to the current indicators
- verifying NSP UI access
- verifying the service list in NSP's service management views

Upgrade or enable additional components and systems

4

If the NSP deployment includes the VSR-NRC, upgrade the VSR-NRC as described in the VSR-NRC documentation.

5

If you are including an existing NFM-P system at an earlier release in the deployment, perform one of the following.

a. Upgrade the NFM-P to the NSP release; see “NFM-P system upgrade from Release 22.6 or earlier” (p. 628).

b. Enable NFM-P and NSP compatibility; perform 11.4 “To enable NSP compatibility with an earlier NFM-P system” (p. 333).

Note: An NFM-P system upgrade procedure includes steps for upgrading the following components in an orderly fashion.

- auxiliary database

- NSP Flow Collectors / Flow Collector Controllers
- NSP analytics servers

6

If the NSP system includes the WS-NOC, perform the appropriate procedure in "WS-NOC and NSP integration" (p. 340) to enable WS-NOC integration with the upgraded NSP system.

8.3 Workflow for DR NSP system upgrade from Release 22.6 or earlier

8.3.1 Purpose

The following is the sequence of high-level actions involved in the upgrade of a DR Release 22.6 or earlier NSP system.

8.3.2 Stages

Prepare for upgrade

1

Perform "How do I display the NSP cluster status?" in the *NSP System Administrator Guide* to:

- identify the primary and standby NSP clusters
- verify the operational state of each NSP cluster

Upgrade standby NSP cluster

2

In the standby data center, perform 8.5 "To prepare for an NSP system upgrade from Release 22.6 or earlier" (p. 232), to do the following:

- back up the NSP software configuration
- download the NSP installation software
- verify the cluster readiness for the upgrade
- perform special upgrade preconfiguration

3

In the standby data center, perform the following phases of 8.6 "To upgrade a Release 22.6 or earlier NSP cluster" (p. 237); each phase has links to step sections in the procedure.

1. **Disable existing cluster**—Step 1 to Step 8
   - "Stop and undeploy NSP cluster" (p. 238)
   - "Uninstall IPRC, CDRC" (p. 239)
   - "Preserve NSP cluster configuration" (p. 240)
2. **Create new container environment**—Step 9 to Step 111
   - "Create NSP deployer host" (p. 240)

- “Configure NSP deployer host network interface” (p. 241)
- “Install NSP Kubernetes registry” (p. 244)
- “Migrate legacy cluster parameters” (p. 246)
- “Create NSP cluster VMs” (p. 248)
- “Configure NSP cluster interfaces” (p. 249)
- “Deploy container environment” (p. 251)
- “Restore NSP system configuration” (p. 254)
- “Label NSP cluster nodes” (p. 255)
- “Configure NSP software” (p. 256)

Note: The standby cluster, which becomes the new primary cluster, is not started until after you stop the primary cluster.

Prepare primary NSP cluster for upgrade

4

In the primary data center, perform 8.5 “To prepare for an NSP system upgrade from Release 22.6 or earlier” (p. 232) to do the following:

- back up the NSP software configuration, databases, and system data
- download the NSP installation software
- verify the cluster readiness for the upgrade
- perform special upgrade preconfiguration

5

In the primary data center, perform the following phase of 8.6 “To upgrade a Release 22.6 or earlier NSP cluster” (p. 237) .

Disable existing cluster—Step 1 to Step 8

- “Stop and undeploy NSP cluster” (p. 238)—**marks the beginning of the network visibility loss associated with the upgrade**
- “Uninstall IPRC, CDRC” (p. 239)
- “Preserve NSP cluster configuration” (p. 240)

Configure and start new primary (former standby) NSP cluster

6

In the standby data center, perform the following phase of 8.6 “To upgrade a Release 22.6 or earlier NSP cluster” (p. 237).

Configure and start NSP cluster—Step 112 to Step 135 (end of procedure)

- “Restore dedicated MDM node labels” (p. 260)
- “Deploy NSP cluster” (p. 261)
- “Restore NSP data” (p. 262)

- “Start NSP” (p. 262)
- “Monitor NSP initialization” (p. 262)—**successful startup marks the end of the network visibility loss**
- “Verify upgraded NSP cluster operation” (p. 264)
- “Upgrade MDM adaptors” (p. 264)
- “Synchronize auxiliary database password” (p. 265)
- “Perform post-upgrade tasks” (p. 265)

Perform sanity check of new primary NSP cluster

7

On the new primary NSP cluster, verify various NSP system functions by performing actions such as:

- comparing the benchmarks recorded before the upgrade to the current indicators
- verifying NSP UI access
- verifying the service list in NSP's service management views

Upgrade or enable additional primary components and systems

8

If the NSP deployment includes the VSR-NRC, upgrade the VSR-NRC In the new primary (former standby) data center, as described in the VSR-NRC documentation.

9

If you are including an existing NFM-P system at an earlier release in the deployment, perform one of the following In the new primary (former standby) data center.

a. Upgrade the NFM-P to the NSP release; see “NFM-P system upgrade from Release 22.6 or earlier” (p. 628).

b. Enable NFM-P and NSP compatibility; perform 11.4 “To enable NSP compatibility with an earlier NFM-P system” (p. 333).

Note: An NFM-P system upgrade procedure includes steps for upgrading the following components in an orderly fashion.

- auxiliary database
- NSP Flow Collectors / Flow Collector Controllers
- NSP analytics servers

10

If the NSP system includes the WS-NOC, perform the appropriate procedure in “WS-NOC and NSP integration” (p. 340) to enable WS-NOC integration with the upgraded NSP system.

Upgrade new standby (former primary) NSP cluster

11

In the former primary data center, perform the following phases of 8.6 “To upgrade a Release 22.6 or earlier NSP cluster” (p. 237).

1. **Create new container environment**—Step 9 to Step 111
   - “Create NSP deployer host” (p. 240)
   - “Configure NSP deployer host network interface” (p. 241)
   - “Install NSP Kubernetes registry” (p. 244)
   - “Migrate legacy cluster parameters” (p. 246)
   - “Create NSP cluster VMs” (p. 248)
   - “Configure NSP cluster interfaces” (p. 249)
   - “Deploy container environment” (p. 251)
   - “Restore NSP system configuration” (p. 254)
   - “Label NSP cluster nodes” (p. 255)
   - “Configure NSP software” (p. 256)
2. **Install and start NSP**—Step 112 to Step 135 (end of procedure)
   - “Restore dedicated MDM node labels” (p. 260)
   - “Deploy NSP cluster” (p. 261)
   - “Start NSP” (p. 262)
   - “Monitor NSP initialization” (p. 262)
   - “Verify upgraded NSP cluster operation” (p. 264)
   - “Perform post-upgrade tasks” (p. 265)

Perform sanity check of new standby NSP cluster

12

Use a browser to open the standby NSP cluster URL.

13

Verify the following.

- The browser is redirected to the primary cluster address.
- The NSP sign-in page opens.
- The NSP UI opens after you sign in.

Upgrade or enable additional standby components and systems

14

If the NSP deployment includes the VSR-NRC, upgrade the VSR-NRC In the new standby (former primary) data center, as described in the VSR-NRC documentation.

15

If you are including an existing NFM-P system at an earlier release in the deployment, perform one of the following In the new standby (former primary) data center.

a. Upgrade the NFM-P to the NSP release; see "NFM-P system upgrade from Release 22.9 or later" (p. 819).

b. Enable NFM-P and NSP compatibility; perform 11.4 "To enable NSP compatibility with an earlier NFM-P system" (p. 333).

Note: An NFM-P system upgrade procedure includes steps for upgrading the following components in an orderly fashion.

- auxiliary database
- NSP Flow Collectors / Flow Collector Controllers
- NSP analytics servers

16

If the NSP system includes the WS-NOC, perform the appropriate procedure in "WS-NOC and NSP integration" (p. 340) to enable WS-NOC integration with the upgraded NSP system.

8.4 To back up the Release 22.3 or earlier NSP file service data

8.4.1 Purpose

Perform this procedure to manually back up the NSP file service data before you upgrade a Release 22.3 or earlier system.

8.4.2 Steps

1

Log in as the root user on the NSP cluster VM that is called the NSP configurator VM or NSP cluster host.

2

Open a console window.

3

Perform one of the following to change to the file service pod.

a. For a Release 21.3 NSP system, enter the following:

```
# kubectl exec -it nsp-file-service-app-0 -c nsp-file-service-app
bin/bash ↵
```

b. For an NSP system at Release 21.6 or later, enter the following:

```
# kubectl exec -it nsp-file-service-app-0 bin/bash ↵
```

4

Enter the following:

```
# cd /opt/nsp/containers/nspvolume/fileservice ↵
```

5

Enter the following:

```
# tar -cvf fileServiceData.tar * ↵
```

The files that are backed up are listed, and added to a backup file in the current directory called fileServiceData.tar.

The files may include MDM adaptor suite and device mapping files.

6

Perform one of the following to copy the backup file to the local file system.

a. For a Release 21.3 NSP system, enter the following:

```
# kubectl cp nsp-file-service-app-0:
/opt/nsp/containers/nspvolume/fileservice/fileServiceData.tar
fileServiceData.tar -c nsp-file-service-app ↵
```

b. For an NSP system at Release 21.6 or later, enter the following:

```
# kubectl cp nsp-file-service-app-0:
/opt/nsp/containers/nspvolume/fileservice/fileServiceData.tar
fileServiceData.tar ↵
```

7

Transfer the backup file from the current directory to a secure location in a separate facility for safekeeping.

Note: It is strongly recommended that for the greatest fault tolerance, you transfer the backup file to a secure facility that is outside the local data center.

8

To conserve system resources, it is recommended that you remove the backup file from the nsp-file-service-app pod.

Perform the following steps.

1. Enter the following:

```
# kubectl exec -it nsp-file-service-app-0 bin/bash ↵
```

2. Enter the following:

```
# cd /opt/nsp/containers/nspvolume/fileservice ↵
```

3. Enter the following:

```
# rm -f fileServiceData.tar ↵
```

The backup file is deleted.

9

Close the console window.

End of steps

8.5 To prepare for an NSP system upgrade from Release 22.6 or earlier

8.5.1 Purpose

Perform this procedure to prepare for an NSP system upgrade from Release 22.6 or earlier.

> **Note:** *release-ID* in a file path has the following format:
> *R.r.p*-rel.*version*
> where
> *R.r.p* is the NSP release, in the form *MAJOR.minor.patch*
> *version* is a numeric value

8.5.2 Steps

Back up NSP databases, system data

1

Log in as the root user on the appropriate station, based on the installed NSP release:

- Release 22.3 or earlier—NSP configurator VM
- Release 22.6—NSP deployer host

2

Transfer the appropriate file, based on the installed NSP release, to a secure location on a separate station that is unaffected by the upgrade activity:

- Release 22.3 or earlier—/opt/nsp/NSP-CN-*release-ID*/appliedConfigs/nspConfiguratorConfigs.zip
- Release 22.6—/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/appliedConfigs/nspConfiguratorConfigs.zip

3

If you are upgrading a standalone NSP cluster, or the primary cluster in a DR deployment, perform the following steps.

> **Note:** The backup operations may take considerable time, during which you can start the software download described in Step 4.

1. Back up the NSP databases; perform the appropriate NSP database backup procedure in the *NSP System Administrator Guide* for the currently installed NSP release.

2. If the NSP system is at Release 22.3 or earlier and includes the NSP file service, perform 8.4 “To back up the Release 22.3 or earlier NSP file service data” (p. 230).
3. If the NSP deployment includes IP resource control deployed outside the NSP cluster, back up the IPRC Tomcat database of IP resource control as described in the *NSP System Administrator Guide* for the currently installed NSP release.

Obtain installation software

4

Download the following from the NSP downloads page on the Nokia Support portal to a local station that is not affected by the upgrade activity:

Note: You must also download the .cksum file associated with each.

- NSP_K8S_DEPLOYER_*R_r*.tar.gz—bundle for installing the registry and deploying the container environment
- one of the following RHEL OS images for creating the NSP deployer host and NSP cluster VMs:
  - NSP_K8S_PLATFORM_RHEL8_*yy_mm*.qcow2
  - NSP_K8S_PLATFORM_RHEL8_*yy_mm*.ova
- NSP_DEPLOYER_*R_r*.tar.gz—bundle for installing the NSP application software

where

R_r is the NSP release ID, in the form *Major_minor*

yy_mm represents the year and month of issue

5

Record benchmarks such as system KPIs, equipment inventories, and service lists for verification after the upgrade.

6

It is strongly recommended that you verify the message digest of each NSP image file or software bundle that you download from the Nokia Support portal. The download page includes checksums for comparison with the output of the RHEL md5sum, sha256sum, or sha512sum command.

To verify a file checksum, perform the following steps.

1. Enter the following:

   ```
   # command file ↵
   ```

   where

   command is md5sum, sha256sum, or sha512sum

   file is the name of the file to check

   A file checksum is displayed.
2. Compare the checksum value and the value in the .cksum file.

3. If the values do not match, the file download has failed. Download a new copy of the file, and then repeat this step.

Back up Elasticsearch log data

7

If log forwarding to Elasticsearch is not enabled in the NSP system, go to Step 20.

Starting in NSP Release 23.4, OpenSearch replaces Elasticsearch as the NSP log-viewing utility. If you are upgrading from an NSP release that uses Elasticsearch for viewing NSP logs, it is strongly recommended that you preserve the Elasticsearch log data collected by the NSP before you upgrade the NSP.

You can later restore the backed-up data for import by an Elasticsearch server in order to review the log data, if required, as described in “How do I restore the NSP Elasticsearch log data?” in the *NSP System Administrator Guide*.

Log in as the root user on the station that has the downloaded NSP_DEPLOYER_*R_r*.tar.gz file.

8

Navigate to the directory that contains the NSP_DEPLOYER_*R_r*.tar.gz file.

9

Enter the following:

```
# tar xvf NSP_DEPLOYER_R_r.tar.gz '*nsp-log-collector.zip'
'*README.txt' ↵
```

The nsp-log-collector.zip file and a README.txt file are extracted to the following directory path below the current directory:

NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/tools/support/logCollector

Note: The README.txt contains information about using the backup utility.

10

Log in as the root user on NSP cluster node 1, which is called one of the following, based on the installed NSP release:

- Release 22.3 or earlier—NSP configurator VM
- Release 22.6—NSP cluster host

11

Open a console window.

12

Navigate to a directory that has sufficient free space for the backup log data, such as /opt.

Note: The space required for the log backup is based on the number of days for which log data is stored by the NSP, which is specifed by the logRetentionPeriodInDaysOverride parameter value in the NSP cluster configuration file, and the average amount of log data per day.

13

Transfer the extracted nsp-log-collector.zip and README.txt files to the current directory.

14

In order to perform an ElasticSearch data backup, the java-1.8.0-openjdk RHEL OS package must be installed. However, the package may not be present on an earlier system.

Enter the following:

```
# yum -y install java-1.8.0-openjdk ↵
```

If the package is not installed, the yum utility installs the package. Otherwise, the utility indicates that the package is installed, and nothing is done.

15

Enter the following:

```
# unzip nsp-log-collector.zip ↵
```

The following files are created in an nsp-log-collector-*release-ID*/bin directory in the current directory:

- nsp-log-collector
- nsp-log-collector.bat

16

After the files are extracted, enter the following:

```
# cd nsp-log-collector-release-ID/bin ↵
```

17

Enter the following to back up all collected Elasticsearch log data:

```
# ./nsp-log-collector --getAll path ↵
```

where *path* is the local directory in which to store the backed-up log data

The following prompt is displayed:

```
Do you want to proceed with log collection? (y/n) :
```

18

Enter y.

The backup process begins.

The backup process creates the following .zip file in the specified *path* directory:

Logs-*timestamp*.zip

where *timestamp* is the backup creation date and fime

19

Transfer the Logs-*timestamp*.zip file for safekeeping to a secure location on a station that is not part of the NSP deployment.

Check and prepare NSP cluster

20

Perform the following steps to verify that the local NSP cluster is fully operational.

1. Log in as the root user on an NSP cluster member in the data center.
2. Enter the following:

   ```
   # kubectl get pods -A ↵
   ```

   The status of each pod is displayed.

   The NSP cluster is operational if the status of each member pod is Running or Completed.
3. If any pod is not in the Running or Completed state, you must correct the condition; see the *NSP Troubleshooting Guide* for information about troubleshooting an errored pod.

21

Ensure that the RHEL chronyd time-synchronization service is running on each component, and that chronyd is actively tracking a central time source. See the RHEL documentation for information about using the chronyc command to view the chronyd synchronization status.

ℹ **Note:** NSP deployment is blocked if the chronyd service is not active.

22

Identify the dedicated MDM nodes in the NSP cluster; you require the information for restoring the cluster configuration later in the procedure.

1. Log in as the root user on any NSP cluster node.
2. Open a console window..
3. Enter the following:

   ```
   # kubectl get nodes --show-labels ↵
   ```
4. Identify the dedicated MDM nodes, which have only the following label and no other NSP labels:

   ```
   mdm=true
   ```

   For example:

   ```
   /os=linux,mdm=true
   ```
5. Record the name of each dedicated MDM node.

23

WARNING

Upgrade Failure

An NSP system upgrade from Release 22.3 or earlier fails if any logical inventory adaptor suites are installed.

In order to successfully upgrade an NSP system at Release 22.3 or earlier, you must remove each logical inventory adaptor suite before the upgrade.

The NSP upgrade procedure includes a step for re-installing the adaptor suites after the upgrade.

If you are upgrading from Release 22.3 or earlier, perform “How do I uninstall MDM adaptor suites?” in the *NSP System Administrator Guide* for each installed logical inventory adaptor suite.

END OF STEPS

8.6 To upgrade a Release 22.6 or earlier NSP cluster

8.6.1 Purpose

CAUTION

Network management outage

The procedure requires a shutdown of the NSP system, which causes a network management outage.

Ensure that you perform the procedure only during a scheduled maintenance period with the assistance of technical support.

Perform this procedure to upgrade a standalone or DR NSP system at Release 22.6 or earlier after you have performed 8.5 “To prepare for an NSP system upgrade from Release 22.6 or earlier” (p. 232).

Note: *release-ID* in a file path has the following format:

R.r.p-rel.*version*

where

R.r.p is the NSP release, in the form *MAJOR.minor.patch*

version is a numeric value

Note: If you are upgrading from an NSP release earlier than 22.6, LLDP link discovery is performed by Original Service Fulfillment by default, rather than NSP Network Infrastructure Management. You can change this behavior only when the lldpv2 adaptors are available or deployed for all managed devices; otherwise, a loss of LLDP data occurs. See 6.5 “Configuring LLDP link discovery” (p. 185) for more information.

8.6.2 Steps

Stop and undeploy NSP cluster

1

Log in as the root user on the appropriate station, based on the installed NSP release:

- Release 22.3 or earlier—NSP configurator VM
- Release 22.6—NSP deployer host

2

Perform the following steps to preserve the existing cluster data.

1. Open the appropriate file, based on the installed NSP release, using a plain-text editor such as vi:
   - Release 22.3 or earlier—/opt/nsp/NSP-CN-*release-ID*/config/nsp-config.yml
   - Release 22.6—/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml
2. Edit the following line in the **platform** section, **kubernetes** subsection to read:

   ```
   deleteOnUndeploy:false
   ```
3. Save and close the file.

3

CAUTION

Data Loss

Undeploying an NSP cluster as described in this step permanently removes the cluster data.

If you are upgrading a DR NSP system, you must ensure that you have the latest database backup from the primary cluster before you perform this step.

Undeploy the NSP cluster:

Note: If you are upgrading a standalone NSP system, or the primary NSP cluster in a DR deployment, this step marks the beginning of the network management outage associated with the upgrade.

Note: If the NSP cluster members do not have the required SSH key, you must include the --ask-pass argument in the command, as shown in the following example, and are subsequently prompted for the common root password of each cluster member:

```
command --ask-pass option option ↵
```

a. If you are upgrading from Release 22.3 or earlier, enter the following:

```
# /opt/nsp/NSP-CN-DEP-release-ID/bin/nsp-config.bash --undeploy
--clean ↵
```

b. If you are upgrading from Release 22.6 or later, enter the following:

```
# /opt/nsp/NSP-CN-DEP-release-ID/bin/nspdeployerctl uninstall
--undeploy --clean ↵
```

The NSP cluster is undeployed.

4

Before you create new NSP cluster VMs, you must disable each existing VM in the NSP cluster. The following options are available.

- stop but do not delete existing VMs—simplifies upgrade rollback, but requires sufficient platform resources for new VMs
- delete existing VMs—complicates upgrade rollback, but conserves platform resources

1. Log in as the root user on the station that hosts the NSP cluster VM.
2. Enter the following:

   ```
   # virsh list ↵
   ```

   The NSP cluster VMs are listed.
3. Enter the following for each listed VM:

   ```
   # virsh destroy VM ↵
   ```

   where *VM* is the VM name

   The VM stops.
4. To delete the VM, enter the following:

   ```
   # virsh undefine VM ↵
   ```

   The VM is deleted.

Uninstall IPRC, CDRC

5

If you are upgrading from Release 22.3 and the NSP deployment includes IP resource control or cross-domain resource control, uninstall each IPRC and CDRC server.

1. Log in as the root user on the IPRC or CDRC server station that has the extracted NSP software bundle from the previous installation or upgrade.
2. Open a console window.
3. Navigate to the NSP installer directory; enter the following:

   ```
   # cd path/NSD_NRC_R_r ↵
   ```

   where

   path is the directory that contains the extracted NSP software bundle

   R_r is the NSP software release, in the form *MAJOR_minor*
4. Edit the hosts file in the directory to list only the addresses of the NSP components to uninstall.

   Note: The uninstaller uses the same root password on each server in the list; ensure that you specify only servers that have the same root password.

5. Enter the following; include the --ask-pass option only if each target station has the same root user password:

   ```
   # ./bin/uninstall.sh --ask-pass ↵
   ```

6. Enter the root user password each time you are prompted.

   The NSP software is removed from each server listed in the hosts file.

7. Close the console window.

Preserve NSP cluster configuration

6

Log in as the root user on the existing NSP deployer host.

7

Open a console window.

8

Perform one of the following.

a. If you are upgrading from NSP Release 21.9 or earlier, copy the following file to a separate station that is unaffected by the upgrade activity:

   /opt/pnt/kubespray/inventory/nsp-deployer-default/hosts.yml

b. If you are upgrading from NSP Release 21.11 or 22.3, copy the following file to a separate station that is unaffected by the upgrade activity:

   /opt/nsp/kubespray/inventory/nsp-deployer-default/hosts.yml

c. If you are upgrading from NSP Release 22.6, copy the following file to a separate station that is unaffected by the upgrade activity:

   /opt/nsp/nsp-k8s-deployer-*release-ID*/config/k8s-deployer.yml

Create NSP deployer host

9

Log in as the root user on the station that will host the NSP deployer host VM.

10

Open a console window.

11

Enter the following:

```
# dnf -y install virt-install libguestfs-tools ↵
```

12

Before you create the new NSP deployer host VM, you must disable the existing VM; the following options are available.

- stop but do not delete existing VM—simplifies upgrade rollback, but VM consumes platform resources
- delete existing VM—complicates upgrade rollback, but conserves platform resources

1. Log in as the root user on the station that hosts the NSP deployer host VM.
2. Enter the following to list the VMs on the station:

   ```
   # virsh list ↵
   ```

   The VMs are listed.
3. Enter the following:

   ```
   # virsh destroy VM ↵
   ```

   where *VM* is the name of the NSP deployer host VM

   The NSP deployer host VM stops.
4. To delete the VM, enter the following:

   Note: If you intend to use the same VM name for the new NSP deployer host VM, you must delete the VM.

   ```
   # virsh undefine VM ↵
   ```

   The VM is deleted.

13

Perform one of the following to create the new NSP deployer host VM.

Note: The NSP deployer host VM requires a hostname; you must change the default of ‘localhost’ to an actual hostname.

a. Deploy the downloaded NSP_K8S_PLATFORM_RHEL8_*yy_mm*.qcow2 disk image; perform Step 6 to Step 16 of 2.3 “To deploy an NSP RHEL qcow2 disk image” (p. 30).

b. Deploy the NSP_K8S_PLATFORM_RHEL8_*yy_mm*.ova disk image; see the documentation for your virtualization environment for information.

   Note: For OVA-image deployment, it is strongly recommended that you mount the /opt directory on a separate hard disk that has sufficient capacity to allow for future expansion.

c. Manually install the RHEL OS and configure the disk partitions, as described in “Manual NSP RHEL OS installation” (p. 70) and Chapter 2, “NSP disk setup and partitioning”.

Configure NSP deployer host network interface

14

Enter the following to open a console session on the NSP deployer host VM:

```
# virsh console deployer_host ↵
```

You are prompted for credentials.

15

Enter the following credentials:

- username—root
- password—*available from technical support*

A virtual serial console session opens.

16

Enter the following:

```
# ip a ↵
```

The available network interfaces are listed; information like the following is displayed for each:

```
if_n: if_name: LESSTHANBROADCAST,MULTICAST,UP,LOWER_UPGTRTHAN mtu 1500
qdisc mq state UP group default qlen 1000
    link/ether MAC_address
    inet IPv4_address/v4_netmask brd broadcast_address scope global
noprefixroute if_name
       valid_lft forever preferred_lft forever
    inet6 IPv6_address/v6_netmask scope link
       valid_lft forever preferred_lft forever
```

17

Record the *if_name* and *MAC_address* values of the interface that you intend to use.

18

Enter the following:

```
# nmcli con add con-name con_name ifname if_name type ethernet mac
MAC_address ↵
```

where

con_name is a connection name that you assign to the interface for ease of identification

if_name is the interface name recorded in Step 17

MAC_address is the MAC address recorded in Step 17

19

Enter the following:

```
# nmcli con mod con_name ipv4.addresses IP_address/netmask ↵
```

where

con_name is the connection name assigned in Step 18

IP_address is the IP address to assign to the interface

netmask is the subnet mask to assign

20

Enter the following:

```
# nmcli con mod con_name ipv4.method static ↵
```

21

Enter the following:

```
# nmcli con mod con_name ipv4.gateway gateway_IP ↵
```

gateway_IP is the gateway IP address to assign

22

Enter the following:

Note: You must specify a DNS name server. If DNS is not deployed, you must use a non-routable IP address as a nameserver entry.

Note: Any hostnames used in an NSP deployment must be resolved by a DNS server.

Note: An NSP deployment that uses IPv6 networking for client communication must use a hostname configuration.

```
# nmcli con mod con_name ipv4.dns nameserver_1,nameserver_2...
nameserver_n ↵
```

where *nameserver_1* to *nameserver_n* are the available DNS name servers

23

To optionally specify one or more DNS search domains, enter the following:

```
# nmcli con mod con_name ipv4.dns-search search_domains ↵
```

where *search_domains* is a comma-separated list of DNS search domains

24

Enter the following to set the hostname:

```
# hostnamectl set-hostname hostname ↵
```

where *hostname* is the hostname to assign

25

Enter the following to reboot the deployer host VM:

```
# systemctl reboot ↵
```

26

Close the console session by pressing Ctrl+] (right bracket).

Install NSP Kubernetes registry

27

Log in as the root user on the NSP deployer host.

28

Enter the following:

```
# mkdir /opt/nsp ↵
```

29

Transfer the following downloaded file to the /opt/nsp directory on the NSP deployer host:

NSP_K8S_DEPLOYER_*R_r*.tar.gz

30

Enter the following:

```
# cd /opt/nsp ↵
```

31

Enter the following:

```
# tar xvf NSP_K8S_DEPLOYER_R_r.tar.gz ↵
```

where *R_r* is the NSP release ID, in the form *Major_minor*

The file is expanded, and the following directories are created:

- /opt/nsp/nsp-k8s-deployer-*release-ID*
- /opt/nsp/nsp-registry-*release-ID*

32

Enter the following:

```
# rm -f NSP_K8S_DEPLOYER_R_r.tar.gz ↵
```

The file is deleted.

33

Enter the following:

```
# cd nsp-registry-release-ID/bin ↵
```

34

Enter the following:

```
# ./nspregistryctl install ↵
```

The following prompt is displayed.

```
Enter a registry admin password:
```

35

Create a registry administrator password; the password must:

- be a minimum of 10 characters
- include at least one:
    - uppercase character
    - lowercase character
    - digit
    - special character in the following list:
      ! # $ % & ( ) * + , - . / : ; = ? @ \ ^ _ { | }

36

Enter the password.

The following prompt is displayed.

```
Confirm the registry admin password:
```

37

Re-enter the password.

The registry installation begins, and messages like the following are displayed.

```
✓ New installation detected.
✓ Initialize system.
date time Copy container images ...
date time Install/update package [container-selinux] ...
✓ Installation of container-selinux has completed.
date time Install/update package [k3s-selinux] ...
✓ Installation of k3s-selinux has completed.
date time Setup required tools ...
✓ Initialization has completed.
date time Install k3s ...
date time Waiting for up to 10 minutes for k3s initialization ...
..............................................
✓ Installation of k3s has completed.
➜ Generate self-signed key and cert.
date time Registry TLS key file:
/opt/nsp/nsp-registry/tls/nokia-nsp-registry.key
date time Registry TLS cert file:
/opt/nsp/nsp-registry/tls/nokia-nsp-registry.crt
date time Install registry apps ...
date time Waiting for up to 10 minutes for registry services to be
ready ...
```

```
..........
✓ Registry apps installation is completed.
date time Generate artifacts ...
date time Apply artifacts ...
date time Setup registry.nsp.nokia.local certs ...
date time Setup a default project [nsp] ...
date time Setup a cron to regenerate the k3s certificate [nsp] ...
✓ Post configuration is completed.
✓ Installation has completed.
```

Migrate legacy cluster parameters

38

If you are upgrading from Release 22.6, go to Step 49.

39

Enter the following:

```
# cd /opt/nsp/nsp-k8s-deployer-release-ID/tools ↵
```

40

Copy the hosts.yml file saved in Step 8 to the current directory.

41

Enter the following:

```
# ./extracthosts hosts.yml ↵
```

The current NSP cluster node entries are displayed, as shown in the following example for a three-node cluster:

```
hosts:
- nodeName: node1
nodeIp: 192.168.96.11
accessIp: 203.0.113.11
- nodeName: node2
nodeIp: 192.168.96.12
accessIp: 203.0.113.12
- nodeName: node3
nodeIp: 192.168.96.13
accessIp: 203.0.113.13
```

42

Review the output to ensure that each node entry is correct.

43

Open the following file using a plain-text editor such as vi:

/opt/nsp/nsp-k8s-deployer-*release-ID*/config/k8s-deployer.yml

44

You must configure the cluster node entries using the extracted hosts.yml file output. Table 8-1, “hosts.yml and k8s-deployer.yml parameters” (p. 246) shows the former and new parameter names, and the required value.

Configure the k8s-deployer.yml parameters shown below for each NSP cluster VM; see the descriptive text at the head of the file for parameter information, and 13.9.2 “Hostname configuration requirements” (p. 379) for general configuration information.

ℹ **Note:** The nodeName value:

- can contain only ASCII alphanumeric and hyphen characters
- cannot include an uppercase character
- cannot begin or end with a hyphen
- cannot begin with a number
- cannot include an underscore
- must end with a number

ℹ **Note:** The node order in the k8s-deployer.yml file must match the order in the hosts.yml file.

Table 8-1 hosts.yml and k8s-deployer.yml parameters

hosts.yml parameter	k8s-deployer.yml parameter	Value
node_entry_header	nodeName	node hostname
ansible_host	—	same IP address used for access_ip
ip	nodeIp	IP address; private, if NAT is used
access_ip	accessIp	IP address; public, if NAT is used

45

Configure the following parameter, which specifies whether dual-stack NE management is enabled:

Note: Dual-stack NE management can function only when the network environment is appropriately configured, for example:

- Only valid, non-link-local static or DHCPv6-assigned addresses are used.
- A physical or virtual IPv6 subnet is configured for IPv6 communication with the NEs.

```
enable_dual_stack_networks: value
```

where *value* must be set to true if the cluster VMs support both IPv4 and IPv6 addressing

46

If the existing deployment includes an RPM-based IPRC, add a node entry for the IPRC after the existing node entries.

47

If the deployment includes dedicated MDM cluster VMs, as identified in Step 22 of 8.5 “To prepare for an NSP system upgrade from Release 22.6 or earlier” (p. 232), add an entry for each identified VM.

Note: If the deployment includes the IPRC, you must add the MDM node entries after the IPRC entry.

48

Save and close the file.

Create NSP cluster VMs

49

If you are upgrading from Release 22.6, copy the k8s-deployer.yml file saved in Step 8 to the following directory on the new NSP deployer host:

/opt/nsp/nsp-k8s-deployer-*release-ID*/config

50

For each required NSP cluster VM, perform one of the following to create the VM.

Note: Each NSP cluster VM requires a hostname; you must change the default of ‘localhost’ to an actual hostname.

a. Deploy the downloaded NSP_K8S_PLATFORM_RHEL8_*yy_mm*.qcow2 disk image; perform Step 6 to Step 16 of 2.3 “To deploy an NSP RHEL qcow2 disk image” (p. 30).

b. Deploy the NSP_K8S_PLATFORM_RHEL8_*yy_mm*.ova disk image; see the documentation for your virtualization environment for information.

Note: For OVA-image deployment, it is strongly recommended that you mount the /opt directory on a separate hard disk that has sufficient capacity to allow for future expansion.

c. Manually install the RHEL OS and configure the disk partitions, as described in “Manual NSP

RHEL OS installation" (p. 251) and Chapter 2, "NSP disk setup and partitioning".

51

Perform Step 52 to Step 69 for each NSP cluster VM to configure the required interfaces.

Configure NSP cluster interfaces

52

Enter the following on the NSP deployer host to open a console session on the VM:

```
# virsh console NSP_cluster_VM ↵
```

where *NSP_cluster_VM* is the VM name

You are prompted for credentials.

53

Enter the following credentials:

- username—root
- password—*available from technical support*

A virtual serial console session opens on the NSP cluster VM.

54

Enter the following:

```
# ip a ↵
```

The available network interfaces are listed; information like the following is displayed for each:

```
if_n: if_name: LESSTHANBROADCAST,MULTICAST,UP,LOWER_UPGTRTHAN mtu 1500
qdisc mq state UP group default qlen 1000
    link/ether MAC_address
    inet IPv4_address/v4_netmask brd broadcast_address scope global
noprefixroute if_name
       valid_lft forever preferred_lft forever
    inet6 IPv6_address/v6_netmask scope link
       valid_lft forever preferred_lft forever
```

55

Record the *if_name* and *MAC_address* values of the interfaces that you intend to use.

56

Enter the following for each interface:

```
# nmcli con add con-name con_name ifname if_name type ethernet mac
MAC_address ↵
```

where

con_name is a connection name that you assign to the interface for ease of identification; for example, ClientInterface or MediationInterface

if_name is the interface name recorded in Step 55

MAC_address is the MAC address recorded in Step 55

57

Enter the following for each interface:

```
# nmcli con mod con_name ipv4.addresses IP_address/netmask ↵
```

where

con_name is the connection name assigned in Step 56

IP_address is the IP address to assign to the interface

netmask is the subnet mask to assign

58

Enter the following for each interface:

```
# nmcli con mod con_name ipv4.method static ↵
```

59

Enter the following for each interface:

```
# nmcli con mod con_name ipv4.gateway gateway_IP ↵
```

gateway_IP is the gateway IP address to assign

Note: This command sets the default gateway on the primary interface and the gateways for all secondary interfaces.

60

Enter the following for all secondary interfaces:

```
# nmcli con mod con_name ipv4.never-default yes ↵
```

61

Enter the following for each interface:

Note: You must specify a DNS name server. If DNS is not deployed, you must use a non-routable IP address as a nameserver entry.

Note: Any hostnames used in an NSP deployment must be resolved by a DNS server.

Note: An NSP deployment that uses IPv6 networking for client communication must use a hostname configuration.

```
# nmcli con mod con_name ipv4.dns nameserver_1,nameserver_2...
nameserver_n ↵
```

where *nameserver_1* to *nameserver_n* are the available DNS name servers

62

To optionally specify one or more DNS search domains, enter the following for each interface:

```
# nmcli con mod con_name ipv4.dns-search search_domains ↵
```

where *search_domains* is a comma-separated list of DNS search domains

63

Open the following file with a plain-text editor such as vi:

/etc/sysctl.conf

64

Locate the following line:

```
vm.max_map_count=value
```

65

Edit the line to read as follows; if the line is not present, add the line to the end of the file:

```
vm.max_map_count=262144
```

66

Save and close the file.

67

If you are installing in a KVM environment, enter the following:

```
# mkdir /opt/nsp ↵
```

68

Enter the following to reboot the NSP cluster VM:

```
# systemctl reboot ↵
```

69

Close the console session by pressing Ctrl+] (right bracket).

Deploy container environment

70

Log in as the root user on the NSP deployer host.

71

Open a console window.

72

You must generate an SSH key for password-free deployer host access to each NSP cluster VM.

Enter the following:

```
# ssh-keygen -N "" -f ~/.ssh/id_rsa -t rsa ↵
```

73

Enter the following for each NSP cluster VM to distribute the SSH key to the VM.

```
# ssh-copy-id -i ~/.ssh/id_rsa.pub root@address ↵
```

where *address* is the NSP cluster VM IP address

74

Enter the following:

```
# cd /opt/nsp/nsp-k8s-deployer-release-ID/bin ↵
```

75

Enter the following to create the new hosts.yml file:

```
# ./nspk8sctl config -c ↵
```

76

Enter the following to list the node entries in the new hosts.yml file:

```
# ./nspk8sctl config -l ↵
```

Output like the following example for a four-node cluster is displayed:

Note: If NAT is used in the cluster:

- The *access_ip* value is the public IP address of the cluster node.
- The *ip* value is the private IP address of the cluster node.
- The *ansible_host* value is the same value as *access_ip*

Note: If NAT is not used in the cluster:

- The *access_ip* value is the IP address of the cluster node.
- The *ip* value matches the *access_ip* value.
- The *ansible_host* value is the same value as *access_ip*

```
Existing cluster hosts configuration is:
all:
hosts:
node1:
ansible_host: 203.0.113.11
ip: ip
access_ip: access_ip
```

```
node2:
ansible_host: 203.0.113.12
ip: ip
access_ip: access_ip
node3:
ansible_host: 203.0.113.13
ip: ip
access_ip: access_ip
node4:
ansible_host: 203.0.113.14
ip: ip
access_ip: access_ip
```

77

Verify the IP addresses.

78

Enter the following to import the Kubernetes images to the repository:

```
.# ./nspk8sctl import ↵
```

79

Enter the following:

```
.# ./nspk8sctl install ↵
```

The NSP Kubernetes environment is deployed.

80

The NSP cluster member named node1 is designated the NSP cluster host for future configuration activities; record the NSP cluster host IP address for future reference.

81

Open a console window on the NSP cluster host.

82

Enter the following periodically to display the status of the Kubernetes system pods:

ℹ **Note:** You must not proceed to the next step until each pod STATUS reads Running or Completed.

```
# kubectl get pods -A ↵
```

The pods are listed.

83

Enter the following periodically to display the status of the NSP cluster nodes:

ℹ **Note:** You must not proceed to the next step until each node STATUS reads Ready.

```
# kubectl get nodes -o wide ↵
```

The NSP cluster nodes are listed, as shown in the following three-node cluster example:

```
NAME     STATUS    ROLES     AGE    VERSION    INTERNAL-IP    EXTERNAL-IP
node1    Ready     master    nd      version    int_IP    ext_IP
node2    Ready     master    nd     version    int_IP    ext_IP
node3    Ready     <none>    nd     version    int_IP         ext_IP
```

Restore NSP system configuration

84

Transfer the following downloaded file to the /opt/nsp directory on the NSP deployer host:

NSP_DEPLOYER_*R_r*.tar.gz

85

Enter the following on the NSP deployer host:

```
# cd /opt/nsp ↵
```

86

Enter the following:

```
# tar xvf NSP_DEPLOYER_R_r.tar.gz ↵
```

where *R_r* is the NSP release ID, in the form *Major_minor*

The bundle file is expanded, and the following directory of NSP installation files is created:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*

87

Enter the following:

```
# rm -f NSP_DEPLOYER_R_r.tar.gz ↵
```

The bundle file is deleted.

88

Restore the required NSP configuration files.

1. Enter the following:

   ```
   # mkdir /tmp/appliedConfig ↵
   ```

2. Enter the following:

   ```
   # cd /tmp/appliedConfig ↵
   ```

3. Transfer the following configuration backup file saved in 8.5 “To prepare for an NSP system

upgrade from Release 22.6 or earlier" (p. 232) to the /tmp/appliedConfig directory:

nspConfiguratorConfigs.zip

4. Enter the following:

```
# unzip nspConfiguratorConfigs.zip ↵
```

The configuration files are extracted to the current directory, and include some or all of the following, depending on the previous deployment:

- license file
- nsp-config.yml file
- TLS files; may include subdirectories
- SSH key files
- nsp-configurator/generated directory content

5. Copy the extracted TLS files to the following directory:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/tls

6. Enter the following:

```
# mkdir -p /opt/nsp/nsp-configurator/generated ↵
```

7. Copy all extracted nsp-configurator/generated files to the /opt/nsp/nsp-configurator/generated directory.

Label NSP cluster nodes

89

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

90

Open the following file with a plain-text editor such as vi:

/opt/nsp/NSP-CN-DEP-*release-ID*/config/nsp-deployer.yml

Configure the following parameters:

```
hosts: "hosts_file"
labelProfile: "../ansible/roles/apps/nspos-labels/vars/labels_file"
```

where

hosts_file is the absolute path of the hosts.yml file; the default is /opt/nsp/nsp-k8s-deployer-*release-ID*/config/hosts.yml

labels_file is the file name below that corresponds to your cluster deployment type:Step 73

- node-labels-basic-1node.yml
- node-labels-basic-sdn-2nodes.yml
- node-labels-enhanced-6nodes.yml
- node-labels-enhanced-sdn-9nodes.yml
- node-labels-standard-3nodes.yml

- node-labels-standard-4nodes.yml
- node-labels-standard-sdn-4nodes.yml
- node-labels-standard-sdn-5nodes.yml

91

Save and close the file.

92

Enter the following to apply the node labels to the NSP cluster:

```
# ./nspdeployerctl config ↵
```

93

Enter the following to import the NSP images and Helm charts to the NSP Kubernetes registry:

Note: The import operation may take 20 minutes or longer.

```
# ./nspdeployerctl import ↵
```

94

Open a console window on the NSP cluster host.

95

Enter the following to display the node labels:

```
# kubectl get nodes --show-labels ↵
```

Cluster node information is displayed.

96

View the information to ensure that all NSP labels are added to the cluster VMs.

Configure NSP software

97

You must merge the nsp-config.yml file content from the existing deployment into the new nsp-config.yml file.

Open the following files using a plain-text editor such as vi:

- former configuration file—/tmp/appliedConfig/nsp-config.yml file extracted in Step 88
- new configuration file—/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

Note: See 6.1.1 “nsp-config.yml file format” (p. 173) for configuration information.

98

Copy each configured parameter line from the previous nsp-config.yml file and use the line to overwrite the same line in the new file.

ℹ **Note:** You must maintain the structure of the new file, as any new configuration options for the new release must remain.

ℹ **Note:** You must replace each configuration line entirely, and must preserve the leading spaces in each line.

ℹ **Note:** If NSP application-log forwarding to NSP Elasticsearch is enabled, special configuration is required.

- OpenSearch replaces Elasticsearch as the local log-viewing utility. Consequently, the Elasticsearch configuration cannot be directly copied from the current NSP configuration to the new configuration. Instead, you must configure the parameters in the **logging**—**forwarding**—**applicationLogs**—**opensearch** section of the new NSP configuration file.
- Elasticsearch is introduced as a remote log-forwarding option. You can enable NSP application-log forwarding to a remote Elasticsearch server in the **logging**—**forwarding**—**applicationLogs**—**elasticsearch** section of the new NSP configuration file.

  See "Centralized logging" (p. 167) for more information about configuring NSP logging options.

99

Configure the following parameter in the **platform** section as shown below:

ℹ **Note:** You must preserve the lead spacing of the line.

```
  clusterHost: "cluster_host_address"
```

where *cluster_host_address* is the address of NSP cluster member node1, which is subsequently used for cluster management operations

100

Configure the **type** parameter in the **deployment** section as shown below:

```
deployment:
    type: "deployment_type"
```

where *deployment_type* is one of the parameter options listed in the section

101

If the NSP system currently performs model-driven telemetry or classic telemetry statistics collection, perform the following steps.

1. Enable the following installation option:

   ```
   id: networkInfrastructureManagement-gnmiTelemetry
   ```

2. Configure the **throughputFactor** parameter in the **nsp**—**modules**—**telemetry**—**gnmi**

section; see the parameter description in the nsp-config.yml for the required value, which is based on the management scale:

```
            throughputFactor: n
```

where *n* is the required throughput factor for your deployment

102

If all of the following are true, configure the following parameters in the **integrations** section:

- The NSP system includes the NFM-P.
- You want the NFM-P to forward system metrics to the NSP cluster.
- The NFM-P main server and main database are on separate stations:

```
nfmpDB:
  primaryIp: ""
  standbyIp: ""
```

103

If both of the following are true, configure the following parameters in the **integrations** section:

- The NSP system includes the NFM-P.
- You want the NFM-P to forward system metrics to the NSP cluster.
- The NFM-P system includes one or more auxiliary servers:

```
auxServer:
  primaryIpList: ""
  standbyIpList: ""
```

104

If the NSP system includes one or more Release 22.11 or earlier analytics servers that are not being upgraded as part of the current NSP system upgrade, you must enable NSP and analytics compatibility; otherwise, you can skip this step.

Set the **legacyPortEnabled** parameter in the **analyticsServer** subsection of the **integrations** section to true as shown below:

```
analyticsServer:
  legacyPortEnabled: true
```

105

Specify the user authorization mechanism in the **sso** section, as shown below.

```
sso:
  authMode: "mode"
```

where *mode* is one of the following:

- oauth2—default; uses a local NSP user database, and can include remote authentication servers
- cas—deprecated; uses the NFM-P or remote authentication servers for authentication

106

If you use CAS authentication and are not migrating to OAUTH2 at this time, add the required parameter sections.

Note: The parameters apply only to an NSP system that uses CAS authentication.

1. Add the following to the **nsp**—**modules**—**nspos** section of the file:

```
rest:
  session:
    ttlInMins: 60
    maxNumber: 50
```

2. Add the following to the end of the **nsp**—**sso** section:

```
authMode: "cas"
session:
  concurrentLimitsEnabled: false
  maxSessionsPerUser: 10
  maxSessionsForAdmin: 10
throttling:
  enabled: true
  rateThreshold: 3
  rateSeconds: 9
  lockoutPeriod: 5
loginFailure:
  enabled: false
  threshold: 3
  lockoutMinutes: 1
```

3. Add the required remote authentication subsections from the previous configuration to the end of the section.

107

If you have an updated license, ensure that the location of your license.zip file, as indicated in the nsp-config.yml file, is in the correct location on the NSP deployer host.

108

Save and close the new nsp-config.yml file.

109

Close the previous nsp-config.yml file.

110

If you are configuring the new standby (former primary) cluster in a DR deployment, obtain the TLS and telemetry artifacts from the NSP cluster in the primary data center.

1. Enter the following:

```
# scp root@address:
/opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tls/ca/*
/opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tls/ca/ ↵
```

2. Enter the following:

```
# scp root@address:
/opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tls/telemetry/*
/opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tls/telemetry/ ↵
```

3. Enter the following:

```
# mkdir -p /opt/nsp/nsp-configurator/generated ↵
```

4. If the primary NSP cluster is configured to use OAUTH2 authentication, enter the following:

```
# scp root@address:
/opt/nsp/nsp-configurator/generated/nsp-keycloak-*-secret
/opt/nsp/nsp-configurator/generated/ ↵
```

where *address* is the address of the NSP deployer host in the primary cluster

111

If you are upgrading the new primary (former standby) cluster in a DR deployment, stop here and return to 8.3 “Workflow for DR NSP system upgrade from Release 22.6 or earlier” (p. 226).

Restore dedicated MDM node labels

112

If you are not including any dedicated MDM nodes in addition to the number of member nodes in a standard or enhanced NSP cluster, go to Step 119.

113

Log in as the root user on the NSP cluster host.

114

Open a console window.

115

Perform the following steps for each additional MDM node.

1. Enter the following to open an SSH session as the root user on the MDM node.

   Note: The root password for a VM created using the Nokia qcow2 image is available from technical support.

```
# ssh root@MDM_node_IP_address ↵
```

2. Enter the following:

```
# mkdir -p /opt/nsp/volumes/mdm-server ↵
```

3. Enter the following:

```
# chown -R 1000:1000 /opt/nsp/volumes ↵
```

4. Enter the following:

```
# exit ↵
```

116

Enter the following:

```
# kubectl get nodes -o wide ↵
```

A list of nodes like the following is displayed.

```
NAME    STATUS   ROLES    AGE   VERSION   INTERNAL-IP
EXTERNAL-IP
node1   Ready    master   nd    version   int_IP    ext_IP
node2   Ready    master   nd    version   int_IP    ext_IP
node3   Ready    <none>   nd    version   int_IP    ext_IP
```

117

Record the NAME value of each node whose INTERNAL-IP value is the IP address of a node that has been added to host an additional MDM instance.

118

For each node, enter the following sequence of commands:

```
# kubectl label node node mdm=true ↵
# kubectl cordon node ↵
```

where *node* is the recorded NAME value of the cordoned MDM node

Deploy NSP cluster

119

Enter the following on the NSP deployer host:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

120

If you are upgrading the new standby (former primary) cluster in a DR deployment, go to Step 123.

121

If you are creating the new standalone NSP cluster, or the new primary NSP cluster in a DR deployment, you must start the cluster in restore mode; enter the following:

Note: If the NSP cluster members do not have the required SSH key, you must include the --ask-pass argument in the nspdeployerctl command, as shown in the following example, and are subsequently prompted for the root password of each host:

```
nspdeployerctl install arguments --ask-pass ↵
```

```
# ./nspdeployerctl install --config --restore ↵
```

Restore NSP data

122

If you are creating the new standalone NSP cluster, or the new primary NSP cluster in a DR deployment, you must restore the NSP databases and file service data; perform “How do I restore the NSP cluster databases?” in the *NSP System Administrator Guide*.

Start NSP

123

If you are creating the new standby cluster in a DR deployment, enter the following on the NSP deployer host:

```
# ./nspdeployerctl install --config --deploy ↵
```

The NSP starts.

Monitor NSP initialization

124

Open a console window on the NSP cluster host.

125

If you are including any MDM VMs in addition to a standard or enhanced NSP cluster deployment, perform the following steps to uncordon the nodes cordoned in Step 112.

1. Enter the following:

   ```
   # kubectl get pods -A | grep Pending ↵
   ```

   The pods in the Pending state are listed; an mdm-server pod name has the format mdm-server-*ID*.

   Note: Some mdm-server pods may be in the Pending state because the manually labeled MDM nodes are cordoned in Step 118. You must not proceed to the next step if any pods other than the mdm-server pods are listed as Pending. If any other pod is shown, re-enter the command periodically until no pods, or only mdm-server pods, are listed.

2. Enter the following for each manually labeled and cordoned node:

   ```
   # kubectl uncordon node ↵
   ```

   where *node* is an MDM node name recorded in Step 112

   The MDM pods are deployed.

   Note: The deployment of all MDM pods may take a few minutes.

3. Enter the following periodically to display the MDM pod status:

   ```
   # kubectl get pods -A | grep mdm-server ↵
   ```

4. Ensure that the number of mdm-server-*ID* instances is the same as the **mdm** clusterSize value in nsp-config.yml, and that each pod is in the Running state. Otherwise, contact technical support for assistance.

126

Monitor and validate the NSP cluster initialization.

Note: You must not proceed to the next step until each NSP pod is operational.

Note: If you are upgrading a standalone NSP system, or the primary NSP cluster in a DR deployment, the completed NSP cluster initialization marks the end of the network management outage associated with the upgrade.

1. Enter the following every few minutes:

   ```
   # kubectl get pods -A ↵
   ```

   The status of each NSP cluster pod is displayed; the NSP cluster is operational when the status of each pod is Running or Completed.

2. If the Network Operations Analytics - Baseline Analytics installation option is enabled, ensure that the following pods are listed; otherwise, see the *NSP Troubleshooting Guide* for information about troubleshooting an errored pod:

   Note: The output for a non-HA deployment is shown below; an HA cluster has three sets of three baseline pods, three rta-ignite pods, and two spark-operator pods.

   - analytics-rtanalytics-tomcat
   - baseline-anomaly-detector-*n*-exec-1
   - baseline-trainer-*n*-exec-1
   - baseline-window-evaluator-*n*-exec-1
   - rta-anomaly-detector-app-driver
   - rta-ignite-0
   - rta-trainer-app-driver
   - rta-windower-app-driver
   - spark-operator-*m*-*n*

3. If any pod fails to enter the Running or Completed state, see the *NSP Troubleshooting Guide* for information about troubleshooting an errored pod.

4. Enter the following to display the status of the NSP cluster members:

   ```
   # kubectl get nodes ↵
   ```

   The NSP Kubernetes deployer log file is /var/log/nspk8sctl.log.

127

Enter the following on the NSP cluster host to ensure that all pods are running:

```
# kubectl get pods -A ↵
```

The status of each pod is listed; all pods are running when the displayed STATUS value is Running or Completed.

The NSP deployer log file is /var/log/nspdeployerctl.log.

Verify upgraded NSP cluster operation

128

Use a browser to open the NSP cluster URL.

129

Verify the following.

- The NSP sign-in page opens.
- The NSP UI opens after you sign in.
- In a DR deployment, if the standby cluster is operational and you specify the standby cluster address, the browser is redirected to the primary cluster address.

Note: If the UI fails to open, perform “How do I remove the stale NSP allowlist entries?” in the *NSP System Administrator Guide* to ensure that unresolvable host entries from the previous deployment do not prevent NSP access.

Upgrade MDM adaptors

130

If the NSP system currently performs model-driven telemetry or classic telemetry statistics collection, you must upgrade your MDM adaptors to the latest in the adaptor suite delivered as part of the new NSP release, and install the required Custom Resources, or CRs..

Perform the following steps.

Note: Upgrading the adaptors to the latest version is mandatory in order for gNMI telemetry collection to function.

1. Upgrade the adaptor suites; see “How do I install or upgrade MDM adaptors?” in the *NSP System Administrator Guide* for information.
2. When the adaptor suites are upgraded successfully, use Artifact Administrator to install the required telemetry artifact bundles that are packaged with the adaptor suites.
   - nsp-telemetry-cr-*nodeType*-*version*.rel.*release*.ct.zip
   - nsp-telemetry-cr-*nodeType*-*version*.rel.*release*-va.zip
3. View the messages displayed during the installation to verify that the artifact installation is successful.

Synchronize auxiliary database password

131

If the NSP deployment includes an auxiliary database, perform the following steps on the NSP cluster host.

1. Enter the following:

   ```
   # cd /opt ↵
   ```

2. Enter the following:

   ```
   # sftp root@deployer_IP ↵
   ```

   where *deployer_IP* is the NSP deployer host IP address

   The prompt changes to `sftp>`.

3. Enter the following:

   ```
   sftp> cd
   /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/database ↵
   ```

4. Enter the following:

   ```
   sftp> get sync-auxdb-password.bash ↵
   ```

5. Enter the following:

   ```
   sftp> quit ↵
   ```

6. Enter the following:

   ```
   # chmod 777 sync-auxdb-password.bash ↵
   ```

7. Enter the following:

   ```
   # ./sync-auxdb-password.bash ↵
   ```

   Output like the following is displayed:

   ```
   timestamp: Synchronizing password for Auxiliary DB Output...
   timestamp: deployment.apps/tlm-vertica-output scaled
   timestamp: secret/tlm-vertica-output patched
   timestamp: deployment.apps/tlm-vertica-output scaled
   timestamp: Synchronization completed.
   ```

Perform post-upgrade tasks

132

If you uninstalled any NSP logical inventory adaptor suites in Step 23 of 8.5 “To prepare for an NSP system upgrade from Release 22.6 or earlier” (p. 232), perform the following steps.

1. Perform “How do I install or upgrade MDM adaptors?” in the *NSP System Administrator Guide* to re-install the adaptor suites.
2. Enable logical inventory polling policies in the NSP.

133

Use the NSP to monitor device discovery and to check network management functions.

134

Back up the NSP databases; perform “How do I back up the NSP cluster databases?” in the *NSP System Administrator Guide*.

135

Close the open console windows.

END OF STEPS

9 NSP system upgrade from Release 22.9 or later

9.1 Upgrading from Release 22.9 or later

9.1.1 NSP system upgrade process

CAUTION

Service Disruption

An NSP system upgrade requires a thorough understanding of NSP system administration and platform requirements, and is supported only under the conditions described in this guide, the NSP Planning Guide, and the NSP 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 NSP professional services to assess the requirements of your NSP deployment, and for information about the upgrade service, which you are strongly recommended to engage for any type of deployment.

The following workflows provide comprehensive overviews of the required upgrade activities for advance planning purposes:

- 9.2 “Workflow for standalone NSP system upgrade from Release 22.9 or later” (p. 268)
- 9.3 “Workflow for DR NSP system upgrade from Release 22.9 or later” (p. 269)

Each workflow includes links to the required procedures for completing the upgrade.

Note: An NSP system that manages a large number of NEs may require several hours, or potentially a full day for a very large network, to resynchronize the network following an NSP upgrade. It is important to consider the resynchronization time when planning a maintenance window for NSP upgrade activity.

Licensing

Your NSP system may require a new or updated license, depending on your deployment and the NSP release from which you upgrade. It is recommended that you contact Nokia early in the planning process to obtain the required license for your upgraded deployment.

Kubernetes version

The NSP requires specific Kubernetes registry and deployment software versions. The NSP cluster upgrade procedure includes steps for performing the required Kubernetes environment upgrade.

Note: Attempting to upgrade an NSP system without upgrading Kubernetes as prescribed results in failure.

You can also perform an off-cycle Kubernetes upgrade independent of an NSP software upgrade; see 5.4 “Kubernetes deployment environment” (p. 152) for information.

DR NSP system upgrade

After the preliminary upgrade preparation of each NSP cluster, the standby cluster is stopped while the primary is upgraded. Network visibility is lost during the primary cluster upgrade, as indicated in 9.3 "Workflow for DR NSP system upgrade from Release 22.9 or later" (p. 269), which lists the upgrade operations that are to be performed on each NSP cluster.

Some stages of the DR upgrade process can be performed on each cluster concurrently, for example, data and configuration backups, software downloads, and file transfers.

9.2 Workflow for standalone NSP system upgrade from Release 22.9 or later

9.2.1 Purpose

The following is the sequence of high-level actions required to upgrade a standalone Release 22.9 or later NSP system.

9.2.2 Stages

Prepare for upgrade

1

Perform 9.4 "To prepare for an NSP system upgrade from Release 22.9 or later" (p. 271) to do the following:

- back up the NSP system configuration, databases, and file service data
- download the NSP installation software
- verify the cluster readiness for the upgrade
- perform special upgrade preconfiguration

Upgrade NSP cluster

2

Perform 9.5 "To upgrade a Release 22.9 or later NSP cluster" (p. 277), which has the following step sections in the order shown below:

- "Back up NSP deployer host configuration files" (p. 277)
- "Apply OS update to NSP deployer host" (p. 278)
- "Prepare for Kubernetes upgrade" (p. 278)
- "Upgrade Kubernetes registry" (p. 279)
- "Configure Kubernetes deployer" (p. 280)
- "Update NSP cluster configuration" (p. 281)
- "Configure NSP software" (p. 283)
- "Stop and undeploy NSP cluster" (p. 287)**—marks the beginning of the network management outage**

- “Apply OS update to NSP cluster VMs” (p. 288)
- “Upgrade Kubernetes deployment environment” (p. 288)
- “Label NSP cluster nodes” (p. 289)
- “Upgrade NSP software” (p. 290)
- “Monitor NSP initialization” (p. 291)
- “Verify upgraded NSP cluster operation” (p. 292)—**marks the end of the network management outage**
- “Upgrade MDM adaptors” (p. 293)
- “Upgrade or enable additional components and systems” (p. 293)
- “Synchronize auxiliary database password” (p. 294)
- “Purge Kubernetes image files” (p. 294)
- “Restore SELinux enforcing mode” (p. 295)
- “Purge NSP image files” (p. 295)

9.3 Workflow for DR NSP system upgrade from Release 22.9 or later

9.3.1 Purpose

Table 9-1, “DR system upgrade actions, by NSP cluster” (p. 270) lists the sequence of high-level actions involved in the upgrade of a DR Release 22.9 or later NSP system. The table has a separate column for each NSP cluster.

9.3.2 Concurrent task execution

You can perform some upgrade actions on each cluster at the same time. Actions that you can perform concurrently on each cluster are in table rows that span the Primary NSP cluster and Standby NSP cluster columns.

Table 9-1 DR system upgrade actions, by NSP cluster

DR mode	Primary NSP cluster	Standby NSP cluster
DUPLEX	Perform “How do I display the NSP cluster status?” in the *NSP System Administrator Guide* to: • identify the primary and standby NSP clusters • verify the operational state of each NSP cluster	
	Perform 9.4 “To prepare for an NSP system upgrade from Release 22.9 or later” (p. 271)to do the following: • back up the NSP software configuration • download the NSP installation software • verify the cluster readiness for the upgrade • perform special upgrade preconfiguration	
	The remaining links in the table lead to step sections in 9.5 “To upgrade a Release 22.9 or later NSP cluster” (p. 277).	
	“Back up NSP deployer host configuration files” (p. 277) “Apply OS update to NSP deployer host” (p. 278) “Prepare for Kubernetes upgrade” (p. 278) “Upgrade Kubernetes registry” (p. 279) “Configure Kubernetes deployer” (p. 280) “Update NSP cluster configuration” (p. 281) “Configure NSP software” (p. 283)	
SIMPLEX		“Stop and undeploy NSP cluster” (p. 287) “Apply OS update to NSP cluster VMs” (p. 288)
OUTAGE	“Stop and undeploy NSP cluster” (p. 287) “Apply OS update to NSP cluster VMs” (p. 288) “Upgrade Kubernetes deployment environment” (p. 288) “Label NSP cluster nodes” (p. 289) “Upgrade NSP software” (p. 290) “Monitor NSP initialization” (p. 291)	

Table 9-1 DR system upgrade actions, by NSP cluster (continued)

DR mode	Primary NSP cluster	Standby NSP cluster
SIMPLEX	“Verify upgraded NSP cluster operation” (p. 292) “Upgrade MDM adaptors” (p. 293) “Upgrade or enable additional components and systems” (p. 293)	
		“Upgrade Kubernetes deployment environment” (p. 288) “Label NSP cluster nodes” (p. 289) “Upgrade NSP software” (p. 290) “Monitor NSP initialization” (p. 291) “Verify upgraded NSP cluster operation” (p. 292) “Upgrade MDM adaptors” (p. 293) “Upgrade or enable additional components and systems” (p. 293) “Synchronize auxiliary database password” (p. 294)
DUPLEX	**Note:** The simplex state persists until device discovery is complete. “Purge Kubernetes image files” (p. 294) “Restore SELinux enforcing mode” (p. 295) “Purge NSP image files” (p. 295)	

9.4 To prepare for an NSP system upgrade from Release 22.9 or later

9.4.1 Purpose

Perform this procedure to prepare for an NSP system upgrade from Release 22.9 or later.

Note: *release-ID* in a file path has the following format:

R.r.p-rel.*version*

where

R.r.p is the NSP release, in the form *MAJOR.minor.patch*

version is a numeric value

9.4.2 Steps

Back up NSP databases, system data

1

Log in as the root user on the NSP deployer host.

2

Transfer the following file to a secure location on a separate station that is unaffected by the upgrade activity:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/appliedConfigs/nspConfiguratorConfigs.zip

3

If you are upgrading a standalone NSP cluster, or the primary cluster in a DR deployment, perform “How do I back up the NSP cluster databases?” in the *NSP System Administrator Guide* for the installed release.

Note: The backup operations may take considerable time, during which you can start the software download described in Step 5.

Check current Kubernetes version

4

Record the current Kubernetes version.

1. Log in as the root user on the NSP cluster host.
2. Enter the following:

   ```
   # kubectl get nodes ↵
   ```

   NSP cluster node status information like the following is displayed:

   ```
   NAME         STATUS     ROLES                        AGE       VERSION
   node_name    status     control-plane,master         xxdnnh     version
   ```
3. Record the *version* value, which is the current Kubernetes version.
4. Compare the Kubernetes version with the supported versions for the NSP software release in the *Host Envirnoment Compatibility Guide for NSP and CLM*.

   If your current version is not supported, the procedure directs to upgrade your Kubernetes version in a later step.

Obtain installation software

5

Download the required software bundles from the NSP downloads page on the Nokia Support portal to a local station that is not affected by the upgrade activity:

Note: You must also download the .cksum file associated with each bundle file.

Note: The download takes considerable time, during which you can proceed

1. If the NSP Kubernetes version recorded in Step 4 is not supported, download the following file, which is the bundle for upgrading the Kubernetes registry and deployment environment:

   NSP_K8S_DEPLOYER_*R_r*.tar.gz

   where

   R_r is the NSP release ID, in the form *Major_minor*

   yy_mm represents the year and month of issue

2. Download one of the following RHEL OS images for creating the NSP deployer host and NSP cluster VMs:
   - NSP_K8S_PLATFORM_RHEL8_*yy_mm*.qcow2
   - NSP_K8S_PLATFORM_RHEL8_*yy_mm*.ova

3. Download the following file, which is the bundle for installing the NSP application software:

   NSP_DEPLOYER_*R_r*.tar.gz

6

Record benchmarks such as system KPIs, equipment inventories, and service lists for verification after the upgrade.

7

It is strongly recommended that you verify the message digest of each NSP image file or software bundle that you download from the Nokia Support portal. The download page includes checksums for comparison with the output of the RHEL md5sum, sha256sum, or sha512sum command.

When the bundle downloads are complete, verify each file checksum.

1. Enter the following:

   ```
   # command file ↵
   ```

   where

   command is md5sum, sha256sum, or sha512sum

   file is the name of the file to check

   A file checksum is displayed.

2. Compare the checksum value and the value in the .cksum file.

3. If the values do not match, the file download has failed. Download a new copy of the file, and then repeat this step.

Back up Elasticsearch log data

8

If log forwarding to Elasticsearch is not enabled in the NSP system, go to Step 21.

Starting in NSP Release 23.4, OpenSearch replaces Elasticsearch as the NSP log-viewing utility. If you are upgrading from an NSP release that uses Elasticsearch for viewing NSP logs, it is strongly recommended that you preserve the Elasticsearch log data collected by the NSP before you upgrade the NSP.

You can later restore the backed-up data for import by an Elasticsearch server in order to review the log data, if required, as described in “How do I restore the NSP Elasticsearch log data?” in the *NSP System Administrator Guide*.

Log in as the root user on the station that has the downloaded NSP_DEPLOYER_*R_r*.tar.gz file.

9

Navigate to the directory that contains the NSP_DEPLOYER_*R_r*.tar.gz file.

10

Enter the following:

```
# tar xvf NSP_DEPLOYER_R_r.tar.gz '*nsp-log-collector.zip'
'*README.txt' ↵
```

The nsp-log-collector.zip file and a README.txt file are extracted to the following directory path below the current directory:

NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/tools/support/logCollector

Note: The README.txt contains information about using the backup utility.

11

Log in as the root user on the NSP cluster host:

12

Open a console window.

13

Navigate to a directory that has sufficient free space for the backup log data, such as /opt.

Note: The space required for the log backup is based on the number of days for which log data is stored by the NSP, which is specified by the logRetentionPeriodInDaysOverride parameter value in the NSP cluster configuration file, and the average amount of log data per day.

14

Transfer the extracted nsp-log-collector.zip and README.txt files to the current directory.

15

In order to perform an ElasticSearch data backup, the java-1.8.0-openjdk RHEL OS package must be installed. However, the package may not be present on an earlier system.

Enter the following:

```
# yum -y install java-1.8.0-openjdk ↵
```

If the package is not installed, the yum utility installs the package. Otherwise, the utility indicates that the package is installed, and nothing is done.

16

Enter the following:

```
# unzip nsp-log-collector.zip ↵
```

The following files are created in an nsp-log-collector-*release-ID*/bin directory in the current directory:

- nsp-log-collector
- nsp-log-collector.bat

17

After the files are extracted, enter the following:

```
# cd nsp-log-collector-release-ID/bin ↵
```

18

Enter the following to back up all collected Elasticsearch log data:

```
# ./nsp-log-collector --getAll path ↵
```

where *path* is the local directory in which to store the backed-up log data

The following prompt is displayed:

```
Do you want to proceed with log collection? (y/n) :
```

19

Enter y.

The backup process begins.

The backup process creates the following .zip file in the specified *path* directory:

Logs-*timestamp*.zip

where *timestamp* is the backup creation date and fime

20

Transfer the Logs-*timestamp*.zip file for safekeeping to a secure location on a station that is not part of the NSP deployment.

Check and prepare NSP cluster

21

Perform the following steps to verify that the local NSP cluster is fully operational.

1. Log in as the root user on an NSP cluster member in the data center.

2. Enter the following to display the status of the NSP cluster nodes:

   ```
   # kubectl get nodes -A ↵
   ```

   The status of each cluster node is displayed.

   The NSP cluster is fully operational if the status of each node is Ready.

3. If any node is not in the Ready state, you must correct the condition; contact technical support for assistance, if required.

   Do not proceed to the next step until the issue is resolved.

4. Enter the following to display the NSP pod status:

   ```
   # kubectl get pods -A ↵
   ```

   The status of each pod is displayed.

   The NSP cluster is operational if the status of each pod is Running or Completed.

5. If any pod is not in the Running or Completed state, you must correct the condition; see the *NSP Troubleshooting Guide* for information about troubleshooting an errored pod.

22

Ensure that the RHEL chronyd time-synchronization service is running on each component, and that chronyd is actively tracking a central time source. See the RHEL documentation for information about using the chronyc command to view the chronyd synchronization status.

Note: NSP deployment is blocked if the chronyd service is not active.

23

Identify the dedicated MDM nodes in the NSP cluster; you require the information for restoring the cluster configuration later in the procedure.

1. Log in as the root user on any NSP cluster node.
2. Open a console window.
3. Enter the following:

   ```
   # kubectl get nodes --show-labels ↵
   ```

4. Identify the dedicated MDM nodes, which have only the following label and no other NSP labels:

   ```
   mdm=true
   ```

   For example:

   ```
   /os=linux,mdm=true
   ```

5. Record the name of each dedicated MDM node.

End of steps

9.5 To upgrade a Release 22.9 or later NSP cluster

9.5.1 Purpose

CAUTION

Network management outage

The procedure requires a shutdown of the NSP system, which causes a network management outage.

Ensure that you perform the procedure only during a scheduled maintenance period with the assistance of technical support.

Perform this procedure to upgrade a standalone or DR NSP system at Release 22.9 or later after you have performed 9.4 “To prepare for an NSP system upgrade from Release 22.9 or later” (p. 271).

Note: The following denote a specific NSP release ID in a file path;

- *old-release-ID*—currently installed release
- *new-release-ID*—release you are upgrading to

Each release ID has the following format:

R.r.p-rel.*version*

where

R.r.p is the NSP release, in the form *MAJOR.minor.patch*

version is a numeric value

9.5.2 Steps

Back up NSP deployer host configuration files

1

Log in as the root user on the NSP deployer host.

2

Open a console window.

3

Back up the following NSP Kubernetes registry certificate files:

Note: The files are in one of the following directories, depending on the release you are upgrading from:

- Release 22.9—/opt/nsp/nsp-registry-*old-release-ID*/config
- Release 22.11 or later—/opt/nsp/nsp-registry/tls

- nokia-nsp-registry.crt

- nokia-nsp-registry.key

4

Back up the following Kubernetes deployer configuration file:

/opt/nsp/nsp-k8s-deployer-*old-release-ID*/config/k8s-deployer.yml

5

Back up the following NSP deployer configuration file:

/opt/nsp/NSP-CN-DEP-*old-release-ID*/config/nsp-deployer.yml

6

Copy the files backed up in Step 3, Step 4, and Step 5 to a separate station outside the NSP cluster for safekeeping.

Disable SELinux enforcing mode

7

If SELinux enforcing mode is enabled on the NSP deployer host and NSP cluster members, you must switch to permissive mode on each; otherwise, you can skip this step.

Perform “How do I switch between SELinux modes on NSP system components?” in the *NSP System Administrator Guide* on the NSP deployer host and on each NSP cluster member.

Note: If SELinux enforcing mode is enabled on any NSP component during the upgrade, the upgrade fails.

Apply OS update to NSP deployer host

8

If the NSP deployer host is deployed in a VM created using an NSP RHEL OS disk image, perform 3.4 “To apply a RHEL update to an NSP image-based OS” (p. 67).

9

If your Kubernetes version is supported, as determined in 9.4 “To prepare for an NSP system upgrade from Release 22.9 or later” (p. 271), you do not need to upgrade Kubernetes; go to Step 24.

Prepare for Kubernetes upgrade

10

Transfer the downloaded NSP_K8S_DEPLOYER_*R*_*r*.tar.gz file to the /opt/nsp directory on the NSP deployer host.

11

Enter the following on the NSP deployer host:

```
# cd /opt/nsp ↵
```

12

Enter the following:

```
# tar -zxvf NSP_K8S_DEPLOYER_R_r.tar.gz ↵
```

The bundle file is expanded, and the following directories are created:

- /opt/nsp/nsp-registry-*new-release-ID*
- /opt/nsp/nsp-k8s-deployer-*new-release-ID*

13

After the file expansion completes successfully, enter the following to remove the file, which is no longer required:

```
# rm -f NSP_K8S_DEPLOYER_R_r.tar.gz ↵
```

14

If you are upgrading from Release 22.9, restore the Kubernetes registry certificates.

1. Enter the following on the NSP deployer host:

   ```
   # mkdir -p /opt/nsp/nsp-registry/tls ↵
   ```

2. Copy the following certificate files backed up in Step 3 to the /opt/nsp/nsp-registry/tls directory:
   - nokia-nsp-registry.crt
   - nokia-nsp-registry.key

Upgrade Kubernetes registry

15

Enter the following:

```
# cd /opt/nsp/nsp-registry-new-release-ID/bin ↵
```

16

Enter the following to begin the registry upgrade:

> **Note:** During the registry upgrade, the registry may be temporarily unavailable. During such a period, an NSP pod that restarts on a new cluster node, or a pod that starts, is in the ImagePullBackOff state until the registry upgrade completes. Any such pods recover automatically after the upgrade, and no user intervention is required.

```
# ./nspregistryctl install ↵
```

17

When the registry upgrade is complete, verify the upgrade.

1. Enter the following:

   ```
   # kubectl get nodes ↵
   ```

   NSP deployer node status information like the following is displayed:

   ```
   NAME        STATUS    ROLES                   AGE      VERSION
   node_name   status    control-plane,master    xxdnnh    version
   ```

2. Verify that *status* is Ready, and that *version* is greater than the value recorded in Step 4; do not proceed to the next step otherwise.

3. Enter the following periodically to monitor the NSP cluster initialization:

   ```
   # kubectl get pods -A ↵
   ```

   The status of each pod is displayed.

   The NSP cluster is fully operational when the status of each pod is Running or Completed.

4. If any pod fails to enter the Running or Completed state, correct the condition; see the *NSP Troubleshooting Guide* for information about troubleshooting an errored pod.

Configure Kubernetes deployer

18

Copy the k8s-deployer.yml file backed up in Step 4 to the following directory on the NSP deployer host:

/opt/nsp/nsp-k8s-deployer-*new-release-ID*/config

19

Enter the following on the NSP deployer host:

```
# cd /opt/nsp/nsp-k8s-deployer-new-release-ID/bin ↵
```

20

Enter the following to create the new hosts.yml file:

```
# ./nspk8sctl config -c ↵
```

21

Enter the following to list the node entries in the new hosts.yml file:

```
# ./nspk8sctl config -l ↵
```

Output like the following example for a four-node cluster is displayed:

Note: If NAT is used in the cluster:

- The *access_ip* value is the public IP address of the cluster node.
- The *ip* value is the private IP address of the cluster node.
- The *ansible_host* value is the same value as *access_ip*

Note: If NAT is not used in the cluster:

- The *access_ip* value is the IP address of the cluster node.
- The *ip* value matches the *access_ip* value.
- The *ansible_host* value is the same value as *access_ip*

```
Existing cluster hosts configuration is:
all:
hosts:
node1:
ansible_host: 203.0.113.11
ip: ip
access_ip: access_ip
node2:
ansible_host: 203.0.113.12
ip: ip
access_ip: access_ip
node3:
ansible_host: 203.0.113.13
ip: ip
access_ip: access_ip
node4:
ansible_host: 203.0.113.14
ip: ip
access_ip: access_ip
```

22

Verify the IP addresses.

23

Enter the following to import the Kubernetes images to the repository:

```
.# ./nspk8sctl import ↵
```

Update NSP cluster configuration

24

Transfer the following downloaded file to the /opt/nsp directory on the NSP deployer host:

NSP_DEPLOYER_*R_r*.tar.gz

25

Enter the following on the NSP deployer host:

```
# cd /opt/nsp ↵
```

26

Enter the following:

```
# tar xvf NSP_DEPLOYER_R_r.tar.gz ↵
```

The bundle file is expanded, and the following directory of NSP installation files is created:

/opt/nsp/NSP-CN-DEP-*new-release-ID*/NSP-CN-*new-release-ID*

27

Enter the following:

```
# rm -f NSP_DEPLOYER_R_r.tar.gz ↵
```

The bundle file is deleted.

28

Restore the required NSP configuration files.

1. Enter the following:

   ```
   # mkdir /tmp/appliedConfig ↵
   ```

2. Enter the following:

   ```
   # cd /tmp/appliedConfig ↵
   ```

3. Transfer the following configuration backup file saved in 9.4 “To prepare for an NSP system upgrade from Release 22.9 or later” (p. 271) to the /tmp/appliedConfig directory:

   nspConfiguratorConfigs.zip

4. Enter the following:

   ```
   # unzip nspConfiguratorConfigs.zip ↵
   ```

   The configuration files are extracted to the current directory, and include some or all of the following, depending on the previous deployment:

   - license file
   - nsp-config.yml file
   - TLS files; may include subdirectories
   - SSH key files
   - nsp-configurator/generated directory content

5. Copy the extracted TLS files to the following directory:

   /opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/tls

6. Enter the following:

   ```
   # mkdir -p /opt/nsp/nsp-configurator/generated ↵
   ```

7. Copy all extracted nsp-configurator/generated files to the /opt/nsp/nsp-configurator/generated directory.

29

Open the following file with a plain-text editor such as vi:

/opt/nsp/NSP-CN-DEP-*new-release-ID*/config/nsp-deployer.yml

Configure the following parameters:

```
hosts: "hosts_file"
labelProfile: "../ansible/roles/apps/nspos-labels/vars/labels_file"
```

where

hosts_file is the absolute path of the hosts.yml file; the default is /opt/nsp/nsp-k8s-deployer-*new-release-ID*/config/hosts.yml

labels_file is the file name below that corresponds to your cluster deployment type:Step 73

- node-labels-basic-1node.yml
- node-labels-basic-sdn-2nodes.yml
- node-labels-enhanced-6nodes.yml
- node-labels-enhanced-sdn-9nodes.yml
- node-labels-standard-3nodes.yml
- node-labels-standard-4nodes.yml
- node-labels-standard-sdn-4nodes.yml
- node-labels-standard-sdn-5nodes.yml

30

Save and close the file.

31

Enter the following to import the NSP images and Helm charts to the NSP Kubernetes registry:

Note: The import operation may take 20 minutes or longer.

```
# /opt/nsp/NSP-CN-DEP-new-release-ID/bin/nspdeployerctl import ↵
```

Configure NSP software

32

You must merge the nsp-config.yml file content from the existing deployment into the new nsp-config.yml file.

Open the following files using a plain-text editor such as vi:

- former configuration file—/opt/nsp/NSP-CN-DEP-*old-release-ID*/NSP-CN-*old-release-ID*/config/nsp-config.yml
- new configuration file—/opt/nsp/NSP-CN-DEP-*new-release-ID*/NSP-CN-*new-release-ID*/config/nsp-config.yml

Note: See 6.1.1 “nsp-config.yml file format” (p. 173) for configuration information.

Note: The following REST-session parameters in the **nsp** section of the nsp-config.yml file apply only to an NSP system that uses CAS authentication, and are not to be configured otherwise:

- ttlInMins
- maxNumber

33

Copy each configured parameter line from the previous nsp-config.yml file and use the line to overwrite the same line in the new file.

ℹ **Note:** You must maintain the structure of the new file, as any new configuration options for the new release must remain.

ℹ **Note:** You must replace each configuration line entirely, and must preserve the leading spaces in each line.

ℹ **Note:** If NSP application-log forwarding to NSP Elasticsearch is enabled, special configuration is required.

- OpenSearch replaces Elasticsearch as the local log-viewing utility. Consequently, the Elasticsearch configuration cannot be directly copied from the current NSP configuration to the new configuration. Instead, you must configure the parameters in the **logging**—**forwarding**—**applicationLogs**—**opensearch** section of the new NSP configuration file.
- Elasticsearch is introduced as a remote log-forwarding option. You can enable NSP application-log forwarding to a remote Elasticsearch server in the **logging**—**forwarding**—**applicationLogs**—**elasticsearch** section of the new NSP configuration file.

  See “Centralized logging” (p. 167) for more information about configuring NSP logging options.

34

Configure the following parameter in the **platform** section as shown below:

ℹ **Note:** You must preserve the lead spacing of the line.

```
  clusterHost: "cluster_host_address"
```

where *cluster_host_address* is the address of NSP cluster member node1, which is subsequently used for cluster management operations

35

Configure the **type** parameter in the **deployment** section as shown below:

```
deployment:
    type: "deployment_type"
```

where *deployment_type* is one of the parameter options listed in the section

36

If the NSP system currently performs model-driven telemetry or classic telemetry statistics collection, perform the following steps.

1. Enable the following installation option:

   ```
   id: networkInfrastructureManagement-gnmiTelemetry
   ```

2. Configure the **throughputFactor** parameter in the **nsp**—**modules**—**telemetry**—**gnmi** section; see the parameter description in the nsp-config.yml for the required value, which is based on the management scale:

   ```
               throughputFactor: n
   ```

   where *n* is the required throughput factor for your deployment

37

If all of the following are true, configure the following parameters in the **integrations** section:

- The NSP system includes the NFM-P.
- You want the NFM-P to forward system metrics to the NSP cluster.
- The NFM-P main server and main database are on separate stations:

```
nfmpDB:
  primaryIp: ""
  standbyIp: ""
```

38

If both of the following are true, configure the following parameters in the **integrations** section:

- The NSP system includes the NFM-P.
- You want the NFM-P to forward system metrics to the NSP cluster.
- The NFM-P system includes one or more auxiliary servers:

```
auxServer:
  primaryIpList: ""
  standbyIpList: ""
```

39

If the NSP system includes one or more Release 22.11 or earlier analytics servers that are not being upgraded as part of the current NSP system upgrade, you must enable NSP and analytics compatibility; otherwise, you can skip this step.

Set the **legacyPortEnabled** parameter in the **analyticsServer** subsection of the **integrations** section to true as shown below:

```
analyticsServer:
  legacyPortEnabled: true
```

40

Specify the user authorization mechanism in the **sso** section, as shown below.

```
sso:
  authMode: "mode"
```

where *mode* is one of the following:

- oauth2—default; uses a local NSP user database, and can include remote authentication servers
- cas—deprecated; uses the NFM-P or remote authentication servers for authentication

41

If you use CAS authentication and are not migrating to OAUTH2 at this time, add the required parameter sections.

Note: The parameters apply only to an NSP system that uses CAS authentication.

1. Add the following to the **nsp—modules—nspos** section of the file:

```
rest:
  session:
    ttlInMins: 60
    maxNumber: 50
```

2. Add the following to the end of the **nsp—sso** section:

```
authMode: "cas"
session:
  concurrentLimitsEnabled: false
  maxSessionsPerUser: 10
  maxSessionsForAdmin: 10
throttling:
  enabled: true
  rateThreshold: 3
  rateSeconds: 9
  lockoutPeriod: 5
loginFailure:
  enabled: false
  threshold: 3
  lockoutMinutes: 1
```

3. Add the required remote-authentication subsections from the previous configuration to the end of the section.

42

If you have an updated license, ensure that the location of your license.zip file, as indicated in the nsp-config.yml file, is in the correct location on the NSP deployer host.

43

Save and close the new nsp-config.yml file.

44

Close the previous nsp-config.yml file.

45

The steps in the following section align with the cluster-specific actions described in 9.3 “Workflow for DR NSP system upgrade from Release 22.9 or later” (p. 269).

If you are upgrading a standalone NSP system, go to Step 50.

DR-specific instructions

46

Perform Step 50 to Step 53 on the standby NSP cluster.

47

Perform Step 50 to Step 78 on the primary NSP cluster.

48

Perform Step 54 to Step 78 on the standby NSP cluster.

49

Perform Step 80 to Step 85 on each NSP cluster.

Stop and undeploy NSP cluster

50

Perform the following steps on the NSP deployer host to preserve the existing cluster data.

1. Open the following file using a plain-text editor such as vi:

   /opt/nsp/NSP-CN-DEP-*old-release-ID*/NSP-CN-*old-release-ID*/config/nsp-config.yml

2. Edit the following line in the **platform** section, **kubernetes** subsection to read:

   ```
   deleteOnUndeploy:false
   ```

3. Save and close the file.

51

Enter the following on the NSP deployer host to undeploy the NSP cluster:

ℹ **Note:** If you are upgrading a standalone NSP system, or the primary NSP cluster in a DR deployment, this step marks the beginning of the network management outage associated with the upgrade.

ℹ **Note:** If the NSP cluster members do not have the required SSH key, you must include the --ask-pass argument in the command, as shown in the following example, and are subsequently prompted for the common root password of each cluster member:

nspdeployerctl --ask-pass --*option* --*option* ↵

```
# /opt/nsp/NSP-CN-DEP-old-release-ID/bin/nspdeployerctl uninstall
--undeploy --clean ↵
```

The NSP cluster is undeployed.

52

On the NSP cluster host, enter the following periodically to display the status of the Kubernetes system pods:

Note: You must not proceed to the next step until the output lists only the following:

- pods in kube-system namespace
- nsp-backup-storage pod

```
# kubectl get pods -A ↵
```

The pods are listed.

Apply OS update to NSP cluster VMs

53

If the NSP cluster VMs were created using an NSP RHEL OS disk image, perform the following steps on each NSP cluster VM to apply the required OS update.

1. Log in as the root user on the VM.
2. Perform 3.4 “To apply a RHEL update to an NSP image-based OS” (p. 67) on the VM.

Upgrade Kubernetes deployment environment

54

If your Kubernetes version is supported, as determined in 9.4 “To prepare for an NSP system upgrade from Release 22.9 or later” (p. 271), go to Step 57.

See the *Host Envirnoment Compatibility Guide for NSP and CLM* for Kubernetes version-support information.

55

If you are not upgrading Kubernetes from the immediately previous version supported by the NSP, but from an earlier version, you must uninstall Kubernetes; otherwise, you can skip this step.

Enter the following on the NSP deployer host:

```
# /opt/nsp/nsp-k8s-deployer-old-release-ID/bin/nspk8sctl uninstall ↵
```

The Kubernetes software is uninstalled.

56

Enter the following on the NSP deployer host:

```
.# /opt/nsp/nsp-k8s-deployer-new-release-ID/bin/nspk8sctl install ↵
```

Note: The installation takes considerable time; during the process, each cluster node is cordoned, drained, upgraded, and uncordoned, one node at a time. The operation on each node may take 15 minutes or more.

The NSP Kubernetes environment is deployed.

Label NSP cluster nodes

57

Open a console window on the NSP cluster host.

58

Enter the following periodically to display the status of the Kubernetes system pods:

Note: You must not proceed to the next step until each pod STATUS reads Running or Completed.

```
# kubectl get pods -A ↵
```

The pods are listed.

59

Enter the following periodically to display the status of the NSP cluster nodes:

Note: You must not proceed to the next step until each node STATUS reads Ready.

```
# kubectl get nodes -o wide ↵
```

The NSP cluster nodes are listed, as shown in the following three-node cluster example:

```
NAME     STATUS    ROLES     AGE    VERSION    INTERNAL-IP    EXTERNAL-IP
node1    Ready     master    nd      version    int_IP    ext_IP
node2    Ready     master    nd     version    int_IP    ext_IP
node3    Ready     <none>    nd     version    int_IP         ext_IP
```

60

Enter the following on the NSP deployer host to apply the node labels to the NSP cluster:

```
# /opt/nsp/NSP-CN-DEP-new-release-ID/bin/nspdeployerctl config ↵
```

61

If you are not including any dedicated MDM nodes in addition to the number of member nodes in a standard or enhanced NSP cluster, go to Step 66.

62

Perform the following steps for each additional MDM node.

1. Enter the following on the NSP cluster host to open an SSH session as the root user on the MDM node.

Note: The root password for a VM created using the Nokia qcow2 image is available from technical support.

```
# ssh root@MDM_node_IP_address ↵
```

2. Enter the following:

```
# mkdir -p /opt/nsp/volumes/mdm-server ↵
```

3. Enter the following:

```
# chown -R 1000:1000 /opt/nsp/volumes ↵
```

4. Enter the following:

```
# exit ↵
```

63

Enter the following:

```
# kubectl get nodes -o wide ↵
```

A list of nodes like the following is displayed.

```
NAME    STATUS   ROLES    AGE   VERSION   INTERNAL-IP
EXTERNAL-IP
node1   Ready    master   nd    version   int_IP   ext_IP
node2   Ready    master   nd    version   int_IP   ext_IP
node3   Ready    <none>   nd    version   int_IP   ext_IP
```

64

Record the NAME value of each node whose INTERNAL-IP value is the IP address of a node that has been added to host an additional MDM instance.

65

For each node, enter the following sequence of commands:

```
# kubectl label node node mdm=true ↵
# kubectl cordon node ↵
```

where *node* is the recorded NAME value of the cordoned MDM node

Upgrade NSP software

66

If the NSP currently uses OAUTH2 authentication, you must restore the Keycloak secret files on the NSP deployer host. Otherwise, you can skip this step.

Enter the following sequence of commands as the root user on the NSP deployer host:

```
mkdir -p /opt/nsp/nsp-configurator/generated
cd /tmp/appliedConfig/opt/nsp/nsp-configurator/generated
cp nsp-keycloak-*-secret /opt/nsp/nsp-configurator/generated/
```

67

On the NSP deployer host, enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-new-release-ID/bin ↵
```

68

Enter the following:

```
# ./nspdeployerctl install --config --deploy ↵
```

The NSP starts.

Monitor NSP initialization

69

Open a console window on the NSP cluster host.

70

If you are including any MDM VMs in addition to a standard or enhanced NSP cluster deployment, perform the following steps to uncordon the nodes cordoned in Step 65.

1. Enter the following:

   ```
   # kubectl get pods -A | grep Pending ↵
   ```

   The pods in the Pending state are listed; an mdm-server pod name has the format mdm-server-*ID*.

   Note: Some mdm-server pods may be in the Pending state because the manually labeled MDM nodes are cordoned in Step 65. You must not proceed to the next step if any pods other than the mdm-server pods are listed as Pending. If any other pod is shown, re-enter the command periodically until no pods, or only mdm-server pods, are listed.

2. Enter the following for each manually labeled and cordoned node:

   ```
   # kubectl uncordon node ↵
   ```

   where *node* is an MDM node name recorded in Step 65

   The MDM pods are deployed.

   Note: The deployment of all MDM pods may take a few minutes.

3. Enter the following periodically to display the MDM pod status:

   ```
   # kubectl get pods -A | grep mdm-server ↵
   ```

4. Ensure that the number of mdm-server-*ID* instances is the same as the **mdm** clusterSize value in nsp-config.yml, and that each pod is in the Running state. Otherwise, contact technical support for assistance.

71

Monitor and validate the NSP cluster initialization.

Note: You must not proceed to the next step until each NSP pod is operational.

1. Enter the following every few minutes:

```
# kubectl get pods -A ↵
```

The status of each NSP cluster pod is displayed; the NSP cluster is operational when the status of each pod is Running or Completed.

2. If the Network Operations Analytics - Baseline Analytics installation option is enabled, ensure that the following pods are listed; otherwise, see the *NSP Troubleshooting Guide* for information about troubleshooting an errored pod:

   Note: The output for a non-HA deployment is shown below; an HA cluster has three sets of three baseline pods, three rta-ignite pods, and two spark-operator pods.

   - analytics-rtanalytics-tomcat
   - baseline-anomaly-detector-*n*-exec-1
   - baseline-trainer-*n*-exec-1
   - baseline-window-evaluator-*n*-exec-1
   - rta-anomaly-detector-app-driver
   - rta-ignite-0
   - rta-trainer-app-driver
   - rta-windower-app-driver
   - spark-operator-*m*-*n*

3. If any pod fails to enter the Running or Completed state, see the *NSP Troubleshooting Guide* for information about troubleshooting an errored pod.

4. Enter the following to display the status of the NSP cluster members:

   ```
   # kubectl get nodes ↵
   ```

   The NSP Kubernetes deployer log file is /var/log/nspk8sctl.log.

72

Enter the following on the NSP cluster host to ensure that all pods are running:

```
# kubectl get pods -A ↵
```

The status of each pod is listed; all pods are running when the displayed STATUS value is Running or Completed.

The nsp deployer log file is /var/log/nspdeployerctl.log.

Verify upgraded NSP cluster operation

73

Use a browser to open the NSP cluster URL.

74

Verify the following.

- The NSP sign-in page opens.
- The NSP UI opens after you sign in.
- In a DR deployment, if the standby cluster is operational and you specify the standby cluster address, the browser is redirected to the primary cluster address.

Note: If the UI fails to open, perform “How do I remove the stale NSP allowlist entries?” in the *NSP System Administrator Guide* to ensure that unresolvable host entries from the previous deployment do not prevent NSP access.

Upgrade MDM adaptors

75

If the NSP system currently performs model-driven telemetry or classic telemetry statistics collection, you must upgrade your MDM adaptors to the latest in the adaptor suite delivered as part of the new NSP release, and install the required Custom Resources, or CRs..

Perform the following steps.

Note: Upgrading the adaptors to the latest version is mandatory in order for gNMI telemetry collection to function.

1. Upgrade the adaptor suites; see “How do I install or upgrade MDM adaptors?” in the *NSP System Administrator Guide* for information.
2. When the adaptor suites are upgraded successfully, use Artifact Administrator to install the required telemetry artifact bundles that are packaged with the adaptor suites.
   - nsp-telemetry-cr-*nodeType-version*.rel.*release*.ct.zip
   - nsp-telemetry-cr-*nodeType-version*.rel.*release*-va.zip
3. View the messages displayed during the installation to verify that the artifact installation is successful.

Upgrade or enable additional components and systems

76

If the NSP deployment includes the VSR-NRC, upgrade the VSR-NRC as described in the VSR-NRC documentation.

77

If you are including an existing NFM-P system in the deployment, perform one of the following.

a. Upgrade the NFM-P to the NSP release; see “NFM-P system upgrade from Release 22.9 or later” (p. 819).

b. Enable NFM-P and NSP compatibility; perform 11.4 “To enable NSP compatibility with an earlier NFM-P system” (p. 333).

Note: An NFM-P system upgrade procedure includes steps for upgrading the following components in an orderly fashion:

- auxiliary database
- NSP Flow Collectors / Flow Collector Controllers
- NSP analytics servers

78

If the NSP system includes the WS-NOC, perform the appropriate procedure in “WS-NOC and NSP integration” (p. 340) to enable WS-NOC integration with the upgraded NSP system.

Synchronize auxiliary database password

79

If the NSP deployment includes an auxiliary database, perform the following steps on the NSP cluster host.

1. Enter the following:

   ```
   # cd /opt ↵
   ```

2. Enter the following:

   ```
   # sftp root@deployer_IP ↵
   ```

   where *deployer_IP* is the NSP deployer host IP address

   The prompt changes to `sftp>`.

3. Enter the following:

   ```
   sftp> cd
   /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/database ↵
   ```

4. Enter the following:

   ```
   sftp> get sync-auxdb-password.bash ↵
   ```

5. Enter the following:

   ```
   sftp> quit ↵
   ```

6. Enter the following:

   ```
   # chmod 777 sync-auxdb-password.bash ↵
   ```

7. Enter the following:

   ```
   # ./sync-auxdb-password.bash ↵
   ```

   Output like the following is displayed:

   ```
   timestamp: Synchronizing password for Auxiliary DB Output...
   timestamp: deployment.apps/tlm-vertica-output scaled
   timestamp: secret/tlm-vertica-output patched
   timestamp: deployment.apps/tlm-vertica-output scaled
   timestamp: Synchronization completed.
   ```

Purge Kubernetes image files

80

Note: Perform this and the following step only after you verify that the NSP system is operationally stable and that an upgrade rollback is not required.

Enter the following on the NSP deployer host:

```
# cd /opt/nsp/nsp-k8s-deployer-new-release-ID/bin ↵
```

81

Enter the following:

```
# ./nspk8sctl purge-registry -e ↵
```

The images are purged.

Purge NSP image files

82

Note: Perform this and the following step only after you verify that the NSP system is operationally stable and that an upgrade rollback is not required.

Enter the following on the NSP deployer host:

```
# cd /opt/nsp/NSP-CN-DEP-new-release-ID/bin ↵
```

83

Enter the following:

```
# ./nspdeployerctl purge-registry -e ↵
```

The charts and images are purged.

Restore SELinux enforcing mode

84

If either of the following is true, perform “How do I switch between SELinux modes on NSP system components?” in the *NSP System Administrator Guide* on the NSP deployer host and each NSP cluster VM.

- You switched from SELinux enforcing mode to permissive mode before the upgrade, and want to restore the use of enforcing mode.
- The upgrade has enabled SELinux in the NSP cluster for the first time, but in permissive mode, and you want the more stringent security of enforcing mode.

85

Close the open console windows.

Post-upgrade removal of path control subscriptions

86

In NSP Release 23.11, path control's internal engine - which processes flow records from the flow collector for the purpose of telemetry - was moved into a new dedicated service. If you upgraded from NSP Release 23.4 or later to NSP Release 23.11 or later - and the path control telemetry flow integration was enabled previously - the following REST API must be invoked to remove subscriptions that will no longer be used:

POST https://{{fcc}}:8443/rest/flow-collector-controller/rest/api/v1/export/unsubscribe

```
{
    "subscription" : "nrcp-sub"
}
```

END OF STEPS

10 NSP system conversion

10.1 Overview

10.1.1 Purpose

This chapter describes how to perform NSP system conversion activities that change fundamental aspects of an NSP system or the system operation.

10.1.2 Contents

10.2 Supported NSP system conversions

10.2.1 Conversion scenarios

CAUTION

Service Disruption

An NSP system conversion requires a thorough understanding of NSP system administration and platform requirements, and is supported only under the conditions described in this guide, the NSP Planning Guide, and the NSP 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 NSP professional services to assess the requirements of your NSP deployment, and for information about the upgrade service, which you are strongly recommended to engage for any type of deployment.

The workflow and procedures in this chapter address the following scenarios for changing fundamental aspects of an NSP system:

- standalone NSP system to DR
- enlarging an NSP deployment
- IPv4 NSP system to IPv6, or to IPv4 and IPv6
- single-interface NSP system to multi-interface

Note: 10.7 “Workflow for NSP system conversion to multi-interface” (p. 323) includes links to the deployment procedures in other chapters that you must perform to complete the conversion. Each other conversion scenario has a specific procedure in this chapter.

10.3 To convert a standalone NSP system to DR

10.3.1 Purpose

Perform this procedure to create a DR NSP deployment by adding an NSP cluster in a separate data center to an existing standalone deployment.

Note: Components such as the NFM-P that you intend to include in the DR deployment must also be DR systems.

The following represent the redundant data centers in the procedure:

- DC A—initial standalone data center
- DC B—data center of new DR NSP cluster

Note: You require root user privileges on each station.

Note: Command lines use the # symbol to represent the RHEL CLI prompt for the root user. Do not type the leading # symbol when you enter a command.

Note: *release-ID* in a file path has the following format:

R.r.p-rel.*version*

where

R.r.p is the NSP release, in the form *MAJOR.minor.patch*

version is a numeric value

10.3.2 Steps

Convert NFM-P to redundant system

1

If the NSP system includes a standalone NFM-P system, you must convert the NFM-P system to a redundant system; see the system conversion to redundancy procedure in “NFM-P system conversion to redundancy” (p. 1025) for information.

Note: The **nspos** ip-list parameter in samconfig on each NFM-P main server must include the advertised address of each NSP cluster.

Create NSP cluster in DC B

2

Log in as the root user on the DC B station designated for the new NSP deployer host VM.

3

Open a console window.

4

Perform the following sections of procedure 7.4 “To install the NSP” (p. 193) in DC B.

Note: The number of VMs in each NSP cluster must match.

1. “Create NSP deployer host VM” (p. 194) (Step 1 to Step 5)—creates the NSP deployer host VM in DC B

   Note: The DC B VM specifications, such as disk layout and capacity, must be identical to the DC A VM specifications.

2. “Configure NSP deployer host networking” (p. 195) (Step 6 to Step 16)—sets the NSP deployer host communication parameters
3. “Create NSP cluster VMs” (p. 199) (Step 27 to Step 48)—creates the new NSP cluster VMs

   Note: The DC B VM specifications, such as disk layout and capacity, must be identical to the DC A VM specifications.

4. “Deploy Kubernetes environment” (p. 203) (Step 49 to Step 61)—deploys the NSP cluster in DC B

Reconfigure NSP cluster in DC A

5

Log in as the root user on the NSP deployer host in DC A.

6

Open a console window.

7

Open the following file using a plain-text editor such as vi:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

8

Edit the following line in the **platform** section, **kubernetes** subsection to read as shown below:

```
deleteOnUndeploy:false
```

9

Save and close the file.

10

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

11

Enter the following to stop the NSP cluster in DC A:

```
# ./nspdeployerctl uninstall --undeploy ↵
```

The NSP cluster stops.

12

Open the following file using a plain-text editor such as vi:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

Note: See 6.1.1 “nsp-config.yml file format” (p. 173) for configuration information.

13

Configure the parameters in the **dr** section as shown below:

```
dr:
   dcName: "data_center"
   mode: "dr"
   peer: "peer_address"
   internalPeer: "peer_internal_address"
   peerDCName: "peer_data_center"
```

where

data_center is the unique alphanumeric name to assign to the DC A cluster

peer_address is the address at which the DC B cluster is reachable over the client network

peer_internal_address is the address at which the DC B cluster is reachable over the internal network

peer_data_center is the unique alphanumeric name to assign to the DC B cluster

14

Save and close the file.

15

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

16

Enter the following to start the NSP in DC A:

Note: The command causes a role-mgr pod restart to enable DR, which is not service-affecting.

```
# ./nspdeployerctl install --config --deploy ↵
```

The DC A NSP initializes in DR mode.

17

Transfer the /opt/nsp/NSP-CN--DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml file to the /tmp directory on the NSP cluster host in DC B.

18

Close the open console windows in DC A.

Configure NSP cluster in DC B

19

Log in as the root user on the NSP deployer host in DC B.

20

Open a console window.

21

Enter the following to copy the TLS security artifacts from the NSP in DC A:

```
# scp root@address:/opt/nsp/NSP-CN-release-ID/tls/*
/opt/nsp/NSP-CN-release-ID/tls/ ↵
```

where *address* is the advertised address of the NSP cluster in DC A

22

If the NSP currently uses OAUTH2 user authentication, you must copy the TLS security artifacts from the NSP in DC A.

Perform the following steps.

1. Enter the following:

   ```
   # mkdir -p /opt/nsp/nsp-configurator/generated ↵
   ```

2. Enter the following:

   ```
   # scp root@address:
   /opt/nsp/nsp-configurator/generated/nsp-keycloak-*-secret
   /opt/nsp/nsp-configurator/generated/ ↵
   ```

where *address* is the advertised address of the NSP cluster in DC A

23

Open the following file copied from DC A using a plain-text editor such as vi:

/tmp/nsp-config.yml

Note: See 6.1.1 “nsp-config.yml file format” (p. 173) for configuration information.

24

Configure the cluster addressing parameters in the **platform** section as shown below; you must specify the *client_address* value, which is used as the default for any optional address parameter that you do not configure:

Note: If the client network uses IPv6, you must specify the NSP cluster hostname as the *client_address* value.

Note: You must preserve the lead spacing of each line.

```
  advertisedAddress: "client_address"
  mediationAdvertisedAddress: "IPv4_mediation_address"
  mediationAdvertisedAddressIpv6: "IPv6_mediation_address"
  internalAdvertisedAddress: "internal_cluster_address"
```

where

client_address is the public IPv4 address or hostname that is advertised to clients

IPv4_mediation_address is the optional address for IPv4 NE management traffic

IPv6_mediation_address is the optional address for IPv6 NE management traffic

internal_cluster_address is the optional IPv4 or IPv6 address for internal NSP communication

25

Configure the parameters in the **dr** section as shown below:

```
dr:
   dcName: "data_center"
   mode: "dr"
   peer: "peer_address"
   internalPeer: "peer_internal_address"
   peerDCName: "peer_data_center"
```

where

data_center is the unique alphanumeric name of the DC B cluster

peer_address is the address at which the DC A cluster is reachable over the client network

peer_internal_address is the address at which the DC A cluster is reachable over the internal network

peer_data_center is the unique alphanumeric name of the DC A cluster

26

Save and close the file.

27

Replace the original NSP configuration file with the edited file.

1. Enter the following to create a local backup of the original file:

```
# mv
/opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/config/nsp-config.
yml nsp-config.orig ↵
```

2. Enter the following:

```
# cp /tmp/nsp-config.yml
/opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/config ↵
```

Install NSP software in DC B

28

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

29

Enter the following to deploy the NSP cluster in DC B:

```
# ./nspdeployerctl install --config --deploy ↵
```

The NSP cluster initializes as the standby cluster in the new DR deployment.

30

Enter the following every few minutes to monitor the NSP cluster initialization:

```
# kubectl get pods -A ↵
```

The status of each NSP cluster pod is displayed; the NSP cluster is operational when the status of each pod is Running or Completed. If any pod fails to enter the Running or Completed state, see the *NSP Troubleshooting Guide* for information about troubleshooting an errored pod.

Note: Some pods may remain in the Pending state; for example, MDM pods in addition to the default for a deployment.

Start NFM-P

31

Perform the following steps on each NFM-P main server station to start the server.

Note: If the NFM-P system is redundant, you must perform the steps on the primary main server first.

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.

END OF STEPS

10.4 To enlarge an NSP deployment

10.4.1 Purpose

CAUTION

System Alteration

The procedure includes operations that fundamentally reconfigure the NSP system.

You must contact Nokia support for guidance before you attempt to perform the procedure.

CAUTION

Special Deployment Limitation

Adding MDM nodes to an NSP cluster is supported only during NSP cluster installation or upgrade.

If you intend to add one or more MDM nodes after NSP deployment, contact technical support for assistance.

Perform this procedure to change an NSP deployment to a larger deployment type. Enlarging a deployment may be required, for example, to accommodate additional NSP functions, or to increase the network management growth or scope.

The operation involves the following:

- backing up the current NSP cluster configuration and data
- adding VMs to the cluster, as required
- increasing the deployment scope in the cluster configuration
- restoring the cluster data

Note: *release-ID* in a file path has the following format:

R.r.p-rel.*version*

where

R.r.p is the NSP release, in the form *MAJOR.minor.patch*

version is a numeric value

10.4.2 Rollback operation

To revert to the previous deployment type, as may be required in the event of a problem with the deployment, perform “How do I remove an NSP cluster node?” in the *NSP System Administrator Guide*.

10.4.3 Steps

Prepare required resources

1

Log in to the Nokia NSP Sizing Home page.

2

Submit an NSP Platform Sizing Request for the new deployment type.

Back up NSP databases, configuration

3

If you are expanding a standalone NSP cluster, or the primary cluster in a DR deployment, you must back up the following NSP databases; perform “How do I back up the NSP cluster databases?” in the *NSP System Administrator Guide*.

Note: Ensure that you copy each backup file to a secure location on a station outside the NSP deployment that is reachable from the NSP cluster.

- file-server-app
- nspos-postgresql
- nspos-neo4j
- nsp-tomcat
- nrcx-tomcat

Enlarge cluster, standalone deployment

4

If the NSP is a standalone deployment, go to Step 8.

Enlarge clusters, DR deployment

5

Perform Step 8 to Step 39 on the standby NSP cluster.

6

Perform Step 8 to Step 53 on the primary NSP cluster.

7

Perform Step 47 to Step 53 on the standby NSP cluster.

Uninstall NSP

8

Log in as the root user on the NSP deployer host.

9

Open a console window.

10

Transfer the following file to a secure location on a station outside the NSP cluster that is unaffected by the conversion activity.

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/appliedConfigs/nspConfiguratorConfigs.zip

11

Configure the NSP to completely remove the existing deployment.

1. Open the following file using a plain-text editor such as vi:

   /opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

2. Edit the following line in the **platform** section, **kubernetes** subsection to read as shown below:

   ```
   deleteOnUndeploy:true
   ```

3. Save and close the file.

12

Enter the following to stop the NSP cluster:

```
# /opt/nsp/NSP-CN-DEP-release-ID/bin/nspdeployerctl uninstall
--undeploy --clean ↵
```

Create new NSP cluster

13

Using the resource specifications in the response to your Platform Sizing Request, create the required new NSP cluster VMs and resize the existing VMs, as required.

Resize cluster as required

14

Identify the dedicated MDM nodes in the NSP cluster; you require the information for creating the new cluster configuration later in the procedure.

1. Log in as the root user on the NSP cluster host.
2. Open a console window
3. Enter the following:

   ```
   # kubectl get nodes --show-labels ↵
   ```

4. Identify the dedicated MDM nodes, which have only the following label and no other NSP labels:

   `mdm=true`

   For example:

   `/os=linux,mdm=true`

5. Record the name of each dedicated MDM node.

15

Log in as the root user on the NSP deployer host.

16

Open a console window.

17

Open the following file using a plain-text editor such as vi:

/opt/nsp/nsp-k8s-deployer-*release-ID*/config/k8s-deployer.yml

18

You must add each new node to the **hosts** section, as shown below.

Configure the parameters shown below for each new node; see the descriptive text at the head of the file for parameter information, and 13.9.2 “Hostname configuration requirements” (p. 379) for general configuration information.

ℹ **Note:** Any dedicated MDM nodes must be placed at the end of the hosts section. For example, if you are expanding your NSP cluster from a node-labels-standard-sdn-4nodes deployment to node-labels-standard-sdn-5nodes, the dedicated MDM nodes must be listed after node 5.

ℹ **Note:** The nodeName value:

- can contain only ASCII alphanumeric and hyphen characters
- cannot include an uppercase character
- cannot begin or end with a hyphen
- cannot begin with a number
- cannot include an underscore
- must end with a number

```
nodeName: node5
nodeIp: 192.168.98.196
```

```
accessIp: 203.0.113.5
```

19

Save and close the file.

20

Create a backup copy of the updated k8s-deployer.yml file, and transfer the backup copy to a station that is separate from the NSP system and preferably in a remote facility.

Note: The backup file is crucial in the event of an NSP deployer host failure, so must be available from a separate station.

21

Enter the following:

```
# cd /opt/nsp/nsp-k8s-deployer-release-ID/bin ↵
```

22

Enter the following to create the cluster configuration:

```
# ./nspk8sctl config -c ↵
```

The following is displayed when the creation is complete:

✔ Cluster hosts configuration is created at: /opt/nsp/nsp-k8s-deployer-*release-ID*/config/hosts.yml

23

For each NSP cluster VM that you are adding, enter the following to distribute the SSH key to the VM:

```
# ssh-copy-id -i ~/.ssh/id_rsa.pub root@address ↵
```

where *address* is the NSP cluster VM IP address

24

Enter the following:

```
# ./nspk8sctl install ↵
```

The NSP Kubernetes environment is deployed.

25

Log in as the root user on the NSP cluster host.

26

Enter the following to verify that the new node is added to the cluster:

```
# kubectl get nodes ↵
```

27

Log in as the root user on the NSP deployer host.

28

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

29

Open the following file with a plain-text editor such as vi:

/opt/nsp/NSP-CN-DEP-*new-release-ID*/config/nsp-deployer.yml

Configure the following parameters:

```
hosts: "hosts_file"
labelProfile: "../ansible/roles/apps/nspos-labels/vars/labels_file"
```

where

hosts_file is the absolute path of the hosts.yml file; the default is /opt/nsp/nsp-k8s-deployer-*new-release-ID*/config/hosts.yml

labels_file is the file name below that corresponds to your cluster deployment type:

- node-labels-basic-1node.yml
- node-labels-basic-sdn-2nodes.yml
- node-labels-enhanced-6nodes.yml
- node-labels-enhanced-sdn-9nodes.yml
- node-labels-standard-3nodes.yml
- node-labels-standard-4nodes.yml
- node-labels-standard-sdn-4nodes.yml
- node-labels-standard-sdn-5nodes.yml

30

Enter the following to apply the node labels to the NSP cluster:

```
# ./nspdeployerctl config ↵
```

31

If you are not including any dedicated MDM nodes in addition to the number of member nodes in a standard or enhanced NSP cluster, go to Step 36.

32

Perform the following steps for each additional MDM node.

1. Enter the following on the NSP cluster host to open an SSH session as the root user on the MDM node.

Note: The root password for a VM created using the Nokia qcow2 image is available from technical support.

```
# ssh root@MDM_node_IP_address ↵
```

2. Enter the following:

   ```
   # mkdir -p /opt/nsp/volumes/mdm-server ↵
   ```

3. Enter the following:

   ```
   # chown -R 1000:1000 /opt/nsp/volumes ↵
   ```

4. Enter the following:

   ```
   # exit ↵
   ```

33

Enter the following:

```
# kubectl get nodes -o wide ↵
```

A list of nodes like the following is displayed.

```
NAME    STATUS   ROLES    AGE   VERSION    INTERNAL-IP
EXTERNAL-IP

node1   Ready    master   nd   version   int_IP   ext_IP

node2   Ready    master   nd   version   int_IP   ext_IP

node3   Ready    <none>   nd   version   int_IP   ext_IP
```

34

Record the NAME value of each node whose INTERNAL-IP value is the IP address of a node that has been added to host an additional MDM instance.

35

For each node, enter the following sequence of commands:

```
# kubectl label node node mdm=true ↵

# kubectl cordon node ↵
```

where *node* is the recorded NAME value of the cordoned MDM node

36

On the NSP cluster host, enter the following:

```
# kubectl get nodes --show-labels ↵
```

37

Verify that the labels are added to the nodes.

Configure deployment

38

Perform the following steps on the NSP deployer host to update the NSP configuration.

1. Open the nsp-config.yml file backed up in Step 10 using a plain-text editor such as vi:
2. In the **deployment** subsection of the **nsp** section, configure the **type** parameter to the new deployment type configured in Step 29.
3. If the **deploy** parameter in the **platform** section, **elb** subsection is set to true, add or reconfigure nodes in the **hosts** subsection, as required.
4. Verify the file content to ensure that the configuration is correct.
5. Save and close the file.

39

Configure the NSP to preserve the deployment.

1. Open the following file on the NSP deployer host using a plain-text editor such as vi:

   /opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml
2. Edit the following line in the **platform** section, **kubernetes** subsection to read as shown below:

   ```
   deleteOnUndeploy:false
   ```
3. Save and close the file.

Deploy NSP in restore mode

40

On the NSP deployer host, enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

41

Enter the following:

```
# ./nspdeployerctl install --config --restore ↵
```

The NSP cluster is deployed in restore mode.

Restore databases

42

On the NSP deployer host, enter the following:

```
# kubectl get pods -A ↵
```

The database pods are listed.

43

Verify that the database pods are running; the number of replica pods running depends on the deployment type:

- standard, medium, or basic—one replica each of nspos-neo4j-core, nsp-tomcat, and one of nrcx-tomcat, if included in the deployment
- enhanced—three replicas each of nspos-neo4j-core and nsp-tomcat

44

Perform “How do I restore the NSP cluster databases?” in the *NSP System Administrator Guide*.

Undeploy NSP

45

On the NSP deployer host, enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

46

Enter the following:

```
# ./nspdeployerctl uninstall --undeploy ↵
```

The NSP cluster is undeployed.

Start NSP

47

Enter the following:

```
# ./nspdeployerctl install --config --deploy ↵
```

The NSP cluster is deployed, and the NSP starts.

48

On the NSP cluster host, enter the following every few minutes to display the cluster status:

Note: You must not proceed to the next step until the cluster is fully operational.

```
# kubectl get pods -A ↵
```

The status of each NSP cluster pod is displayed; the NSP cluster is operational when the status of each pod is Running or Completed, with the following exception.

- If you are including any MDM VMs in addition to a standard or enhanced NSP cluster deployment, the status of each mdm-server pod is shown as Pending, rather than Running or Completed.

49

If you are including any MDM VMs in addition to a standard or enhanced NSP cluster deployment, perform the following steps to uncordon the nodes cordoned in Step 35.

1. Enter the following:

   ```
   # kubectl get pods -A | grep Pending ↵
   ```

   The pods in the Pending state are listed; an mdm-server pod name has the format mdm-server-*ID*.

   Note: Some mdm-server pods may be in the Pending state because the manually labeled MDM nodes are cordoned in Step 35. You must not proceed to the next step if any pods other than the mdm-server pods are listed as Pending. If any other pod is shown, re-enter the command periodically until no pods, or only mdm-server pods, are listed.

2. Enter the following for each manually labeled and cordoned node:

   ```
   # kubectl uncordon node ↵
   ```

   where *node* is an MDM node name recorded in Step 35

   The MDM pods are deployed.

   Note: The deployment of all MDM pods may take a few minutes.

3. Enter the following periodically to display the MDM pod status:

   ```
   # kubectl get pods -A | grep mdm-server ↵
   ```

4. Ensure that the number of mdm-server-*ID* instances is the same as the **mdm** clusterSize value in nsp-config.yml, and that each pod is in the Running state. Otherwise, contact technical support for assistance.

50

Use a browser to open the NSP cluster URL.

51

Verify the following.

- The NSP sign-in page opens.
- The NSP UI opens after you sign in.
- In a DR deployment, if the standby cluster is operational and you specify the standby cluster address, the browser is redirected to the primary cluster address.

Note: If the UI fails to open, perform “How do I remove the stale NSP allowlist entries?” in the *NSP System Administrator Guide* to ensure that unresolvable host entries from the previous deployment do not prevent NSP access.

52

Use the NSP to monitor device discovery and to check network management functions.

53

Close the open console windows.

END OF STEPS

10.5 To convert an IPv4 NSP system to an IPv6-enabled NSP system

10.5.1 Purpose

CAUTION

System Alteration

The procedure includes operations that fundamentally reconfigure the NSP system.

You must contact Nokia support for guidance before you attempt to perform the procedure.

Perform this procedure to enable an NSP system that uses only IPv4 to use only IPv6, or IPv4 and IPv6.

10.5.2 Steps

1

Perform 8.6 “To upgrade a Release 22.6 or earlier NSP cluster” (p. 237) to upgrade the NSP system.

2

Log in as the root user on the NSP deployer host.

3

Perform the following steps to preserve the existing deployment configuration.

1. Open the following file using a plain-text editor such as vi:

   /opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

2. Edit the following line in the **platform** section, **kubernetes** subsection to read as shown below:

   ```
   deleteOnUndeploy:false
   ```

3. Save and close the file.

4

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

5

Enter the following to undeploy the NSP:

```
# ./nspdeployerctl uninstall --undeploy ↵
```

6

Open the following file using a plain-text editor such as vi:

/opt/nsp/nsp-k8s-deployer-*release-ID*/config/k8s-deployer.yml

7

Set the following parameter to true, as shown below:

Note: Dual-stack NE management can function only when the network environment is appropriately configured, for example:

- Only valid, non-link-local static or DHCPv6-assigned addresses are used.
- A physical or virtual IPv6 subnet is configured for IPv6 communication with the NEs.

```
enable_dual_stack_networks: true
```

8

Save and close the file.

9

Create a backup copy of the updated k8s-deployer.yml and transfer it to a secure location on a station that is not part of the NSP deployment.

10

Enter the following:

```
# cd /opt/nsp/nsp-k8s-deployer-release-ID/bin ↵
```

11

Enter the following:

```
# ./nspk8sctl install ↵
```

The configuration update is put into effect.

12

When the configuration update is complete, log in as the root user on the NSP cluster host.

13

Restart the coredns and dns-autoscaler pods.

1. Enter the following commands to determine how many replicas of each pod are running:

```
# kubectl describe deployments.apps coredns -n kube-system | grep Replicas ↵
```

```
# kubectl describe deployments.apps dns-autoscaler -n kube-system | grep Replicas ↵
```

2. You must set the number of coredns and dns-autoscaler pod replcas to 0, and then back to the replica count observed in substep 1.

   Enter the following sequence of commands, where initial_count is the number of replicas observed in substep 1:

   ```
   # kubectl scale deployment coredns -n kube-system --replicas=0 ↵
   ```

   ```
   # kubectl scale deployment coredns -n kube-system --replicas=
   initial_count ↵
   ```

   ```
   # kubectl scale deployment dns-autoscaler -n kube-system
   --replicas=0 ↵
   ```

   ```
   # kubectl scale deployment dns-autoscaler -n kube-system
   --replicas=initial_count ↵
   ```

14

Log in as the root user on the NSP deployer host.

15

Perform the following steps to preserve the existing deployment configuration.

1. Open the following file using a plain-text editor such as vi:

   /opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

2. Edit the file to include the required IPv6 addresses; see “IP version support” (p. 164) for information about any requirements or restrictions.

3. Save and close the file.

16

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

17

Enter the following to redeploy the NSP:

```
# ./nspdeployerctl install --config --deploy ↵
```

IPv6 communication is enabled.

18

Close the open console windows.

End of steps

10.6 To migrate from CAS to OAUTH2 NSP user authentication

10.6.1 Purpose

CAUTION

Service disruption

Performing the procedure requires a restart of each NSP cluster, which is service-affecting.

You must perform the procedure only during a scheduled maintenance period.

Nokia strongly recommends migrating from the deprecated CAS authentication mode to OAUTH2 authentication, as described in the following steps.

10.6.2 Steps

Prepare for migration

1

As required, edit NFM-P user accounts to prepare for importing to the NSP local user database; for example, remove duplicate user IDs, or enter e-mail addresses.

Note: For users whose user account includes an e-mail address, the import operation sends a new randomly generated temporary password. Users who lack an e-mail address are assigned a global temporary password.

Undeploy standby NSP cluster

2

Log in as the root user on the NSP deployer host in the standby data center.

3

Open a console window.

4

Perform the following steps to preserve the existing cluster data.

1. Open the following file using a plain-text editor such as vi:

   /opt/nsp/NSP-CN-DEP-*old-release-ID*/NSP-CN-*old-release-ID*/config/nsp-config.yml

2. Edit the following line in the **platform** section, **kubernetes** subsection to read:

   ```
   deleteOnUndeploy:false
   ```

3. Save and close the file.

5

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

6

Enter the following:

```
# ./nspdeployerctl uninstall --undeploy ↵
```

Undeploy and configure primary NSP cluster

7

Log in as the root user on the NSP deployer host in the primary data center.

8

Open a console window.

9

Perform the following steps to preserve the existing cluster data.

1. Open the following file using a plain-text editor such as vi:
   /opt/nsp/NSP-CN-DEP-*old-release-ID*/NSP-CN-*old-release-ID*/config/nsp-config.yml
2. Edit the following line in the **platform** section, **kubernetes** subsection to read:
   ```
   deleteOnUndeploy:false
   ```
3. Save and close the file.

10

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

11

Enter the following:

```
# ./nspdeployerctl uninstall --undeploy ↵
```

12

Open the following file using a plain-text editor such as vi:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

13

Configure the authMode parameter in the **sso** section, as shown below.

```
sso:
  authMode: "oauth2"
```

14

Configure other OAUTH2 parameters, as required, such as the following:

- session timeout or account lockout settings
- any NFM-P remote authentication sources that are migrating to the OAUTH2 configuration

15

Disable the CAS configuration; use a leading # symbol to comment out each CAS-specific SSO parameter line in the file.

16

Save and close the nsp-config.yml file.

17

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

18

Enter the following:

```
# ./nspdeployerctl --config --deploy ↵
```

The NSP configuration change is put into effect, and OAUTH2 authentication is enabled.

Configure standby NSP cluster

19

Copy the secret files for OAUTH2 deployment from the NSP in DC A.

1. Enter the following:

   ```
   # mkdir -p /opt/nsp/nsp-configurator/generated ↵
   ```

2. Enter the following:

   ```
   # scp root@address:
   /opt/nsp/nsp-configurator/generated/nsp-keycloak-*-secret
   /opt/nsp/nsp-configurator/generated/ ↵
   ```

where *address* is the advertised address of the NSP cluster in DC A

20

On the standby NSP deployer host, open the following file using a plain-text editor such as vi:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

21

Configure the authMode parameter in the **sso** section, as shown below.

```
sso:
  authMode: "oauth2"
```

22

Specify the same values for the OAUTH2 parameters that you configured in Step 14.

Note: The primary and standby OAUTH2 configurations must match.

23

Disable the CAS configuration; use a leading # symbol to comment out each CAS-specific SSO parameter line in the file.

24

Save and close the nsp-config.yml file.

25

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

26

Enter the following:

```
# ./nspdeployerctl --config --deploy ↵
```

The NSP configuration change is put into effect, and OAUTH2 authentication is enabled.

27

Close the open console windows.

Set OAUTH2 mode on NFM-P main servers

28

If the NSP deployment includes the NFM-P, you must configure each NFM-P main server to align with the NSP authentication mode. Otherwise, go to Step 41.

29

If the NFM-P system is redundant, perform Step 32 to Step 34 on the standby main server.

30

Perform Step 32 to Step 34 on the standalone or primary main server.

31

Go to Step 35.

32

Log in as the root user on the main server station.

33

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 to stop the main server:

   ```
   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.

5. Enter the following to switch back to the root user:

   ```
   bash$ su - ↵
   ```

34

Update the main server configuration.

1. Enter the following:

   ```
   # samconfig -m main ↵
   ```

   The following is displayed:

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

2. Enter the following:

   ```
   <main> configure nspos authMode oauth2 ↵
   ```

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

3. Enter the following:

   ```
   <main configure nspos> exit ↵
   ```

   The prompt changes to `<main>`.

4. Enter the following:

   ```
   <main> apply ↵
   ```

   The configuration is applied.

5. Enter the following:

   ```
   <main> exit ↵
   ```

   The samconfig utility closes.

Start NFM-P main servers

35

Perform the following steps on each main server to start the main server.

Note: You must perform the steps first on the standalone or primary 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 to start the main server:

   ```
   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.

5. Close the console window.

Import NFM-P users and groups

36

Sign in to the NSP as the admin user.

You are prompted to change your password.

37

Enter a new password.

The NSP UI opens.

38

Open Users and Security.

39

Perform the NFM-P user import procedure in the *NSP System Administrator Guide*.

40

Inform each imported NFM-P user of the new password sent to their e-mail address, or of the global temporary password assigned to the user account, if an e-mail address is not assigned.

41

Close the open console windows.

END OF STEPS

10.7 Workflow for NSP system conversion to multi-interface

10.7.1 Description

The following workflow describes the sequence of high-level actions that are required to convert a single-interface NSP system to a system that uses multiple network interfaces.

An NSP system can use one network for all client, internal, and mediation communication, or the system can segregate different traffic types using separate networks and network interfaces.

See 5.8 “Multi-interface configuration” (p. 165) for information about multi-interface support.

10.7.2 Stages

1

Back up the current NSP databases; perform “How do I back up the NSP cluster databases?” in the *NSP System Administrator Guide*.

2

Back up any customized system files that you need to preserve, for example, TLS certificate files and any custom data files.

3

If the NSP is deployed with OAUTH2 authentication, back up the following files to a secure location that is unaffected by the conversion activity:

- /opt/nsp/nsp-configurator/generated/nsp-keycloak-admin-secret
- /opt/nsp/nsp-configurator/generated/nsp-keycloak-client-secret

4

If you are upgrading from NSP Release 21.9 or earlier, perform the following steps to prevent the deletion of the local storage volumes.

1. Log in as the root user on the station that hosts the NSP deployer host VM.
2. Open a console window.
3. Enter the following:

```
# sed -e '/\/opt\/nsp\/volumes/ s/^#*/#/g' -i
/opt/nsp/kubespray/roles/kubernetes-apps/nspos-reset/defaults/main.
yml ↵
```

5

Perform 12.3 “To uninstall the NSP software from an NSP cluster” (p. 355).

6

Perform 12.5 “To uninstall the NSP Kubernetes registry” (p. 357).

7

Perform 7.3 “To provision the network bridge for NSP VMs” (p. 191) on each physical host to reconfigure the network bridge for KVM access to the guest VMs.

8

Install the NSP, as described in 7.4 “To install the NSP” (p. 193), with the exclusion of Step 27, which describes creating the NSP cluster VMs.

You must specify the IP addresses of the required client, internal, and network interfaces during the installation.

Note: Using the internal NSP network requires that you update the configuration of each other component to use the NSP internal address; the WS-NOC is an exception, and must use the NSP client interface address.

9

Test the converted system to verify the system operation and data integrity, as required.

11 NSP system integration

11.1 Overview

11.1.1 Purpose

This chapter describes how to add and independently deployed system as an integrated component of an NSP system.

11.1.2 Contents

Integrating other systems and the NSP

11.2 System integration support

11.2.1 Compatible systems

CAUTION

Service Disruption

Integrating another system with the NSP requires a thorough understanding of NSP system administration and platform requirements, and is supported only under the conditions described in this guide, the NSP Planning Guide, and the NSP 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 NSP professional services to assess the requirements of your NSP deployment, and for information about the upgrade service, which you are strongly recommended to engage for any type of deployment.

CAUTION

System Degradation

Attempting to integrate an incompatible system with the NSP may seriously damage the NSP or the system that you are integrating.

NSP release compatibility with other systems varies by system type; see the NSP compatibility matrix in the NSP Release Notice for information about the following:

- supported release combinations in shared-mode NSP deployments
- compatibility patches required by either system

The procedures in this chapter describe various scenarios for adding the following independent systems to an existing NSP system as integrated components:

Note: WS-NOC integration rollback procedures are also included.

- NFM-P
- WS-NOC

NFM-P and NSP integration

11.3 To integrate the NSP and NFM-P

11.3.1 Purpose

Perform this procedure to add an existing NFM-P system as an integrated component of an NSP deployment.

Note: When the NSP is integrated with an NFM-P system, the NSP UI is accessible only when the NFM-P is operational.

Note: *release-ID* in a file path has the following format:
R.r.p-rel.*version*
where
R.r.p is the NSP release, in the form *MAJOR.minor.patch*
version is a numeric value

11.3.2 Steps

Start PKI server

1

If you intend to use the PKI server, start the PKI server.

1. Log in as the root user on the NSP deployer host.
2. Open a console window.
3. Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/pki ↵
```

4. Enter the following:

```
# ./pki-server ↵
```

The PKI server starts, and the following is displayed:

```
date time Using Root CA from disk, and serving requests on port
nnnn
```

Configure NFM-P

2

Perform Step 4 to Step 13 on each NFM-P main server station.

Note: If the NFM-P system is redundant, you must perform the steps on the standby main server station first.

3

Go to Step 14.

Configure main server

4

Log in as the nsp user on the NFM-P main server station.

5

Open a console window.

6

Stop the main server, if it is running.

1. Enter the following:

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

2. Enter the following:

   ```
   bash$ ./nmsserver.bash stop ↵
   ```

3. 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.

4. Enter the following to switch to the root user:

   ```
   bash$ su ↵
   ```

5. Enter the following to display the NSP service status:

   ```
   # nspdctl status ↵
   ```

   Information like the following is displayed.

   ```
   Mode:      redundancy_mode
   Role:      redundancy_role
   DC-Role:   dc_role
   DC-Name:   dc_name
   Registry:  IP_address:port
   State:     stopped
   Uptime:    0s
   SERVICE            STATUS
   service_a          inactive
   service_b          inactive
   service_c          inactive
   ```

You must not proceed to the next step until all NSP services are stopped; if the State is not ‘stopped’, or the STATUS indicator of each listed service is not ‘inactive’, repeat this substep.

7

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

8

Configure the NFM-P to use the NSP nspOs instance.

1. Enter the following:

   ```
   <main> configure nspos ip-list cluster1_advertised_address;
   cluster2_advertised_address ↵
   ```

   where

   cluster1_advertised_address and *cluster2_advertised_address* are the advertised addresses of the NSP clusters specified in the NSP configuration file

   For example, specify only one IP address for a standalone NSP system, or two, separated by a semicolon, for a DR deployment.

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

2. Enter the following:

   ```
   <main configure nspos> exit ↵
   ```

   The prompt changes to `<main>`.

9

If you are using the PKI server, perform the following steps.

1. Enter the following:

   ```
   <main> configure tls pki-server server ↵
   ```

   where *server* is the PKI server IP address or hostname

2. Enter the following sequence of commands by copying and pasting at the CLI:

   ```
   no keystore-file
   no keystore-pass
   no truststore-file
   no truststore-pass
   regenerate-certs
   exit
   ```

10

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

Note: Applying the configuration may take up to ten minutes.

11

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

12

Enter the following to switch back to the nsp user:

```
# exit ↵
```

13

If you want to enable mTLS for internal Kafka authentication using two-way TLS, perform the following steps.

Note: Enabling mTLS for internal Kafka authentication is supported only in an NSP deployment that uses separate interfaces for internal and client communication.

Note: The parameter you must configure is displayed only:

- if the ip-list parameter is set to a remote address
- after the configuration is initially applied in a subsequent step

Note: The parameter is configurable only if the **secure** and **internal-certs** parameters in the **nspos** section are set to true.

1. Enter the following:

   ```
   # samconfig -m main ↵
   ```

   The following is displayed:

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

2. Enter the following:

   ```
   # configure nspos mtls-kafka-enabled back ↵
   ```

3. Enter the following:

   ```
   <main> apply ↵
   ```

   The configuration is applied.

4. Enter the following:

   ```
   <main> exit ↵
   ```

The samconfig utility closes.

Start main servers

14

Perform the following steps on each main server to start the server.

Note: If the NFM-P system is redundant, you must perform the steps on the primary main server first.

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.

Stop PKI server

15

If the PKI server is running, press Ctrl+C in the NSP deployer host console window to stop the PKI server.

Add NFM-P to NSP configuration

16

Log in as the root user on the NSP deployer host.

17

Open the following file using a plain-text editor such as vi:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

18

Configure the parameters in the **integration** section, **nfmp** subsection, as shown below:

Note: If the NFM-P system is standalone, you do not need to configure the `standbyIp` parameter.

Note: In the **client** section of samconfig on the NFM-P main servers, if the address for client access is set using the **hostname** parameter, the **primaryIp** and **standbyIp** values in the **nfmp** section of the NSP configuration file, nsp-config.yml, must be set to hostnames.
Likewise, if the **public-ip** parameter in the **client** section is configured on the main servefr, the **primaryIp** and **standbyIp** values in the nsp-config.yml file must be set to IP addresses.

```
integrations:
   nfmp:
     primaryIp: "server_1_address"
     standbyIp: "server_2_address"
     tlsEnabled: value
```

where

server_1_address is the IP address of the standalone main server, or the primary main server in a redundant NFM-P system

server_2_address is the IP address of the standby main server in a redundant NFM-P system

value is true or false

19

If all of the following are true, configure the following parameters in the **integrations** section:

- The NSP system includes the NFM-P.
- You want the NFM-P to forward system metrics to the NSP cluster.
- The NFM-P main server and main database are on separate stations:

```
nfmpDB:
  primaryIp: ""
  standbyIp: ""
```

20

If both of the following are true, configure the following parameters in the **integrations** section:

- The NSP system includes the NFM-P.
- You want the NFM-P to forward system metrics to the NSP cluster.
- The NFM-P system includes one or more auxiliary servers:

```
auxServer:
  primaryIpList: ""
  standbyIpList: ""
```

21

Save and close the file.

Redeploy NSP

22

Enter the following:

```
# /opt/nsp/NSP-CN-DEP-release-ID/bin/nspdeployerctl install --config
--deploy ↵
```

23

Close the open console windows.

END OF STEPS

11.4 To enable NSP compatibility with an earlier NFM-P system

11.4.1 Purpose

In an NSP deployment that includes an NFM-P system at an earlier release, you may need to perform specific actions to enable NSP and NFM-P compatibility.

Note: If OAUTH2 authentication mode is enabled in the NSP, you must apply an NFM-P Service Pack to the older NFM-P system to enable integration of the systems. Ensure that you follow the required Service Pack instructions before you perform this procedure.

Note: NSP release compatibility varies by system type; see the NSP compatibility matrix in the *NSP Release Notice* for the supported release combinations.

Perform this procedure to enable mixed-release NSP and NFM-P compatibility if your NSP deployment includes an NFM-P system at one of the following releases:

- 21.11
- 22.3
- 22.6
- 22.9
- 22.11
- 23.4
- 23.8

Note: *release-ID* in a file path has the following format:
R.r.p-rel.*version*
where
R.r.p is the NSP release, in the form *MAJOR.minor.patch*
version is a numeric value

11.4.2 Steps

CAUTION

Service disruption

Modifying the system configuration may have serious consequences that include service disruption. It is strongly recommended that you perform the procedure only with the assistance of technical support.

Contact your technical support representative before you attempt to perform the procedure.

1

Perform the following steps on each main server station to transfer the patch files for the NFM-P release from the NSP.

Note: In a redundant NFM-P system, it is recommended to perform the steps on the primary main server station first.

1. Log in as the root user on the station.
2. Open a console window.
3. Enter the following:

```
# mkdir -p /opt/nsp/patches ↵
```

4. Enter the following:

```
# scp -rp root@address:
/opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/src/ansible/roles/
config/files/compatibility/nfmp/NFMP_R_r/* /opt/nsp/patches/ ↵
```

where

address is the address of the NSP deployer host

R_r is the release of the NFM-P system

2

Perform the following steps on each main server station to stop the server.

Note: In a redundant NFM-P system, you must perform the steps on the standby main server station first.

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 to stop the main server:

```
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.

5. Enter the following to switch back to the root user:

```
bash$ su - ↵
```

6. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to display the nspOS service status:

```
# nspdctl status ↵
```

Information like the following is displayed.

```
Mode:      redundancy_mode
Role:      redundancy_role
DC-Role:   dc_role
DC-Name:   dc_name
Registry:  IP_address:port
State:     stopped
Uptime:    0s
SERVICE             STATUS
service_a           inactive
service_b           inactive
service_c           inactive
```

You must not proceed to the next step until all NSP services are stopped; if the State is not ‘stopped’, or the STATUS indicator of each listed service is not ‘inactive’, repeat this substep.

3

If the NFM-P is at Release 22.6, 22.9, or 22.11, go to Step 6.

4

If the NFM-P is at Release 23.4 or 23.8, go to Step 7.

5

Apply the compatibility patch to a Release 21.11 or 22.3 NFM-P system.

Note: In a redundant NFM-P system, you must perform the steps on each main server station.

Perform each action in Table 11-1, “Compatibility actions, NFM-P Release 21.11 or 22.3” (p. 336) by executing the commands associated with the action.

To facilitate the command execution, you can copy a command block and paste the block into the console window.

Table 11-1 Compatibility actions, NFM-P Release 21.11 or 22.3

Action and commands
1. Create backup directories
mkdir -p /opt/nsp/patches/backup/alu_orbw mkdir -p /opt/nsp/patches/backup/nms mkdir -p /opt/nsp/patches/backup/nspos
2. Back up Orbweaver files
cd /opt/nsp/nms/lib/alu_orbw cp equipment-model-avro.jar /opt/nsp/patches/backup/alu_orbw/ cp fm-model-avro.jar /opt/nsp/patches/backup/alu_orbw/ cp service-model-avro.jar /opt/nsp/patches/backup/alu_orbw/
3. Back up nspos adapter files
cd /opt/nsp/nms/lib/nspos cp nms_nspos_equipment_model_adapter.jar /opt/nsp/patches/backup/nspos/ cp nms_nspos_fm_model_adapter.jar /opt/nsp/patches/backup/nspos/ cp nms_nspos_model_adapter.jar /opt/nsp/patches/backup/nspos/ cp nms_nspos_service_model_adapter.jar /opt/nsp/patches/backup/nspos/
4. Back up trackedClasses.properties file
cd /opt/nsp/nms/config cp trackedClasses.properties /opt/nsp/patches/backup/nms
5. Apply compatibility-patch files
cd /opt/nsp/patches chown nsp:nsp * cp -p equipment-model-avro.jar /opt/nsp/nms/lib/alu_orbw/ cp -p fm-model-avro.jar /opt/nsp/nms/lib/alu_orbw/ cp -p service-model-avro.jar /opt/nsp/nms/lib/alu_orbw/ cp -p nms_nspos_equipment_model_adapter.jar /opt/nsp/nms/lib/nspos/ cp -p nms_nspos_fm_model_adapter.jar /opt/nsp/nms/lib/nspos/ cp -p nms_nspos_model_adapter.jar /opt/nsp/nms/lib/nspos/ cp -p nms_nspos_service_model_adapter.jar /opt/nsp/nms/lib/nspos/ cp -p trackedClasses.properties /opt/nsp/nms/config

6

Apply the compatibility patch to a Release 22.6, 22.9, or 22.11 NFM-P system.

Note: In a redundant NFM-P system, you must perform the steps on each main server station.

Perform each action in Table 11-2, “Compatibility actions, NFM-P Releases 22.6, 22,9, and 22.11” (p. 336) by executing the commands associated with the action.

To facilitate the command execution, you can copy a command block and paste the block into the console window.

Table 11-2 Compatibility actions, NFM-P Releases 22.6, 22,9, and 22.11

Action and commands
1. Create backup directories
mkdir -p /opt/nsp/patches/backup/alu_orbw mkdir -p /opt/nsp/patches/backup/nms mkdir -p /opt/nsp/patches/backup/nspos
2. Back up Orbweaver files
cd /opt/nsp/nms/lib/alu_orbw cp equipment-model-avro.jar /opt/nsp/patches/backup/alu_orbw/ cp service-model-avro.jar /opt/nsp/patches/backup/alu_orbw/
3. Back up nspos adapter files
cd /opt/nsp/nms/lib/nspos cp nms_nspos_equipment_model_adapter.jar /opt/nsp/patches/backup/nspos/ cp nms_nspos_model_adapter.jar /opt/nsp/patches/backup/nspos/ cp nms_nspos_service_model_adapter.jar /opt/nsp/patches/backup/nspos/
4. Back up trackedClasses.properties file
cd /opt/nsp/nms/config cp trackedClasses.properties /opt/nsp/patches/backup/nms
5. Apply compatibility-patch files
cd /opt/nsp/patches chown nsp:nsp * cp -p equipment-model-avro.jar /opt/nsp/nms/lib/alu_orbw/ cp -p service-model-avro.jar /opt/nsp/nms/lib/alu_orbw/ cp -p nms_nspos_equipment_model_adapter.jar /opt/nsp/nms/lib/nspos/ cp -p nms_nspos_model_adapter.jar /opt/nsp/nms/lib/nspos/ cp -p nms_nspos_service_model_adapter.jar /opt/nsp/nms/lib/nspos/ cp -p trackedClasses.properties /opt/nsp/nms/config

7

Apply the compatibility patch to a Release 23.4 or 23.8 NFM-P system.

Note: In a redundant NFM-P system, you must perform the steps on each main server station.

Perform each action in Table 11-3, “Compatibility actions, NFM-P Releases 23.4 and 23.8” (p. 337) by executing the commands associated with the action.

To facilitate the command execution, you can copy a command block and paste the block into the console window.

Table 11-3 Compatibility actions, NFM-P Releases 23.4 and 23.8

Action and commands
1. Create backup directories
mkdir -p /opt/nsp/patches/backup/alu_orbw mkdir -p /opt/nsp/patches/backup/nms mkdir -p /opt/nsp/patches/backup/nspos
2. Back up Orbweaver files
cd /opt/nsp/nms/lib/alu_orbw cp equipment-model-avro.jar /opt/nsp/patches/backup/alu_orbw/ cp service-model-avro.jar /opt/nsp/patches/backup/alu_orbw/
3. Back up nspos adapter files
cd /opt/nsp/nms/lib/nspos cp nms_nspos_equipment_model_adapter.jar /opt/nsp/patches/backup/nspos/ cp nms_nspos_service_model_adapter.jar /opt/nsp/patches/backup/nspos/
4. Back up trackedClasses.properties file
cd /opt/nsp/nms/config cp trackedClasses.properties /opt/nsp/patches/backup/nms
5. Apply compatibility-patch files
cd /opt/nsp/patches chown nsp:nsp * cp -p equipment-model-avro.jar /opt/nsp/nms/lib/alu_orbw/ cp -p service-model-avro.jar /opt/nsp/nms/lib/alu_orbw/ cp -p nms_nspos_equipment_model_adapter.jar /opt/nsp/nms/lib/nspos/ cp -p nms_nspos_service_model_adapter.jar /opt/nsp/nms/lib/nspos/ cp -p trackedClasses.properties /opt/nsp/nms/config

8

Start each NFM-P main server.

Note: In a redundant NFM-P system, you must perform this step on the primary main server station first.

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 to start the main server:

   ```
   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.

5. Close the console window.

END OF STEPS

WS-NOC and NSP integration

11.5 To enable WS-NOC compatibility with an NSP system

11.5.1 Purpose

Perform this procedure to ensure compatibility with a Release 21.12, 22.6, 22.12, 23.6, or 23.12 WS-NOC system in your NSP deployment. NSP release compatibility varies by system type; see the NSP compatibility matrix in the *NSP Release Notice* for the release combinations that are supported in shared-mode deployments, including any release-specific patches that the WS-NOC may require.

Note: The WS-NOC supports only IPv4, so can be integrated only with an NSP system that uses IPv4 in the client and internal networks.

Note: If integrating with WS-NOC version 21.12 or later, the secure parameter in the **nspos** block of the configuration file must be set to “true” in order for the NSP and WS-NOC to interoperate, and all other components in the deployment must also be installed in secure mode.

11.5.2 Steps

1

If the **secure** parameter in the **nspos** section of the NSP configuration file is set to true, perform the following steps in each data center to enable deprecated TLS version support:

1. Log in as the root user on the NSP deployer host.
2. Open the following file using a plain-text editor such as vi:

   /opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml
3. Locate the nspos section, which resembles the following:

   ```
   nspos:
     secure: true
   ```
4. Edit the section to read as follows:

   ```
   nspos:
     secure: true
   ```
5. Save and close the nsp-config.yml file.
6. Enter the following to put the changes into effect:

   ```
   # /opt/nsp/NSP-CN-DEP-release-ID/bin/nspdeployerctl install
   --config --deploy ↵
   ```

2

Note: In a redundant WS-NOC system, you must perform the steps on each WS-NOC server.

Login to the mnc-fm container on the WS-NOC VM and execute the following command:

```
docker exec -it mnc-fm bash
```

3

Open the /nfmt/instance/nfmt-adapters/config/NfmtAdapter.properties file.

4

Perform one of the following:

a. If integrating with a 21.12 WS-NOC system, modify the following attributes to read as follows:

```
EQUIPMENT_ENABLED=true

SERVICE_ENABLED=true
```

b. If integrating with a 22.6 WS-NOC system, modify the following attributes to read as follows:

```
EQUIPMENT_ENABLED=true
SERVICE_ENABLED=true
FMADAPTER_VERSION=21.6.0-rel
EQUIPMENTADAPTER_VERSION=22.6.0-rel
SERVICEADAPTER_VERSION=22.6.0-rel
```

c. If integrating with a 22.12 WS-NOC system, modify the following attributes to read as follows:

```
EQUIPMENT_ENABLED=true
SERVICE_ENABLED=true
FMADAPTER_VERSION=21.6.0-rel
EQUIPMENTADAPTER_VERSION=22.6.0-rel
SERVICEADAPTER_VERSION=22.11.0-rel
```

d. If integrating with a 23.6 or 23.12 WS-NOC system, modify the following attributes to read as follows:

```
EQUIPMENT_ENABLED=true
SERVICE_ENABLED=true
FMADAPTER_VERSION=21.6.0-rel
EQUIPMENTADAPTER_VERSION=23.4.0-rel
SERVICEADAPTER_VERSION=23.4.0-rel
```

5

Copy the file into the following directory. Execute:

```
mkdir -p /nfmt/config/tempcustom/nfmt/instance/nfmt-adapters/config
```

```
cp /nfmt/instance/nfmt-adapters/config/NfmtAdapter.properties
/nfmt/config/tempcustom/nfmt/instance/nfmt-adapters/config/
```

6

Restart Nfmt-Adapters. Perform one of the following:

a. If you are integrating a Release 21.12 or 22.6 WS-NOC system, perform the following:

   1. Stop Nfmt-Adapters. Execute:

      ```
      pkill -f Nfmt-Adapters
      ```

   2. Start Nfmt-Adapters. Execute:

      ```
      /umc/plat/script/mngApp startup Nfmt-Adapters
      ```

b. If you are integrating a Release 22.12 or later WS-NOC system, restart NSP-Adapters. Execute:

   ```
   pkill -f NSP-Adapters
   ```

   Note: The NSP-Adapters process will start automatically.

7

If the NSP was installed using FQDN, the FQDN of the NSP should be updated in the /<installroot>/config/bench/fqdn.cfg file before integrating with WS-NOC. The format is as follows:

nsp-a;<nsp-a alias>;<nsp-a IPv4 address>

nsp-b;<nsp-b alias>;<nsp-b IPv4 address>

where

nsp-a alias is the alias of the primary NSP cluster

nsp-a IPv4 address is the IPv4 address of the primary NSP cluster

nsp-b alias is the alias of the standby NSP cluster

nsp-b IPv4 address is the IPv4 address of the standby NSP cluster

End of steps

11.6 To map external user groups to predefined WS-NOC roles

11.6.1 Purpose

In shared-mode deployments that include the WS-NOC product, nspOS is hosted on the NSP cluster rather than the WS-NOC server. When the CAS authenticates a user against an authentication source, and that user needs access to WS-NOC, that user group property needs to be mapped to an WS-NOC predefined role (except for read-only viewer access).

11.6.2 Steps

1

Install the WS-NOC with “External LDAP” bench option. This tells the WS-NOC to read from the following file in order to convert external user groups into WS-NOC defined authorization profiles:

/opt/hpws/tomcat/webapps/oms1350/WEB-INF/classes/ext-aut-map.properties

See the *WS-NOC Installation Guide*; Appendix E - Remote authentication; “External LDAP configuration” for more information.

2

Configure an LDAP server in the WS-NOC bench options.

Note: In a shared-mode deployment that includes the WS-NOC, LDAP server properties are not used by WS-NOC or CAS.

3

After installing the WS-NOC product, navigate to the */opt/hpws/tomcat/webapps/oms1350/WEB-INF/classes/* directory and create the *ext-auth-map.properties* file with the appropriate mapping between the external user groups returned by the CAS, to the predefined WS-NOC profiles.

The following is an example of the file contents:

```
extldap.defaultprofile=Viewer
profile.map.num=8
extauth.map.1.extrole=Administrator
extauth.map.1.profile=Administrator
extauth.map.2.extrole=RadiusGroup
extauth.map.2.profile=Constructor
extauth.map.3.extrole=Operator
extauth.map.3.profile=Operator
extauth.map.4.extrole=Viewer
extauth.map.4.profile=Viewer
extauth.map.5.extrole=ldapadmin
extauth.map.5.profile=Administrator
extauth.map.6.extrole=ldapconstruct
extauth.map.6.profile=Constructor
extauth.map.7.extrole=ldapoper
extauth.map.7.profile=Operator
extauth.map.8.extrole=ldapviewer
extauth.map.8.profile=Viewer
```

where

extrole is the external user group property that is returned by the CAS

profile is the predefined WS-NOC role

RadiusGroup is the group, configured within the RADIUS server, that is returned upon successful authentication

See the *WS-NOC Installation Guide*; Appendix E - Remote authentication; “Post Installation actions” for more information.

4

Configure or install the nspOS instance (NSP cluster) to reference the needed authentication sources (RADIUS, AD, LDAP, and so on).

End of steps

11.7 To install the NSP templates for NSP service management on the NFM-P

11.7.1 Purpose

In order to use NSP's service management function to create PCC-initiated LSPs on NFM-P-managed NEs, you must install a set of NSP XML templates on the NFM-P.

Perform this procedure to install the required NSP XML templates on the NFM-P.

11.7.2 Steps

1

Log in as the root user on the NSP cluster host in the standalone or primary data center.

2

Enter the following to copy the templates from the nsp-tomcat pod to the local file system:

```
# kubectl cp  -n $(kubectl get pods -A | awk '/nsp-tomcat/
{print$2;exit}')  nsp-tomcat-default-0:
/opt/nsp/configure/nfmpTemplates /opt/nfmpTemplates -c nsp-tomcat ↵
```

3

Create the following directory on the NFM-P main server:

/opt/nsp/configure/nfmpTemplates

4

Transfer the contents of the /opt/nfmpTemplates directory on the NSP cluster host to the /opt/nsp/configure/nfmpTemplates directory on the NFM-P main server.

5

Open the /opt/nsp/configure/nfmpTemplates/README file on the main server station.

6

Follow the instructions in the README file to install the templates.

END OF STEPS

11.8 To integrate a containerized Release 21.12, 22.6, 22.12, 23.6, or 23.12 WS-NOC and the NSP

11.8.1 Purpose

Perform this procedure to add the NSP clusters to a containerized Release 21.12, 22.6, 22.12, 23.6, or 23.12 WS-NOC system, or to add a containerized Release 21.12, 22.6, 22.12, 23.6, or 23.12 WS-NOC system to an existing NSP deployment.

Integrated NSP and WS-NOC systems must be at compatible releases. NSP release compatibility with other systems varies; see the NSP compatibility matrix in the *NSP Release Notice* for the supported release combinations in shared-mode deployments.

Note: The WS-NOC supports only IPv4, so can be integrated only with an NSP system that uses IPv4 in the client and internal networks.

Note: For a shared-mode deployment, Nokia recommends that you use a common root CA in order to ensure trust among the components.

Note: *release-ID* in a file path has the following format:

R.r.p-rel.*version*

where

R.r.p is the NSP release, in the form *MAJOR.minor.patch*

version is a numeric value

CAUTION

Service Disruption

Performing the procedure requires stopping and starting the WS-NOC, which is service-affecting.

Perform the procedure only during a maintenance period of low network activity.

CAUTION

Data loss

Adding an WS-NOC system to an existing deployment that includes an NSP cluster does not restore the Neo4j or PostgreSQL databases from the WS-NOC system. The WS-NOC system is synchronized with the NSP, after which manual actions are required to recreate the data.

When the integration is complete, you must recreate the WS-NOC system and user settings in the NSP.

Note: You require *root* and *nsp* user privileges on each WS-NOC server station and each NSP cluster host 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

Note: Ensure that the “IPCalc” package is installed on all VMs that will host any WS-NOC software.

11.8.2 Before you begin

If the containerized WS-NOC 21.12, 22.6, or 22.12 system was deployed in HA mode, Step 13 through Step 23 must be performed on both the primary and standby servers in the following order:

- Integrate standby WS-NOC server (for example, Site2)
- Perform WS-NOC switchover (Site1 -> Site2)
- Integrate Site1 (which is now standby)

11.8.3 Steps

1

Perform one of the following:

a. If integrating a WS-NOC system at Release 22.6, 22.12, 23.6, or 23.12 continue to Step 2.

b. If integrating a WS-NOC system at a release earlier than 22.6, go to Step 13.

Integrate WS-NOC Release 22.6, 22.12, 23.6, or 23.12 with the NSP

2

Ensure that the WS-NOC Release 22.6, 22.12, 23.6, or 23.12 system is running and operational.

3

Log in to the WS-NOC server as the root user.

4

Perform the following steps.

1. Open the following file with a plain-text editor such as vi:

   install_dir/config/bench/configuration.json
2. Set the remoteAuthentication.active parameter to "nsp".
3. Set the remoteAuthentication.nsp.noc.ipv4 or remoteAuthentication.noc.ipv6 parameter using the NSP client network IP address, depending on the WS-NOC IP version in use.
4. Set the remoteAuthentication.nsp.noc.alias parameter to the NSP alias.
5. If the NSP is a DR deployment, configure the parameters in the remoteAuthentication.drc section.

Note: When NSP is set as the authentication server for WS-NOC, a corresponding user with the required permissions must be created on WS-NOC application for each user created on NSP. See the *WS-NOC Administration Guide* for information about user management on WS-NOC.

5

Perform one of the following:

a. If you are using customer-provided certificates, perform the following on WS-NOC server:

1. Verify that the customer-provided certificate is usable. Execute:

```
# cd /<installroot>/setup/config/httpscertificates/data ↵
# openssl req -noout -text -in nfmt-CSR-certificate.pem ↵
```

2. Verify that the customer-provided certificate is properly signed by CustomerCACertificate. Execute:

```
# cd /<installroot>/setup/config/httpscertificates ↵
# openssl verify -CAfile CustomerCACertificate CustomerCertificate
↵
```

   The returned result should be 'OK'.

3. `# cp /<installroot>/setup/config/httpscertificates/CustomerC* /tmp ↵`
4. `# scp root@<NSP_DEPLOYER_IP>: /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tls/ca_internal* /tmp ↵`
5. `# cd /tmp ↵`
6. `# tar cvf nspca.tar CustomerCACertificate CustomerCertificate ca_internal.key ca_internal.pem ↵`
7. `# cp nspca.tar /nokia ↵`

b. If you are using NSP-generated TLS certificates, transfer the certificates to the WS-NOC server:

1. Log in as the root user on the NSP deployer node.
2. Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tls/ca ↵
```

3. Enter the following:

```
# tar cvf nspca.tar ca* ↵
```

4. Enter the following:

```
# scp nspca.tar root@<WS-NOC IP>:/install_dir/config/bench/ ↵
```

6

Delete the nspca.tar file. Execute:

```
# rm -rf
/opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tls/ca/nspca.tar
```

7

Enter the following:

```
# /install_dir/setup/config.sh ↵
```

The WS-NOC configuration is updated.

8

Perform one of the following:

a. Enter the following to restart the WS-NOC:

```
# sudo /install_dir/setup/mnc.sh restart apps ↵
```

Note: If deployed in HA mode, this command needs to be executed on both the primary and standby WS-NOC servers.

b. If you are using a customer-signed certificate, enter the following to restart the WS-NOC.

```
# /install_dir/setup/mnc.sh restart system ↵
```

9

On the WS-NOC server, enter the following:

```
# /install_dir/setup/generateAndAlignCertificates.sh ↵
```

The WS-NOC aligns the TLS certificates.

10

If the WS-NOC is being integrated in a shared NSP installation, remove the reference to the nspos container from zookeeper:

1. Enter the following:

```
# docker exec -u otn -it mnc-admin bash ↵
```

2. Enter the following:

```
# /nfmt/system-monitor/scripts/remove_oldref.sh nspos ↵
```

3. Exit the mnc-admin container:

```
# exit
```

4. Enter the following to restart the otntomcat container:

   Note: This step not required for WS-NOC Release 23.6 or later.

   ```
   # sudo mnc.sh start containerName=otntomcat ↵
   ```

11

If you are integrating a WS-NOC in HA mode, perform the following steps. These steps must be performed on both HA sites, first for the standby site and then for the primary site. Do not perform functional tests before this part of the procedure is completed.

1. Stop HA data replication.
2. Connect to the WS-NOC standby main VM as mncmaintuser.
3. Edit the configuration.json file as described in Step 4.
4. Stop the WS-NOC system:

   ```
   # sudo /install_dir/setup/mnc.sh stop system ↵
   ```
5. Store the nspca.tar file in the /*install_dir*/config/bench directory.
6. Connect to the MncMain VM.
7. Enter the following to perform a new configuration, specifying the HA site on which the procedure is being performed as the value for *site*:

   ```
   # sudo /install_dir/setup/config.sh site=site ↵
   ```
8. Start the WS-NOC system by entering the following:

   ```
   # sudo /install_dir/setup/mnc.sh start system ↵
   ```
9. Align the certificates by entering the following:

   ```
   # sudo /install_dir/setup/generateAndAlignCertificates.sh ↵
   ```
10. Perform an activity switchover, then repeat steps 1 to 9 on the new active WS-NOC.

When these steps have been performed on both HA sites, first on standby and then on primary, the HA replica can be restarted.

12

Go to Step 23.

Configure WS-NOC

13

If using customer-provided certificates, perform the following:

1. Verify that the customer-provided certificate is usable. Execute the following commands:

   ```
   cd /install_dir/setup/config/httpscertificates/data ↵
   openssl req -noout -text -in nfmt-CSR-certificate.pem ↵
   ```
2. Verify that the customer-provided certificate is properly signed by CustomerCACertificate. Execute:

   ```
   cd /install_dir/setup/config/httpscertificates ↵
   openssl verify -CAfile CustomerCACertificate CustomerCertificate ↵
   ```

The returned result should be 'OK'.

14

Perform one of the following:

a. If using customer-provided certificates, tar the CustomerCACertificate and CustomerCertificate files from *install_dir*/setup/config/httpscertificates into nspca.tar. Execute the following commands:

```
# cp /install_dir/setup/config/httpscertificates/CustomerC* /tmp ↵
# scp root@NSP_deployer_node_IP:
/opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tls/ca_internal*
/tmp ↵
# cd /tmp ↵
# tar cvf nspca.tar CustomerCACertificate CustomerCertificate
ca_internal.key ca_internal.pem ↵
# cp nspca.tar /nokia ↵
```

b. If using NSP-generated TLS certificates, on the NSP deployer, tar the certificates and scp them to the /tmp directory on the WS-NOC server. Execute the following commands:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tls/ca ↵
# tar cvf nspca.tar ca* ↵
# scp nspca.tar root@WS-NOC_IP:/tmp ↵
```

15

Delete the nspos.tar file from the NSP. Execute:

```
# rm -rf nspos.tar
```

16

Open the following file on the WS-NOC server using a plain-text editor such as vi:

/nfmt/config/bench/parameters.cfg

17

Set the NSP_OS_CONFIGURED parameter to “true”.

18

Save and close the file.

19

Execute:

```
mkdir /nokia ↵
cp /tmp/nspca.tar /nokia/ ↵
touch /nokia/nspOS.cfg
```

Note: If the NSP was deployed in a 1+1 redundancy configuration, both the primary and standby NSP server IP addresses must be specified, separated by a semicolon.

20

Edit the nspOS.cfg file, adding the NSP_IP parameter.

Note: If the NSP system was deployed in a DR configuration, both the active and standby addresses should be added in the following format: NSP_IP1; NSP_IP2.

21

Perform one of the following:

a. If using customer-provided certificates, restart the WS-NOC

```
# sudo /setup/mnc.sh restart apps ↵
# sudo /install_dir/setup/generateAndAlignCertificates.sh ↵
```

If deployed in HA mode, this command needs to be executed on both the primary and standby WS-NOC servers.

b. If using NSP-generated TLS certificates, stop data replication, then restart. Execute:

```
/nfmt/setup/mnc.sh restart system ↵
# sudo /install_dir/setup/generateAndAlignCertificates.sh ↵
```

22

If you are integrating an WS-NOC running Release 21.12, the nspos container on the WS-NOC will display as being down. To address this issue by removing the container reference, run the following commands:

```
# docker exec -it mnc-admin bash ↵
# su otn ↵
# /nfmt/system-monitor/scripts/remove_oldref.sh nspos ↵
# /nfmt/setup/mnc.sh restart containerName=otntomcat ↵
```

Roll back configuration, if required

23

If required, rollback the integration by performing the following:

a. For WS-NOC Release 21.12:

1. Delete the nspOS.cfg file from the /nokia and /nfmt/config/bench directories.
2. Execute:

```
rm -rf /nokia/nspOS.cfg ↵
rm -rf /nfmt/config/bench/nspOS.cfg ↵
rm -rf /nokia/nspca.tar ↵
```

3. Restart the system. Execute:

```
/nfmt/setup/mnc.sh restart system ↵
```

b. For WS-NOC Release 22.6 and later:

1. Connect to the WS-NOC main VM as mncmaintuser.
2. Edit the /*install_dir*/config/bench/configuration.json file using a plain-text editor such as vi.
3. Remove the "nsp" property from the "remoteAuthentication" => "active" field.
4. Save the changes and close the file.
5. Enter the following command:

```
# rm -rf /install_dir/config/bench/activenspos.cfg ↵
```

6. Enter the following command:

```
# cd/install_dir/app/templates/MW-INT
```

7. Remove the following entries from the file:

```
MWSVC-WEB_plat.properties.base
plat.preserver.3.mwsvcport=5138
plat.preserver.3.supporteddatatypes=Log
plat.preserver.3.nativedatatypes=Log
plat.preserver.3.hostname=nspos
plat.preserver.3.mwsvcserviceport=5035
plat.preserver.3.systype=OTNE
plat.preserver.3.showcpu=false
```

8. Run bench config. Execute:

```
# sudo /install_dir/app/common/bench_config.sh
```

9. Remove ZooKeeper from system admin. Execute:

```
# sudo /install_dir/app/tools/sh mnc-admin
```

10. Stop the WS-NOC. Execute:

```
# sudo /install_dir/setup/mnc.sh stop system ↵
```

11. Delete the nspca.tar file and nspOS.cfg file from the /*install_dir*/config/bench directory.
12. Run the WS-NOC configuration command:

```
# sudo /install_dir/setup/config.sh ↵
```

13. Start the WS-NOC. Execute:

```
# sudo /install_dir/setup/mnc.sh start system ↵
```

Enable the Back to Launchpad option on the WS-NOC GUI

24

Log in to the WS-NOC VM.

25

Connect to the otntomcat container on WS-NOC. Execute the following commands:

1. `docker exec -ti otntomcat bash ↵`
2. `cd /nokia/1350OMS/NMA/WDM_WEB/20.11.0/lib/otn/resources/common/menu/ ↵`

   or

   `cd /nokia/1350OMS/NMA/WDM_WEB/21.4.0/lib/otn/resources/common/menu/ ↵`

26

Modify the systemProperty.json and the systemProperty.json.VMs files so that the "nspIsConfigured" parameter is set to false.

27

Exit the container and refresh the GUI page.

Note: The otntomcat container does not need to be restarted.

Post-integration steps required when using customer-provided certificates:

28

If WS-NOC is deployed in HA mode, execute the following on the standby WS-NOC server to align HA status:

```
# sudo rm -rf /install_dir/setup/config/httpscertificates ↵
```

```
# su - root scp -r <active alias or IP>:/install_dir/setup/config/httpscertificates /install_dir/setup/config/ ↵
```

```
# sudo rm -rf /install_dir/app/common/.ssl ↵
```

```
# su -root scp -r active_alias_or_IP:/install_dir/app/common/.ssl install_dir/app/common/ ↵
```

```
# sudo docker start nfmt-setup ↵
```

```
# sudo mnc.sh restart apps ↵
```

29

In the mnc-admin and nrct-tapi containers, execute:

```
chmod 644 /nfmt/instance/certificates/External/keystore.ks ↵
```

```
chmod 644 /nfmt/instance/certificates/External/key.pem ↵
```

```
mkdir -p /nfmt/config/tempcustom/nfmt/instance/certificates/External/ ↵
```

```
cp /nfmt/instance/certificates/External/keystore.ks /nfmt/config/tempcustom/nfmt/instance/certificates/External/ ↵
```

```
cp /nfmt/instance/certificates/External/key.pem /nfmt/config/tempcustom/nfmt/instance/certificates/External/ ↵
```

30

In the mnc-fm, pm-components, pm-hadoop, pm-kafka, and pm-spark containers, execute:

```
chmod 644 /nfmt/instance/certificates/External/keystore.ks ↵
```

```
mkdir -p /nfmt/config/tempcustom/nfmt/instance/certificates/External/
↵
```

```
cp /nfmt/instance/certificates/External/keystore.ks
/nfmt/config/tempcustom/nfmt/instance/certificates/External/ ↵
```

31

Navigate to System Control within WS-NOC. If any processes are 'down', login to their individual containers and start them by executing:

```
/umc/plat/script/mngApp startup process_name ↵
```

32

Close the open console windows.

END OF STEPS

12 NSP system uninstallation

12.1 Introduction

12.1.1 Description

The procedures in this chapter describe how to remove the NSP software from an NSP cluster, and how to remove the NSP deployment environment from the NSP host stations.

Note: To uninstall the software or environment in a DR NSP system, you must perform the procedures in each data center.

12.2 Workflow to uninstall an NSP cluster

12.2.1 Purpose

The following is the sequence of high-level actions required to uninstall the NSP software, and optionally, the Kubernetes deployment environment, in a data center that hosts an NSP cluster.

12.2.2 Stages

1

To uninstall the NSP software from the NSP cluster, perform 12.3 “To uninstall the NSP software from an NSP cluster” (p. 355).

2

To uninstall the NSP Kubernetes environment, for example, if the cluster host stations are to be recommissioned for another purpose, perform 12.4 “To uninstall the NSP Kubernetes software” (p. 357).

3

To uninstall the Kubernetes registry from the NSP deployer host, for example, if you intend to replace the Kubernetes environment of your NSP system, perform 12.5 “To uninstall the NSP Kubernetes registry” (p. 357).

12.3 To uninstall the NSP software from an NSP cluster

12.3.1 Purpose

Perform this procedure to remove the NSP software from the nodes in an NSP cluster.

Note: You require root user privileges on each NSP cluster station.

Note: *release-ID* in a file path has the following format:

R.r.p-rel.*version*

where

R.r.p is the NSP release, in the form *MAJOR.minor.patch*

version is a numeric value

12.3.2 Steps

1

Log in as the root user on the NSP deployer host.

2

Open a console window.

3

If the NSP is deployed with OAUTH2 authentication, back up the following files to a secure location:

- /opt/nsp/nsp-configurator/generated/nsp-keycloak-admin-secret
- /opt/nsp/nsp-configurator/generated/nsp-keycloak-client-secret

4

To preserve the cluster configuration, perform the following steps.

1. Open the following file using a plain-text editor such as vi:

   /opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml
2. Edit the following line in the **platform** section, **kubernetes** subsection to read:

   ```
   deleteOnUndeploy:false
   ```
3. Save and close the file.

5

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

6

Enter the following:

```
# ./nspdeployerctl uninstall --undeploy --clean ↵
```

The NSP software is removed from each NSP cluster member.

END OF STEPS

12.4 To uninstall the NSP Kubernetes software

12.4.1 Purpose

Perform this procedure to remove the NSP Kubernetes software.

Note: You require root user privileges on the NSP deployer host.

Note: *release-ID* in a file path has the following format:
R.r.p-rel.*version*
where
R.r.p is the NSP release, in the form *MAJOR.minor.patch*
version is a numeric value

12.4.2 Steps

1

Log in as the root user on the NSP deployer host.

2

Open a console window.

3

Enter the following:

```
# cd /opt/nsp/nsp-k8s-deployer-release-ID/bin ↵
```

4

Enter the following:

Note: The action affects all NSP cluster VMs specified in the hosts.yml file.

```
# ./nspk8sctl uninstall ↵
```

The NSP Kubernetes software is uninstalled.

END OF STEPS

12.5 To uninstall the NSP Kubernetes registry

12.5.1 Purpose

Perform this procedure to remove the NSP Kubernetes registry and environment from an NSP deployer host.

Note: You require root user privileges on the NSP deployer host.

Note: *release-ID* in a file path has the following format:

R.r.p-rel.*version*
where
R.r.p is the NSP release, in the form *MAJOR.minor.patch*
version is a numeric value

12.5.2 Steps

1

Log in as the root user on the NSP deployer host.

2

Open a console window.

3

Enter the following:

```
# cd /opt/nsp/nsp-registry-release-ID/bin ↵
```

4

Enter the following to remove the NSP Kubernetes environment:

Note: The NSP Kubernetes registry log is /var/log/nspregistryctl.log.

```
# ./nspregistryctl uninstall -y ↵
```

The NSP Kubernetes registry and environment are uninstalled.

5

Close the console window.

END OF STEPS

Part III: NSP component deployment

Overview

Purpose

This part of the *NSP Installation and Upgrade Guide* describes the deployment of NSP components that are hosted outside the NSP container environment.

Contents

13 NSP component configuration

13.1 Overview

13.1.1 Purpose

This chapter describes how to specify the deployment criteria for NSP components that provide supplemental NSP functions, for example, NSP analytics, and are hosted outside the NSP cluster environment.

For component platform information such as hardware recommendations and scaling guidelines, see the *NSP Planning Guide*.

For platform configuration information such as preparing disk partitions or installing the RHEL OS, see Part I: “Getting started”.

13.1.2 Contents

Configuring NSP component deployments

13.2 Common configuration elements

13.2.1 Platform configuration

The deployment requirements and methods for components outside the NSP cluster can vary. However, some aspects of platform configuration are common to all components.

Time synchronization

CAUTION

Service Degradation

Some components, for example, members of an etcd cluster, fail to trust data integrity in the presence of a time difference. Failing to closely synchronize the system clocks among components complicates troubleshooting and may cause a service outage.

Ensure that you use only the time service described in this section to synchronize the NSP components.

The system clocks of the NSP components must always be closely synchronized. The RHEL chronyd service is the mandatory time-synchronization mechanism that you must engage on each NSP component during deployment.

Note: Only one time-synchronization mechanism can be active in an NSP system. Before you enable chronyd on an NSP component, you must ensure that no other time-synchronization mechanism, for example, the VMware Tools synchronization utility, is enabled.

13.2.2 RHEL /etc/hosts file

You must edit the /etc/hosts file on a component station to include:

- an entry for each component in the NSP deployment with which it communicates
- an entry for the advertised address of the NSP cluster

An entry consists of one line for each server that maps the server IP address to the server hostname. The following is an example hosts file for an NSP deployment that has Chicago and New York data centers; each data center has three NSP cluster members and redundant NFM-P main servers:

```
198.51.100.7 nsdchicago1.company.org

198.51.100.8 nsdchicago2.company.org

198.51.100.9 nsdchicago3.company.org

198.51.100.13 nfmpchicago1.company.org

198.51.100.14 nfmpchicago2.company.org

203.0.113.5 nsdnewyork1.company.org
```

```
203.0.113.6 nsdnewyork2.company.org

203.0.113.7 nsdnewyork3.company.org

203.0.113.17 nfmpnewyork1.company.org

203.0.113.18 nfmpnewyork2.company.org
```

13.3 NSP hosts file

13.3.1 Description

The NSP hosts file specifies the addresses of the NSP components that the NSP Flow Collectors and Flow Collector Controllers communicate with.

Note: If you specify a hostname in the config.yml configuration file, you must specify the hostname in the associated NSP hosts file entry, and not an IP address.

Note: An example hosts file is in the following directory; use a modified copy of the file for installation:
NSP_installer_directory/NSD_NRC_*R_r*/examples

Configuring the NSP hosts file

Each line in the example file has a leading “#” character, which causes the line to be interpreted as a comment and not processed. To enable the processing of a line, you must remove the leading # character from the line. A section for a discrete system element begins with an [*element*] tag, for example, [nspos], which is the section for the nspOS configuration.

The hosts file has separate sections for specific deployment types; each section has a descriptive two- or three-line header, and includes the required parameters for the deployment. The section headers are shown below, by deployment type.

Standalone:

```
# Sample Ansible hosts file for an NSP standalone system

# Replace the IPs below by your own
```

1+1 geographic redundancy, or HA:

```
# Sample Ansible hosts file for an NSP geo-redundant system

# Enter 2 IPs per group when installing in geo-redundancy mode

# and add the variable 'dc' to differentiate the datacenters.
```

Deployment in a NAT environment

For deployment in a NAT environment, you can add the optional advertised_address parameter to the IP address line of a component. The parameter enables the advertisement of the component hostname or public IP address to other components.

For remote installation in a NAT environment, you can also add the ansible_host parameter, which enables the installer to reach the remote host. The options are described in the following section of the example hosts file:

```
# Optional configuration
```

For example, to specify a remote NSP Flow Collector in a NAT environment:

```
[fc]
```

```
private_IP advertised_address=public_IP ansible_host=IP_reachable_by_installer
```

where

private_IP is the private IP address of the NSP Flow Collector

public_IP is the public IP address of the NSP Flow Collector

IP_reachable_by_installer is the NSP Flow Collector IP address that is reachable from the station on which the NSP installer runs

The section also includes other optional addressing parameters.

Table 13-1 NSP hosts file sections and parameters

Component	Required hosts file entry
NSP cluster (any configuration)	`[nspos]`

Flow Collector Controller and Flow Collector (standalone)	`[fcc]`
	`Controller_IP`
	`[fc]`
	`Collector_IP` `fc_mode=`*`mode`*
	where
	Controller_IP is the NSP Flow Collector Controller IP address; in a NAT environment, specify the private IP address
	NOTE: An NSP Flow Collector Controller and the associated Flow Collectors must be on the same subnet as the NSP components with which they communicate, for example, NFM-P main servers and an auxiliary database.
	Collector_IP is the NSP Flow Collector IP address; in a NAT environment, specify the private IP address
	mode is the NSP Flow Collector mode, which is one of the following; if unspecified, the default is AA:
	• AA—enables the collection of AA Cflowd records
	• SYS—enables the collection of IPFIX system Cflowd and Netflow v5 records

Table 13-1 NSP hosts file sections and parameters (continued)

Component	Required hosts file entry

Flow Collector Controller and Flow Collector (1+1)	`[fcc]`
	`Controller_IP`
	`[fc]`
	`Collector_IP dc=data_center fc_mode=mode`
	where
	Controller_IP is the NSP Flow Collector Controller IP address; in a NAT environment, specify the private IP address
	NOTE: An NSP Flow Collector Controller and the associated Flow Collectors must be on the same subnet as the NSP components with which they communicate, for example, NFM-P main servers and an auxiliary database.
	Collector_IP is the NSP Flow Collector IP address; in a NAT environment, specify the private IP address
	data_center is the name of the data center
	mode is the NSP Flow Collector mode, which is one of the following; if unspecified, the default is AA:
	• AA—enables the collection of AA Cflowd records
	• SYS—enables the collection of IPFIX system Cflowd and Netflow v5 records

Advertised addresses and ansible hosts	`[fc]`
	`IP_address advertised_address=advertised_IP ansible_host=ansible_IP`
	`[fcc]`
	`IP_address advertised_address=advertised_IP ansible_host=ansible_IP`
	where
	IP_address is the IP address of the NSP component
	advertised_IP is the advertised IP address of the NSP component
	ansible_IP is the IP address of the NSP component ansible host
	cluster_address is the advertised_address of the NSP cluster

13.4 NSP RPM-based configuration file

13.4.1 Using the config.yml file

The config.yml file specifies the deployment criteria for RPM-based NSP components. Based on your requirements, you must edit the config.yml sections that apply to your deployment; an example configuration file is in the following directory:

NSP_installer_directory/NSD_NRC_*R_r*/examples

Note: It is strongly recommended that you use a modified copy of the example configuration file for your deployment.

Configuring parameters

To enable a section and the required parameters in the section, you must do the following:

1. Remove the leading # character from the section label.
2. Remove the leading # character from each parameter that you need to configure.

3. Enter the required value for each parameter, as described in the comment lines above the section label.

Note: It is recommended that you remove parameter lines that you do not require from the configuration file. Also, failing to provide a parameter value may have undesired consequences.

Note: In the event of a discrepancy between information in a configuration file and the NSP documentation, or if the documentation fails to adequately describe a specific configuration, the configuration file information is to be followed and considered correct. Also, the *NSP Release Notice* describes configuration updates and corrections that are not captured in the core documentation.

13.4.2 RPM-based deployment parameters

Table 13-2, “config.yml parameters” (p. 366) lists and describes the config.yml file sections and parameters that are specific to the RPM-based components of an NSP deployment.

Table 13-2 config.yml parameters

Section and parameters	Description
nfmp — NFM-P integration parameters	
primary_ip	IP address of primary NFM-P main server Default: none
standby_ip	IP address of standby NFM-P main server Default: none
tls_enabled	Whether TLS communication with NFM-P is enabled You can set the parameter to true only when the NSP system is not integrated with the WS-NOC. Default: true
cert_provided	Whether custom TLS certificate is to be used for communication with NFM-P Default: false
resync_augmentation_scripts_path	Path to the scripts that augment NFM-P re-synchronization in IPRC server
nfmt — WS-NOC integration parameters	
primary_ip	IP address of primary WS-NOC server Default: none
standby_ip	IP address of standby WS-NOC server Default: none
cert_provided	Whether custom TLS certificate is to be used for communication with WS-NOC Default: false
nrct — WS-RC integration parameters	

Table 13-2 config.yml parameters (continued)

Section and parameters		Description
primary_ip		IP address of primary WS-RC server Default: none
standby_ip		IP address of standby WS-RC server Default: none
remote		Specifies that the WS-RC is in a remote authentication space, relative to the CDRC server
username		User name to be used when authenticating to an WS-RC in a remote authentication space
password		Password to be used with the supplied user name
sros — required when integrating NSP with an SROS VM		
enabled		Whether path computation using SROS VM is enabled Default: false **Note:** When set to true, the SROS block of the hosts file must be configured.
openflow		Whether OpenFlow is enabled Default: false
pcep		Whether PCEP is enabled Default: false
bgpls		Whether BGP LS is enabled Default: false
vms	ip	IP address of SROS VM
	router_id	SROS VM router ID
	v_id	SROS VM virtual ID; must be an integer value **NOTE:** The value must be the same for redundant VMs.
	openflow	Whether OpenFlow is enabled Default: false
	pcep	Whether PCEP is enabled Default: false
	bgpls	Whether BGP LS is enabled Default: false
ean — EAN customization parameters		
max_subscribers		Maximum number of clients that can subscribe for EAN
remote_syslog_for_nsp_activity_logs — remote syslog server parameters		
enabled		Whether NSP activity-log forwarding to a remote syslog server is enabled Default: false
remote_syslog_ip_address		Remote syslog server IP address

Table 13-2 config.yml parameters (continued)

Section and parameters	Description
remote_syslog_port	Remote server TCP port
remote_syslog_ca_cert_path	Absolute local path of TLS certificate copied from remote server

13.4.3 Manual WS-NOC deployment

If the install parameter in the **nfmt** section of the configuration file is set to false, the NSP cannot integrate with the WS-NOC, and you must use the oms-server.conf file instead. The file is populated as follows:

```
oms {
    OMSServers=[ {
        id="WS-NOC_ID"
        OMSMain={
            host="primary_address"
            host2="standby_address"
            username="username"
            password="password"
        }
    } ]
    tls-enabled="value"
    tls-directory="TLS_dir"
}
```

where

WS-NOC is the unique WS-NOC system identifier

primary_address is the IP address of the standalone WS-NOC server, or the primary WS-NOC server in a redundant deployment

standby_address is the IP address of standby WS-NOC server in a redundant deployment

username is the username required for WS-NOC login

password is the password required for WS-NOC login

value specifies whether TLS is enabled on the WS-NOC, and is true or false

TLS_dir specifies the directory that contains the TLS certificates, if TLS is enabled

NFM-P deployment configuration

13.5 NFM-P deployment requirements

13.5.1 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 NokiaAirFrame 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 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 unless NFM-P OS support restrictions exist.
- An NFM-P main server creates a small number of RHEL system users for internal functions, so requires available system user IDs on the host station. If no system reserved IDs are available, the main server configuration from samconfig cannot be applied, and the main server installation fails.
- 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 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 Planning Guide*, you must use a disk array with the main database to increase performance. See Chapter 2, “NSP disk setup and partitioning” 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 Bash shell is the supported command shell for RHEL CLI operations.

13.5.2 Security requirements

> **Note:** The use of sudo to gain root user privileges is supported for NFM-P installation, and for any other NFM-P operation 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 client 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.

13.5.3 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 address of the peer main server after a main server communication failure.

To resolve the two addresses, 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.

Regardless of the network addressing scheme and configuration, for example, whether NAT, hostnames, or multiple interfaces are used, the /etc/hosts file of a component must contain valid address entries for reaching other components at the following times:

- during normal operation
- after a network or NFM-P component failure

Using NAT

Network Address Translation adds an extra level of complexity to an NFM-P network. If NAT is to be used in the NFM-P management network, hostname resolution for GUI and XML API client communication is strongly recommended.

The following are the basic network configuration requirements; see 13.9 “Using hostnames in the management network” (p. 379) for more information, including an example network configuration that uses hostnames.

- When you use a hostname to identify an NFM-P or NSP component, you must use local hostname resolution; the use of DNS is supported only for non-NSP components such as OSS or external systems.
- The first uncommented entry in the /etc/hosts file must map the local hostname to the private IP address of the interface to the other NFM-P components.

- The hostname of an NFM-P component must:
  - contain only ASCII alphanumeric and hyphen characters.
  - not begin or end with a hyphen.
  - not begin with a number.
  - comply with the format defined in IETF RFC 1034.
  - use period characters delimit the FQDN components.
  - not exceed 63 characters.
- 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.

Firewalls

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 *NSP Planning Guide* lists the open ports required by each component.

Note: If you intend to use firewalld, you must configure firewalld according to the rules in the *NSP Planning Guide*, which describes using NFM-P templates to create firewalld rules.

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
- A standalone 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 cluster must be on the same side of the management LAN, and not geographically dispersed.
- The internal communication among the stations in an auxiliary database cluster must be isolated to a dedicated private network. Each station IP address used for internal communication must be associated with an interface connected to the private network, and must be the only IP address of the interface.
- 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
- Specifying a TCP or UDP port other than the default 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.

Hostname usage in an NFM-P system has special configuration requirements. See 13.9 “Using hostnames in the management network” (p. 379) for an example management network configuration, and 13.5.3 “Network requirements” (p. 371) for specific configuration information.

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.

Note: Before you upgrade an NFM-P system that manages 7705 SAR, 7705 SAR-Hm, or VSR NEs using NGE, you must observe the following:

- 7705 SAR - Release 8.0 R3 and earlier support only NGE version 1; Release 8.0 R4 and later support only NGE version 2.
- 7705 SAR-Hm and VSR - Release 15.0 R3 and earlier support only NGE version 1; Release 15.0 R4 and later support only NGE version 2.

If you want to manage such devices after the NFM-P upgrade using NGE version 2, you must do the following:

1. Upgrade each device to a release that supports NGE version 2.
2. Use the NFM-P to specify NGE version 2 for each device.

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 NE. If this is not true, you must perform one of the following before you attempt the upgrade, or service disruption may occur.
  - Upgrade the NE 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 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.

13.5.4 Software deployment 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. 13.8 “To obtain the UUID of a station” (p. 378) describes how to obtain a station UUID.

    Note: An NFM-P component upgrade from Release 22.6 or earlier is also a platform migration to a new RHEL OS version. Consequently, the host station UUID changes, and an upgraded main server does not recognize the existing NFM-P license.

    An NFM-P system upgrade from Release 22.6 or earlier requires a new licence based on the new main server UUIDs.
  - A license 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.

13.6 NFM-P deployment restrictions

13.6.1 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 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 open a console window on an NFM-P main database station, 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.

- 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.
- The RHEL TFTP server conflicts with the NFM-P TFTP server, and must be disabled on a main or auxiliary server station.
- 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:
  - You can configure an NFM-P system to concurrently manage IPv4 and IPv6 networks.
  - An NFM-P GUI or browser-based 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 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.

13.6.2 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.

13.6.3 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.

13.6.4 Software deployment restrictions

You must observe the following NFM-P software deployment restrictions.

- 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 the *NSP System Administrator Guide* for information about importing a license.

13.7 Configuring an NFM-P system deployment

13.7.1 Deployment conditions

Before you attempt to install the NFM-P, you must comply with the conditions in this section and ensure that the NFM-P platform is correctly configured, as described in Part I: “Getting started”.

Chapter 3, “RHEL OS deployment for the NSP” contains OS-specific information about single-user GUI client and client delegate server deployment.

Platform support

You can deploy NFM-P components in virtual machines, or VMs. See the *NSP Planning Guide* for VM host requirements, and 13.10 “Deployment in a VM” (p. 382) for VM deployment requirements and restrictions.

An NFM-P system has the following 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
- optionally, one or more auxiliary servers
- optionally, an auxiliary database

An NFM-P system can also include the following:

- NSP Flow Collectors
- NSP analytics servers

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 13-3 NFM-P platform support by component

NFM-P component	Mac OS X	Microsoft Windows	RHEL
Main server			✓
Main database			✓
Auxiliary server			✓
Auxiliary database			✓
Client delegate server		✓	✓
Single-user client	✓	✓	✓

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
- 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 during the initial login attempt.
- 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.

13.8 To obtain the UUID of a station

13.8.1 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.

Upgrading from Release 22.6 or earlier

An NFM-P upgrade from Release 22.6 or earlier is also a platform migration to a new RHEL OS version. Consequently, each host station UUID changes, and an upgraded main server does not recognize the existing NFM-P license.

An NFM-P system upgrade from Release 22.6 or earlier requires a new licence based on the new main server UUIDs.

ℹ **Note:** If you are using an ILO Management system, ensure that you obtain the UUID of the intended VM and not the UUID of the ILO module.

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

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

13.8.2 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 in your NFM-P license request.

END OF STEPS

13.9 Using hostnames in the management network

13.9.1 Introduction

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.

Also, some CA signing authorities accept 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.

Note: In the **client** section of samconfig on the NFM-P main servers, if the address for client access is set using the **hostname** parameter, the **primaryIp** and **standbyIp** values in the **nfmp** section of the NSP configuration file, nsp-config.yml, must be set to hostnames.

Likewise, if the **public-ip** parameter in the **client** section is configured on the main server, the **primaryIp** and **standbyIp** values in the nsp-config.yml file must be set to IP addresses.

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.

13.9.2 Hostname configuration requirements

Only local hostname lookup is supported for NFM-P and NSP component hostname resolution. You can use a DNS server to resolve the addresses of non-NSP components such as OSS or external systems.

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

- Configure the /etc/hosts file on each component to ensure that each hostname translates to the correct IP address; the hostname must:
  - contain only ASCII alphanumeric and hyphen characters.
  - not begin or end with a hyphen.
  - not begin with a number.
  - comply with the format defined in IETF RFC 1034.
  - use period characters to delimit the FQDN components.
  - not exceed 63 characters.
- During component deployment, specify hostnames instead of IP addresses.

Note: A hostname is case-sensitive.

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

Component-specific hostname configuration

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

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 Planning Guide* for more information.

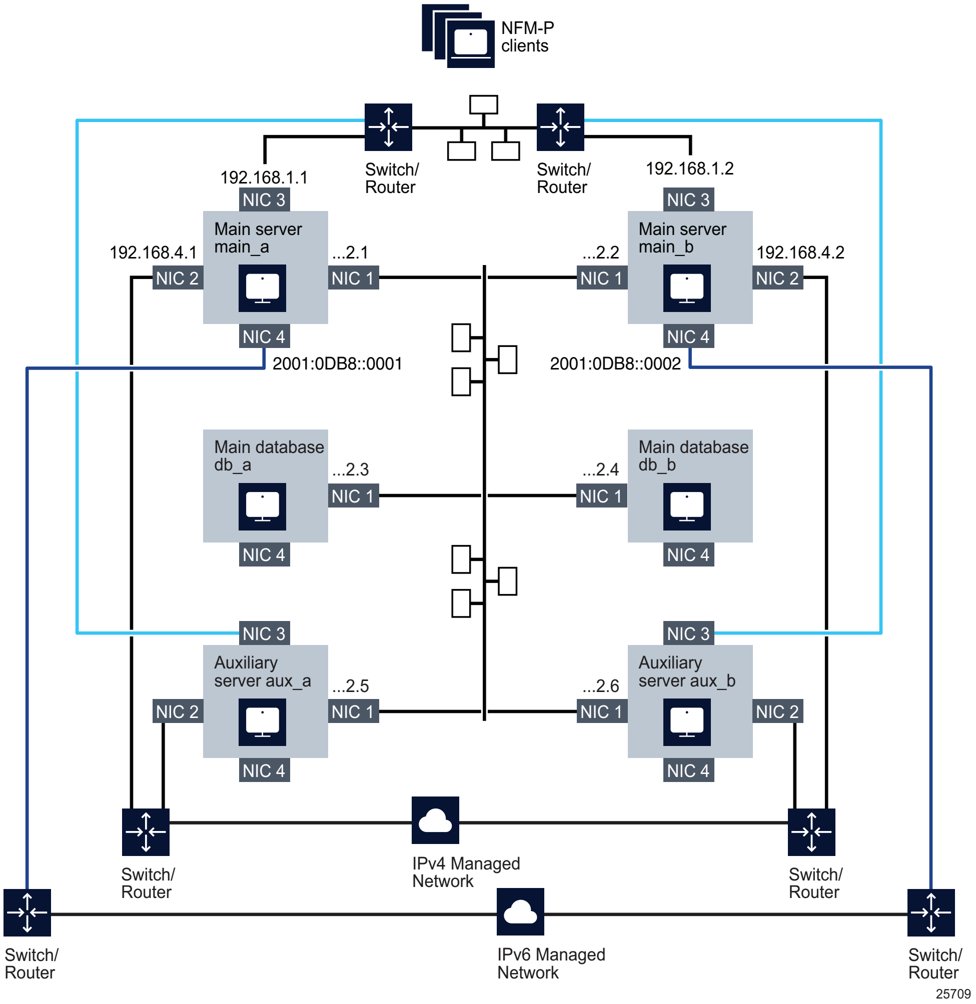
Note: When using hostname configuration of NSP components, the hostnames must be resolvable by DNS.

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.

13.9.3 Management network configuration example

The following is a configuration example for hostname resolution in a moderately complex NFM-P management network that may or may not include a NAT configuration. In the example, each main server communicates with multiple networks using separate interfaces, as shown in Figure 13-1, “Management network topology” (p. 380).

Figure 13-1 Management network topology



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:

```
192.168.2.1 main_a

192.168.2.2 main_b

192.168.2.5 aux_a

192.168.2.6 aux_b

192.168.2.3 db_a

192.168.2.4 db_b

127.0.0.1 localhost
```

The /etc/hosts file on station aux_a requires the following entries:

```
192.168.2.5 aux_a

192.168.2.6 aux_b

192.168.2.1 main_a

192.168.2.2 main_b

192.168.2.3 db_a

192.168.2.4 db_b

127.0.0.1 localhost
```

The /etc/hosts file on station db_a requires the following entries:

```
192.168.2.3 db_a

192.168.2.4 db_b

127.0.0.1 localhost
```

13.10 Deployment in a VM

13.10.1 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 13.5 “NFM-P deployment requirements” (p. 370) 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 Planning Guide* for the hardware virtualization requirements, and for the specific configuration requirements of a supported environment.

13.10.2 VM deployment using disk images

You can use disk images to deploy the following in a KVM or RHEL OpenStack environment:

- RHEL OS, for subsequent NFM-P component installation; see 2.2 “Introduction” (p. 28)
- NFM-P system; see 14.10 “ Using an NFM-P disk image” (p. 436)

13.10.3 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 a supported version of RHEL, as specified in the *NSP Planning Guide*.
- RHEL deployment on VMware requires VMXNET 3 NIC adapters; see the VMware documentation for information.

13.10.4 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 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, NEtO, 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 Planning Guide*.

13.11 Enabling FIPS security for NFM-P network management

13.11.1 Description

CAUTION

Management Disruption

Enabling FIPS may prevent the management of some SNMPv3 NEs, or prevent clients from connecting to the NFM-P, if the NEs or clients do not support one of the FIPS 140-2 ciphers or algorithms that the NFM-P offers.

Ensure that all managed NEs, and all GUI and OSS clients, support the FIPS 140-2 standard before you consider enabling FIPS.

The NFM-P supports enabling Federal Information Processing Standards, or FIPS, security for NE management. Enabling FIPS mode reduces the number of ciphers and encryption algorithms that the NFM-P uses for NE management and client communication. Clients and NEs require FIPS-compatible ciphers and algorithms in order to communicate with the NFM-P.

For example, the 7750 SR family of devices supports FIPS security. When NFM-P FIPS mode is enabled, each such managed NE must be FIPS-compliant. For example, an NE that uses MD5/DES or SHA/DES encryption cannot be managed by an NFM-P system in FIPS mode, as FIPS does not support DES encripition.

SSH connectivity to NEs from an NFM-P system in FIPS mode also requires that the NEs comply with the FIPS security framework.

Note: FIPS mode applies only to SNMPv3-managed NEs, and does not affect NEs managed using SNMPv1 or v2

13.11.2 NFM-P FIPS implementation

By default, FIPS mode is disabled in the NFM-P, and is to be enabled only if all clients and NEs are compatible with the FIPS 140-2 encryption ciphers and algorithms.

FIPS mode is supported on NFM-P main servers and auxiliary servers.

The following document includes general TLS implementation guidelines for FIPS:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf

See this link for the FIPS 140-2 cryptography security requirements.

13.11.3 OSS considerations

NFM-P JMS clients must meet the following requirements if FIPS mode is enabled.

- The client must be made FIPS-aware by setting the following JVM option:
  -Dnfmp.fips.enabled=true
- The client must use the BCFKS keystore format.
- The client must include the following Bouncy Castle FIPS jars in the class path:
  - bc-fips-1.0.2.1.jar

- bctls-fips-1.0.12.2.jar

13.12 Workflow for FIPS-enabled NFM-P discovery of a new device

13.12.1 Description

The following are the high-level steps required to commission and discover a device for NFM-P management using FIPS security.

Note: In order to use the workflow, the following must be true:

- FIPS is enabled in each NFM-P main server configuration.
- Each main server is running and operational.

FIPS is enabled on a main server using a parameter in the top-level section of samconfig, as described in the NFM-P system installation procedures.

13.12.2 Stages

1

Manually enable FIPS mode on the device; see the device documentation for information.

Note: You cannot use the NFM-P to enable FIPS mode on a device.

2

Manually create a FIPS-compliant SNMPv3 user account on the device

Note: You cannot use the NFM-P to create an SNMPv3 user account on a device.

3

Create an NFM-P SNMPv3 user account that matches the device user account.

4

Create a FIPS-compliant NFM-P discovery rule for the device, and specify the NFM-P SNMPv3 user in the associated mediation policy.

In accordance with the NFM-P polling policy, the NFM-P discovers and manages the device using FIPS security during the next discovery-rule scan.

13.13 Workflow for NE conversion to FIPS mode

13.13.1 Description

The following are the high-level steps required to commission and discover a device for NFM-P management using FIPS security.

Note: In order to use the workflow, the following must be true:

- FIPS is enabled in each NFM-P main server configuration.
- Each main server is running and operational.

- The NFM-P has a FIPS-compliant SNMPv3 user account for device mediation.

FIPS is enabled on a main server using a parameter in the top-level section of samconfig, as described in the NFM-P system installation procedures.

13.13.2 Stages

1

Modify the NFM-P discovery rule for the device to be FIPS-compliant; you must also ensure that the user named in the associated mediation policy is FIPS-compliant.

2

Manually commission the device for FIPS-secured management:

Note: You cannot use the NFM-P to enable FIPS mode or create an SNMPv3 user on a device.

1. Enable FIPS mode on the device; see the device documentation for information.
2. Create a FIPS-compliant SNMPv3 user on the device.
3. If any user account on the device is not FIPS-compliant, remove the account.

   Note: If any non-compliant account remains, the device cannot reboot correctly.
4. Reboot the device, if required.

When the reboot is complete, the NFM-P discovers and manages the device using FIPS security during the next discovery-rule scan, in accordance with the NFM-P polling policy.

13.14 GPG-signed RPM files

13.14.1 Introduction

The RHEL OS must prevent the installation of software, patches, service packs, device drivers, or OS components of local packages without prior verification that the packages are digitally signed by a recognized or approved CA.

Nokia digitally signs each NSP software RPM file using GNU Privacy Guard, or GPG, to enable you to ensure the integrity of the file before use. It is recommended that you download and import the NSP GPG public key for your NSP release, and then verify each downloaded NSP RPM file before installation to ensure that the file has not been altered since being signed by Nokia.

13.15 To verify the GPG keys

13.15.1 Purpose

The following steps describe how to download and verify the NSP GPG public key and third-party keys in order to verify the GPG signatures of downloaded NSP RPM installation files.

13.15.2 Steps

1

Download the following file from the Nokia Support Portal to a temporary directory on a RHEL station:

nsp-signing-keys.zip

2

Log in as the root user on the RHEL station.

3

Open a console window.

4

Navigate to the directory that contains the downloaded file.

5

Enter the following:

```
# unzip nsp-signing-keys.zip ↵
```

The GPG key files are extracted to the current directory.

6

Enter the following to display the NSP key fingerprint:

```
# gpg gpg --show-keys --with-fingerprint --keyid-format=short
nsp-rpm-signing-public-key.key ↵
```

Output like the following is displayed:

```
pub   rsa4096/C7C20997 date [SCEA]

      Key fingerprint = 7809 77B0 BA34 052A 1E18  56CE B78C C956 C7C2
0997

uid                     Nokia Corporation (NOKIA-RPM-GPG-KEY)
<portal.support@nokia.com>
```

7

Review and verify the fingerprint.

8

If you are not performing the procedure on an NFM-P main server, go to Step 11.

9

Enter the following to display the td-agent key fingerprint:

```
# gpg --show-keys --with-fingerprint --keyid-format=short
GPG-KEY-td-agent↵
```

Output like the following is displayed:

```
pub   rsa4096/AB97ACBE date [SC]
      Key fingerprint = BEE6 8228 9B22 17F4 5AF4  CC3F 901F 9177 AB97
ACBE
uid                     Treasure Data, Inc (Treasure Agent Official
Signing key) <support@treasure-data.com>
sub   rsa4096/A71065E9 date [E]
```

10

Review and verify the fingerprint.

11

If the fingerprint value matches the value shown in the command output, the key is valid; otherwise, contact Nokia technical support.

12

Close the console window.

END OF STEPS

13.16 To verify Nokia RPM-file GPG signatures

13.16.1 Purpose

The following steps describe how to verify that RPM files downloaded from Nokia are GPG-signed by Nokia.

13.16.2 Steps

1

Log in as the root user on a station that has no network connection to any station in a current or proposed NFM-P deployment.

2

Import the NSP GPG public key.

1. Enter the following.

   ```
   # rpm -qa | grep gpg-pubkey ↵
   ```

2. Enter the following.

   ```
   # sudo rpm --import nsp_publickey.key ↵
   ```

3. Enter the following.

```
# rpm -qa | grep gpg-pubkey ↵
```

The public key is imported; the import is successful if a line like the following is displayed:

```
gpg-pubkey-version-release
```

3

If you are performing the procedure on an NFM-P main server, import the td-agent public key.

1. Enter the following.

   ```
   # rpm -qa | grep gpg-pubkey ↵
   ```

2. Enter the following.

   ```
   # sudo rpm --import GPG-KEY-td-agent ↵
   ```

3. Enter the following.

   ```
   # rpm -qa | grep gpg-pubkey ↵
   ```

   The public key is imported; the import is successful if a line like the following is displayed:

   ```
   gpg-pubkey-version-release
   ```

4

Enter the following to verify that the imported GPG public key is from Nokia:

```
# rpm -q gpg-pubkey --qf '%{name}-%{version}-%{release} -->
%{summary}\n' ↵
```

Output like the following is displayed if the key is from Nokia:

```
gpg-pubkey-version-release --> gpg(Nokia Corporation
(NOKIA-RPM-GPG-KEY) <portal.support@nokia.com>)
```

5

If the command output indicates a provider other than Nokia or other recognizable providers, contact technical support.

6

Record the *version* and *release* values.

7

Enter the following for each key:

```
# rpm -qi gpg-pubkey-version-release ↵
```

The GPG key information is displayed; the following is the Nokia GPG public key information:

```
Name        : gpg-pubkey
Version     : version
Release     : release
Architecture: (none)
Install Date: date time
Group       : Public Keys
```

```
Size        : 0
License     : pubkey
Signature   : (none)
Source RPM  : (none)
Build Date  : date time
Build Host  : localhost
Relocations : (not relocatable)
Packager    : Nokia Corporation (NOKIA-RPM-GPG-KEY) <portal.
support@nokia.com>
Summary     : gpg(Nokia Corporation (NOKIA-RPM-GPG-KEY) <portal.
support@nokia.com>)
Description :
-----BEGIN PGP PUBLIC KEY BLOCK-----
GSG public key information
-----END PGP PUBLIC KEY BLOCK-----
```

8

To verify an RPM-file signature using the GPG key, enter the following:

```
# rpm -v -K RPM_file ↵
```

where *RPM_file* is the absolute path of the RPM file to check

Signing information like the following is displayed.

```
RPM_file:
    Header V4 RSA/SHA1 Signature, key ID key_ID: OK
    Header SHA1 digest: OK (SHA1_message_digest)
    V4 RSA/SHA1 Signature, key ID key_ID: OK
    MD5 digest: OK (MD5_message_digest)
Signature   : (none)
rpm -qpi RPM_file
Name        : RPM-file
Epoch       : 0
Version     : R.r.0
Release     : rel.v
Architecture: x86_64
Install Date: (not installed)
Group       : Applications/Communications
Size        : file_size
License     : YYYY, Nokia
Signature   : RSA/SHA1, date time, Key ID key_ID
```

```
Source RPM   : RPM_file
Build Date   : data time
Build Host   : hostname
Relocations  : (not relocatable)
Packager     : Nokia
Vendor       : Nokia
URL          : http://www.nokia.com
Summary      : content_descriptor
Description  :
```

9

Review the information.

The Signature output is as shown above for a signed file; for an unsigned file, the Signature output is the following:

```
Signature    : (none)
```

10

If the key ID matches the version recorded in Step 6 for the Nokia key, and the file is signed, the file is valid; otherwise, contact technical support.

11

Close the console window.

END OF STEPS

13.17 Common Access Card security

13.17.1 Enabling CAC

The NFM-P supports Common Access Card, or CAC, security, in which an access card and an Active Directory Federation Service, or ADFS, validate client access. Enabling the function is described in each NFM-P system deployment procedure.

13.18 GUI client deployment

13.18.1 Single-user GUI client and client delegate server deployment

The following NFM-P GUI client deployment scenarios are supported:

- separate single-user client installations
- remote user connections to a common client instance on a client delegate server

You can install multiple single-user GUI clients on one station, or on separate stations. The multiple clients installed on one station can be at various releases and associated with the different NFM-P systems.

You can also configure one single-user client to connect to multiple NFM-P systems. For information , see 13.19 “To configure a GUI client login form to list multiple NFM-P systems” (p. 394).

A client delegate server allows NFM-P access to multiple remote clients using one client software instance. If multiple client delegate servers are required, they are deployed on separate stations.

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 or client delegate server 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 also automatically applied.

See the following for client installation and upgrade information:

- “NFM-P single-user GUI client installation” (p. 585)
- “NFM-P client delegate server installation” (p. 591)

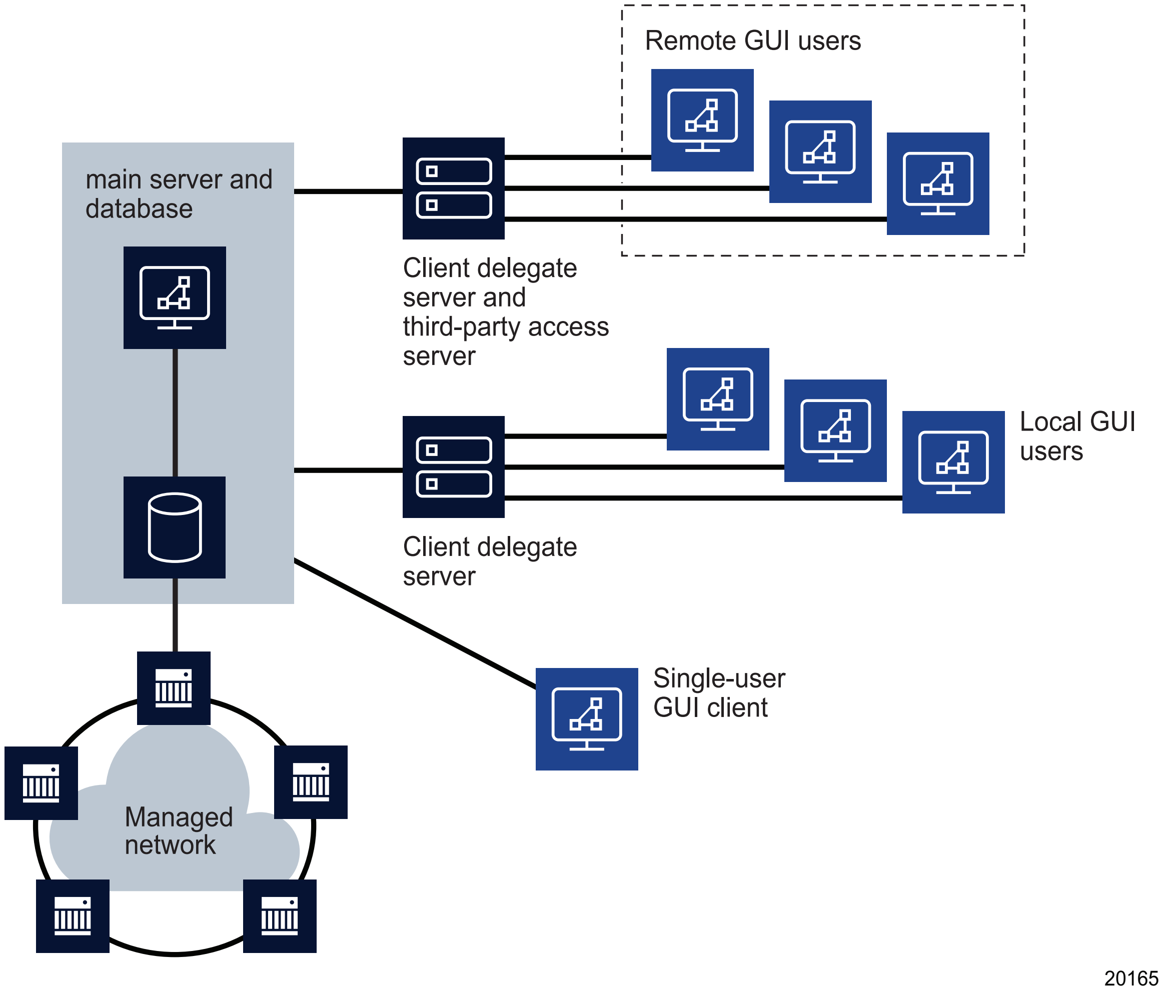
13.18.2 Client delegate servers

A client delegate server supports multiple simultaneous GUI sessions using one client software installation. A client delegate server can host local and remote user sessions, and supports the use of a third-party remote access tool such as a Citrix gateway. Client delegate server deployment is supported on multiple platforms.

A GUI session that is opened through a client delegate server is functionally identical to a single-user client GUI session. The client delegate server locally stores the files that are unique to each user session, such as the client logs and GUI preference files, using a directory structure that includes the RHEL or Windows username.

Figure 13-2, “Client delegate servers” (p. 393) shows two client delegate servers in an NFM-P management network. Multiple local users log in to a client delegate server directly, and remote users log in through a client delegate server that hosts a third-party access tool, for example, a Citrix gateway. Another local user opens a session on a single-user client station.

Figure 13-2 Client delegate servers



If a client delegate server becomes unreachable, the NFM-P raises an alarm and changes the color of the associated session entries in the GUI. The alarm clears when the server is again reachable.

You can use the client software on a client delegate server from the local console. It is recommended that you install a client delegate server, rather than a single-user client, to facilitate the deployment of additional clients.

A main server monitors the registered client delegate servers and displays information about them in the GUI. To register a client delegate server, you specify the client delegate server IP address and installation location during main server installation, upgrade, or configuration.

You can use a client GUI to list the following:

- registered client delegate servers and the availability of each

- active client delegate server sessions
- active client sessions on a specific client delegate server
- active client sessions for a specific NFM-P user

The number of allowed NFM-P client sessions on a client delegate server is configurable as a threshold using the client GUI. If a user tries to open a client session that reaches or exceeds the threshold, the session proceeds and the client delegate server raises an alarm. This threshold-crossing function can help to balance the session load across multiple client delegate servers. You require the Update user permission on the Server package to configure the threshold.

The following restrictions apply to client delegate servers.

- The installation of only one client delegate server on a station is supported.
- You cannot change a single-user client to a client delegate server.
- A client delegate server connects to one release of main server; multiple main servers to which the client delegate server connects must be at the same release.
- Depending on the platform type, specific deployment requirements and restrictions may apply.

13.18.3 Software upgrades

After an NFM-P main server upgrade, a single-user GUI client or client delegate server 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.

13.18.4 Configuration updates

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 instance detects and applies the update at the start of the next client session. See the *NSP System Administrator Guide* for information about globally updating the client configurations.

ℹ **Note:** A client backs up the existing configuration files as part of a configuration update.

13.19 To configure a GUI client login form to list multiple NFM-P systems

13.19.1 Purpose

By default, an NFM-P GUI client login form lists the main servers in one NFM-P system. If you manage multiple NFM-P systems at the same release, you can configure one login form to list the main servers in each system as login options.

Note: You cannot configure a client delegate server to display multiple server options on the client login form. If you need client connections to multiple NFM-P systems through a client delegate server, you must install one client delegate server software instance for each system.

Observe the following.

- All main servers to which the client connects must be at the same NFM-P release.
- The TLS truststore of the client must trust each NFM-P system in the multi-system configuration, which requires that the certificate of each system is signed by the same CA.
- You can choose among multiple main servers only if you open the client using the desktop icon.
- Performing a client download from the NFM-P https://*server*:*port*/client/ page overwrites the multiple-server configuration.
- Uninstalling the client removes the client from the configuration of each main server listed on the login form.

13.19.2 Steps

1

Click on Application→Exit to close the NFM-P client GUI, if it is open. The client GUI closes.

2

Navigate to the client configuration directory, which by default is /opt/nsp/client/nms/config on RHEL, and C:\nsp\client\nms\config on Windows.

3

Open the nms-client.xml file using a plain-text editor.

4

Find the lines that begin with the <j2ee> and <systemMode> tags.

By default, the lines contain the IP address and port of each main server in the NFM-P system specified during the client installation.

5

For each standalone main server or redundant main server pair to display on the client GUI login form, perform the following steps:

1. Copy the <j2ee> and <systemMode> sections.
2. Paste the sections after the original <j2ee> and <systemMode> sections.
3. Change the ejbServerHost IP address to the IP address or hostname of either main server in the system.
4. Change the haJndiServerIpAddressOne and haJndiServerIpAddressTwo to the IP address or hostname of the main servers in the system.

   Note: For a standalone system, leave haJndiServerIpAddressOne and haJndiServerIpAddressTwo blank.

5. Optionally, change the nameOne parameter for a standalone system, or the nameOne and nameTwo parameters for a redundant system.

   Note: Optionally, the nameOne and nameTwo values can be used as labels to help identify the NFM-P system. The nameOne and nameTwo parameters do not need to match the network domain of the main servers, and may be the same for the primary and standby main servers in a redundant system. In a standalone system, leave nameTwo blank.

6. Save the changes and close the file.

6

Log in to the client GUI. The Server drop-down menu lists the multiple main servers.

END OF STEPS

IGP topology data source configuration

13.20 Configuring the IGP topology data source

13.20.1 Purpose

The default IGP topology data source for the Network Supervision and Service Supervision applications depends on the NSP deployment type. For some deployment types, you can configure an alternative data source, as shown in Table 13-4, "IGP topology data sources" (p. 397).

See 13.21 "To change the IGP topology data source" (p. 397) for information about how to change the IGP topology data source for the Network Supervision and Service Supervision applications.

Table 13-4 IGP topology data sources

Deployment type	Default data source	Alternative data source
Resource control-only	CPAM	Not configurable
NSP deployment with classic and IP management	VSR-NRC	CPAM
NSP deployment with optical and classic IP management	VSR-NRC	CPAM
NSP deployment for model-driven management only	VSR-NRC	Not configurable

13.21 To change the IGP topology data source

13.21.1 Purpose

Perform this procedure to specify an IGP topology data source other than the default for the Network Supervision and Service Supervision applications.

See Table 13-4, "IGP topology data sources" (p. 397) for a list of the supported IGP topology data sources for each deployment type.

Note: It is strongly recommended that you contact technical support before changing the IGP topology data source.

Note: You must perform the procedure on the NSP cluster in each data center.

Note: *release-ID* in a file path has the following format:

R.r.p-rel.*version*

where

R.r.p is the NSP release, in the form *MAJOR.minor.patch*

version is a numeric value

13.21.2 Steps

1

Log in as the root user on the NSP deployer host.

2

Open a console window.

3

Open the following file using a plain-text editor such as vi:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

4

Locate the section that begins with the following:

```
nspos:
```

5

Edit the topologySource parameter in the igp subsection to read:

ℹ **Note:** If no source is specified, the NSP uses the default for the deployment listed in Table 13-4, “IGP topology data sources” (p. 397).

```
igp:
  topologySource:  "source"
```

where *source* is one of the following:

- CPAM
- SDN, which specifies the VSR-NRC

6

Save and close the file.

7

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

8

Enter the following:

```
# ./nspdeployerctl install --config ↵
```

9

Log in as the root user on the NSP cluster host.

10

Open a console window.

11

Enter the following:

```
# helm uninstall assurance-tomcat -n $(helm list -A | awk
'/assurance-tomcat/ {print$2;exit}') ↵
```

12

Return to the NSP deployer host console window.

13

Enter the following:

```
# /opt/nsp/NSP-CN-DEP-release-ID/bin/nspdeployerctl install --deploy ↵
```

The configuration is applied.

14

Close the console window.

END OF STEPS

14 NSP component installation

14.1 Overview

14.1.1 Purpose

This chapter describes the installation of NSP components in addition to the NSP cluster for standalone, HA, and DR deployments.

14.1.2 Contents

Installing NSP components

14.2 NSP component installation overview

14.2.1 Component installation support

The chapter includes procedures for installing the following:

- NSP Flow Collector Controllers and NSP Flow Collectors—see “NSP Flow Collector / Flow Collector Controller installation” (p. 404)
- NSP analytics servers—see “NSP analytics server installation” (p. 414)
- WS-RC—see “WS-RC installation” (p. 424)
- VSR-NRC—see “VSR-NRC installation” (p. 426)
- NFM-P—see “NFM-P installation” (p. 431)

Note: Some components such as NSP Flow Collector Controllers and NSP Flow Collectors can be installed independently, and do not need to be installed as part of a larger NSP deployment. See the component installation procedure for information.

Before you attempt to perform a procedure in this chapter, you must ensure that your planned deployment meets the hardware and software requirements described in the *NSP Planning Guide*.

Note: It is strongly recommended that you verify the GPG signature of each RPM file that you download from Nokia to ensure that each file has a valid Nokia signature.

Note: It is strongly recommended that you verify the message digest of each NSP image file or software bundle that you download from the Nokia Support portal. The download page includes the MD5, SHA256, and SHA512 checksums for comparison with the output of the RHEL md5sum, sha256sum, or sha512sum command. See the associated RHEL man page for command usage information.

NSP Flow Collector / Flow Collector Controller installation

14.3 To install NSP Flow Collectors and Flow Collector Controllers

14.3.1 Purpose

Perform this procedure to install one or more NSP Flow Collectors and Flow Collector Controllers, which support collocated and distributed deployment.

Note: For a small-scale deployment, you can collocate an NSP Flow Collector Controller and an NSP Flow Collector on one station, as described in the procedure. A small-scale deployment has a maximum of two stations, and supports the following:

- standalone—one station that hosts a Flow Collector Controller and Flow Collector, and a second station that hosts only a Flow Collector
- redundant—two stations that each host a Flow Collector Controller and Flow Collector

Note: The root user password on each NSP Flow Collector Controller and Flow Collector station must be identical.

Note: An NSP Flow Collector or Flow Collector Controller uninstallation backs up the component configuration files in the /opt/nsp/backup_flow directory on the station. A subsequent NSP Flow Collector or Flow Collector Controller installation on the station automatically reloads the saved configuration files. If you do not want the previous configuration restored during a subsequent installation, you must delete the /opt/nsp/backup_flow directory before the installation.

Note: The install.sh utility requires SSH access to a target station. To enable SSH access, you must do one of the following.

- Configure the required SSH keys on the stations.
- If each remote station has the same root user password, include the --ask-pass argument in the install.sh command; for example:

```
./install.sh --ask-pass --target remote_station
```

14.3.2 Steps

1

Download the NSP component installer package NSP_NSD_NRC_*R_r*.tar.gz) from OLCS and extract it on any station running a supported version of RHEL. This does not have to be the station on which an NSP Flow Collector Controller or Flow Collector is to be installed; the installer can perform remote installations.

Note: In subsequent steps, the directory is called the *NSP_installer_directory*.

The *NSP_installer_directory*/NSD_NRC_*R_r* directory is created, where *R_r* is the NSP release identifier in the form *MAJOR_minor*.

2

Open a console window.

3

Enter the following as the root user:

```
# cd NSP_installer_directory/NSD_NRC_R_r ↵
```

4

Create a hosts file in the current directory that contains the required entries in the following sections:

- [nspos]—one entry for each ZooKeeper host; the ZooKeeper hosts are one of the following:
  - if the NSP system includes only the NFM-P, the NFM-P main servers
  - otherwise, the VIP address of each NSP cluster
- [fcc]—one line entry for each Flow Collector Controller
- [fc]—one line entry for each Flow Collector

Note: If an NSP Flow Collector Controller and Flow Collector are to be collocated on one station, specify the same address for in the [fc] and [fcc] sections; for example:

```
[fcc] 203.0.113.3 advertised_address=198.51.100.3 ansible_host=
198.51.100.3
[fc] 203.0.113.3 ansible_host=198.51.100.3 fc_mode=AA
```

See 13.3 “NSP hosts file” (p. 364) for configuration information.

Note: A sample hosts file is in the following directory; you must use a modified copy of the file for installation:

- *NSP_installer_directory*/NSD_NRC_*R_r*/examples

  where *R_r* is the NSP software release

5

Create a config.yml file in the NSP installer directory that includes the following sections; see 13.4 “NSP RPM-based configuration file” (p. 366) for information.

- multi-component deployment:
  - **sso**
  - **tls**
  - section for each component to install
- independent deployment, for example, if you are adding a Flow Collector or Flow Collector Controller to an NFM-P-only system:
  - **sso**
  - **tls**

Note: The following parameter values in the **tls** section must match the values in the NSP configuration file; otherwise, the values must match the values in the NFM-P main server configuration:

- secure
- PKI server parameters
  You can use the samconfig “show” command on a main server to display the **tls** parameters. See 14.9 “NFM-P samconfig utility” (p. 432) for information about using the samconfig utility.

Note: A sample config.yml file is in the following directory; you must use a modified copy of the file for installation:

- *NSP_installer_directory*/NSD_NRC_*R_r*/examples
  where *R_r* is the NSP software release

6

If you intend to use the PKI server, start the PKI server.

1. Log in as the root user on the NSP cluster host.
2. Open a console window.
3. Enter the following:
   ```
   # cd /opt/nsp/NSP-CN-release-ID/tools/pki ↵
   ```
4. Enter the following:
   ```
   # ./pki-server ↵
   ```
   The PKI server starts, and the following is displayed:
   ```
   date time Using Root CA from disk, and serving requests on port
   nnnn
   ```

7

Enter the following:

```
# cd NSP_installer_directory/NSD_NRC_R_r/bin ↵
```

8

Enter the following:

Note: Include the --ask-pass option only if each target station has the same root user password.

```
# ./install.sh --ask-pass --target target_list ↵
```

where *target_list* is a comma-separated list of the NSP Flow Collector Controller and NSP Flow Collector internal IP addresses

The NSP Flow Collector Controller or NSP Flow Collector software is installed on the stations.

Configure NFM-P in DR deployment

9

If the NSP cluster and NSP Flow Collector Controllers are not deployed in a DR deployment, go to Step 15.

10

Log in as the root user on the NFM-P main server in the same data center as the NSP Flow Collector Controller.

11

Open a console window.

12

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.

5. Enter the following to switch back to the root user:

   ```
   bash$ su ↵
   ```

6. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to display the nspOS service status:

   ```
   # nspdctl status ↵
   ```

   Information like the following is displayed.

   ```
   Mode:     DR
   Role:     redundancy_role
   DC-Role:  dc_role
   DC-Name:  dc_name
   Registry: IP_address:port
   State:    stopped
   Uptime:   0s
   SERVICE          STATUS
   service_a        inactive
   service_b        inactive
   service_c        inactive
   ```

You must not proceed to the next step until all NSP services are stopped; if the State is not ‘stopped’, or the STATUS indicator of each listed service is not ‘inactive’, repeat this substep.

13

You must create an association between the local NSP Flow Controller and the local NFM-P main server to ensure that the Flow Collector and Controller remain in communication with the local NFM-P during NSP DR activity.

Add the local data center name to the main-server configuration.

Note: The data center name must be a name other than “default”.

1. Enter the following:

   ```
   # samconfig -m main ↵
   ```

   The samconfig utility opens, and the following is displayed:

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

2. Enter the following:

   ```
   <main> configure nspos dc-name data_center ↵
   ```

   where *data_center* is the data center name, which must match the **dcName** value for the local NSP cluster in the NSP configuration file

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

3. Enter the following:

   ```
   <main configure nspos> exit ↵
   ```

   The prompt changes to `<main>`.

4. Enter the following:

   ```
   <main> apply ↵
   ```

   The configuration is applied.

5. Enter the following:

   ```
   <main> exit ↵
   ```

   The samconfig utility closes.

14

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.

Start NSP Flow Collector Controllers

15

Perform the following steps on each NSP Flow Collector Controller station.

Note: If an NSP Flow Collector is also installed on the station, the Flow Collector starts automatically.

1. Log in to the station as the nsp user.
2. Enter the following:

   ```
   bash$ /opt/nsp/flow/fcc/bin/flowCollectorController.bash start ↵
   ```

   The NSP Flow Collector Controller starts.
3. Close the console window.

Configure NSP Flow Collector Controllers

16

Perform Step 18 to Step 24 for each NSP Flow Collector Controller.

17

Go to Step 25.

18

Use a browser to open the following URL:

https://*server*:8443/fcc/admin

where *server* is the NSP Flow Collector Controller IP address or hostname

19

When the login form opens, enter the required user credentials and click OK. The default user credentials are available from technical support.

The NSP Flow Collector Controller page opens.

20

Click on the NFM-P Configuration tab.

21

Configure the parameters in the following table.

Table 14-1 NSP Flow Collector Controller parameters, NFM-P Configuration tab

Parameter	Description
NFM-P	
Active	The public IP address or hostname of the standalone main server, or the primary main server in a redundant deployment
Standby	The public IP address or hostname of the standby main server in a redundant deployment
XML API	
User Name	The NFM-P user for XML API file transfers
Password	The NFM-P user password for XML API file transfers
HTTPS Port	The HTTPS port for file transfers
JMS	
JNDI Port	The TCP port on the main server for JMS communication
Reconnect	Whether the NSP Flow Collector attempts to reconnect to the NFM-P after a connection failure
Durable	Whether the NFM-P JMS subscription is durable
Reconnect Attempts	The number of times to attempt to reconnect to the NFM-P after a connection failure
Reconnect Delay	The time, in seconds, to wait between NFM-P reconnection attempts
Connection Timeout	The time, in seconds, to wait for a response to an NFM-P connection attempt
File Transfer	
Protocol	The protocol to use for main server file transfers
Port	The main server TCP port for file transfers
User Name	The FTP or SFTP username required for main server transfers from the
Password	The FTP or SFTP password for file transfers from the main server

22

Click Save NFM-P configuration.

23

Click on the Operations tab.

24

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.

a. If the NSP Flow Collectors are to collect AA flow statistics, click Force AA Snapshot Extraction.

b. If the NSP Flow Collectors are to collect system flow statistics, click Force SYS Snapshot Extraction.

The NSP Flow Collector Controller extracts the managed network information from the NFM-P.

Start NSP Flow Collectors

25

Start each NSP Flow Collector that is not collocated with an NSP Flow Collector Controller.

Note: Any NSP Flow Collector that is collocated with a Flow Collector Controller is automatically started earlier in the procedure.

1. Log in to the NSP Flow Collector station as the nsp user.
2. Enter the following:

```
bash$ /opt/nsp/flow/fc/bin/flowCollector.bash start ↵
```

   The NSP Flow Collector starts.
3. Close the console window.

Configure NSP Flow Collectors

26

As required, perform the following steps on each NSP Flow Collector station to specify the NEs from which the NSP Flow Collector is to collect statistics.

1. Use a browser to open the following URL:

   https://*server*:8443/fc/admin

   where *server* is the NSP Flow Collector IP address or hostname

   The Collection Policy configuration page opens.
2. Click Add. A new table row is displayed.
3. Configure the following parameters:
   - System ID

     The System ID value must match the System ID that the NFM-P associates with the NE, for example, as shown on the NE properties form in the GUI.

You can specify multiple MDAs on one NE by adding one table row for each MDA and using the same System ID in each row.

- Description
- Source IPFIX Address

  The Source IPFIX Address value is the NE address specified in the discovery rule for the NE.
- Port

4. If the NSP Flow Collector is to collect system Cflowd statistics, use the Flow Protocol drop-down to choose a protocol.
5. To delete an NE, select the Delete on save check box beside the NE.
6. Click Save Configuration. The configuration is saved.

27

Click on the Aggregation Policy tab.

28

Perform one of the following:

a. If the NSP Flow Collector is to collect system Cflowd statistics, select the required aggregation types from the tabs in the lower panel.

b. If the NSP Flow Collector is to collect AA statistics, select one or more statistics classes in the Subscriber Collection panel to enable aggregation for the classes.

29

Configure the aggregations.

Note: The statistics collection interval affects NSP Flow Collector performance. A larger interval results in proportionally larger files, which take longer to store and transfer.

Note: For BB NAT statistics, you must set the collection interval no higher than the following, based on the expected flow rate:

- 350 000 flows/sec—1 minute
- 80 000 flows/sec—5 minutes
- 40 000 flows/sec—15 minutes

  You can achieve the statedrates only if you use a remote FTP client to retrieve the records and do not enable the record transfer in Step 30.

  If you enable the record transfer in Step 30, you must set the collection interval no higher than the following, based on the expected flow rate:
- 100 000 flows/sec—1 minute
- 50 000 flows/sec—5 minutes
- 25 000 flows/sec—15 minutes

1. Use the Interval drop-down menus in the Aggregation Intervals panel to specify the aggregation interval for each statistic type, as required.

2. The Interval Closing Timeout parameter specifies a latency value that is applied at the end of a collection interval to ensure that any queued statistics are written to the current file. Typically, the default value of one second is adequate; configure the parameter only at the request of technical support.
3. Click on the tab in the lower panel that corresponds to the statistic type.
4. Select or deselect aggregations, as required.

30

Configure the transfer of BB NAT records in CSV format to a file server, if required.

ℹ **Note:** A minimum 1 Gbyte/s link is required between the NSP Flow Collector and the file server.

ℹ **Note:** SFTP transfers are considerably slower than FTP transfers.

1. Click on the NAT Transfer tab.
2. Configure the parameters:
   - Enable Transfer—whether file transfers are enabled
   - Transfer Protocol—FTP or SFTP
   - IP Address / Host name—file server address
   - Port—file server port
   - Location—file server directory that is to contain the files
   - User—FTP or SFTP username
   - Password—FTP or SFTP password

31

Click Save Configuration. The configuration is saved.

32

Close the open browser pages.

33

If no other components are to be deployed, stop the PKI server by entering Ctrl+C in the console window.

34

Close the open console windows.

End of steps

NSP analytics server installation

14.4 To install an NSP analytics server

14.4.1 Purpose

CAUTION

Installation Failure

If you attempt to install an analytics server before the NSP Analytics function is fully initialized, the installation may fail.

Before you attempt to install an analytics server, you must ensure that the NSP Analytics function is fully initialized.

The following steps describe how to install the NSP analytics server software on a station.

Note: Each running NSP analytics server and each running auxiliary database in the NSP system must be at the same release.

Note: Performing the procedure creates the nsp user account on the analytics server station.

Note: You require the following user privileges:

- on each main server station—root, nsp
- on the analytics server 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

14.4.2 Steps

Verify NFM-P configuration

1

If one of the following is true, go to Step 3:

- The NSP system does not include the NFM-P.
- The NSP system includes the NFM-P, but IP validation on each main database is not enabled.
- The NSP system includes the NFM-P, and IP validation on each NFM-P main database is enabled and configured to include the IP address of each NSP analytics server.

2

In an NSP system that includes an NFM-P with IP validation enabled, you must ensure that each analytics server is listed as a remote server in the NFM-P IP validation configuration of each NFM-P main database.

Also, you must ensure that each system is running before you install an analytics server. Otherwise, analytics report generation is compromised.

Perform the following high-level steps to configure IP validation in each NFM-P system that communicates with the analytics servers.

For information about starting and stopping NFM-P components, see the *NSP System Administrator Guide*.

For information about using the samconfig utility, see 14.9 “NFM-P samconfig utility” (p. 432).

1. Stop each main server; in a redundant system, you must stop the standby main server first.
2. Stop the standalone or primary main database.
3. Use the samconfig utility on the main database station to add each analytics-server IP address to the **remote-servers** parameter in the **ip-validation** section.
4. Start the main database.
5. Start the main server.

   Note: You must not proceed to the next step until the standalone or primary main server is fully initialized and operational.
6. If the NFM-P system is a standalone system, go to Step 4.
7. Use the samconfig utility on the standby main database station to add each analytics-server IP address to the **remote-servers** parameter in the **ip-validation** section.
8. Start the standby main database.
9. Start the standby main server.

Install analytics server packages

3

If the NSP system includes an NFM-P system that is not currently running, start the NFM-P system; see the *NSP System Administrator Guide* for information about starting the NFM-P.

4

Log in as the root user on the analytics server station.

5

Download the following 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 number

6

Open a console window.

7

Ensure that the analytics server hostname, or an analytics server IP address that can be resolved by a DNS server, is configured in the /etc/hosts file on the analytics server station.

8

Navigate to the directory that contains the downloaded installation files.

9

Enter the following:

```
# chmod +x *.rpm ↵
```

10

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

11

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

Obtain required system files

12

If you are installing the first of multiple analytics servers, go to Step 18.

13

Enter the following to switch to the nsp user:

```
# su - nsp ↵
```

14

Transfer the following files from the first installed analytics server to the /opt/nsp directory on the analytics server that you are currently installing:

Note: If for any reason you uninstall the analytics software after you copy the files, for example, if the initial installation attempt fails, you must copy the files again before you retry the installation.

- /opt/nsp/.jrsks
- /opt/nsp/.jrsksp

15

Enter the following:

```
# chown nsp:nsp /opt/nsp/.jrsks ↵
```

16

Enter the following:

```
# chown nsp:nsp /opt/nsp/.jrsksp ↵
```

17

If you are currently operating on the final analytics server to be installed, perform the following steps on each analytics server other than the first installed analytics server to restart the analytics server.

Note: You must not restart the first installed analytics server, only the other analytics servers. The restarts are required in order to correctly establish communication among the analytics servers.

1. Log in to the analytics server station as the nsp user.
2. Enter the following to stop the analytics server:

   ```
   bash$ /opt/nsp/analytics/bin/AnalyticsAdmin.sh stop ↵
   ```

3. Enter the following to start the analytics server:

   ```
   bash$ /opt/nsp/analytics/bin/AnalyticsAdmin.sh start ↵
   ```

Configure analytics server

18

If you are manually configuring TLS, perform the following steps.

Note: For information about manual TLS configuration in an NSP system, including generating keystore and truststore files, see 4.9 “To generate custom TLS certificate files for the NSP” (p. 108).

1. Enter the following to switch to the root user, if you are not currently root:

   ```
   bash$ su - ↵
   ```

2. Transfer the required TLS keystore and truststore files to the analytics server station.

   Note: The files must be located on a path that is owned by the nsp user.

3. Enter the following:

   ```
   # chown nsp:nsp keystore_file ↵
   ```

   where *keystore_file* is the absolute path of the keystore file

4. Enter the following:

   ```
   # chown nsp:nsp truststore_file ↵
   ```

   where *truststore_file* is the absolute path of the truststore file

19

Enter the following to switch to the nsp user, if you are not currently nsp:

```
# su - nsp ↵
```

20

Enter the following:

```
bash$ cd /opt/nsp/analytics/bin ↵
```

21

Enter the following:

```
bash$ ./AnalyticsAdmin.sh updateConfig ↵
```

The script displays the following message and prompt:

```
THIS ACTION UPDATES THE CONFIG FILE
Please type 'YES' to continue
```

22

Enter YES.

The script displays the following, and the first in a series of prompts.

```
Config file found.
```

23

At each prompt, enter a parameter value; to accept a default in brackets, press ↵.

The following table lists and describes each parameter.

Table 14-2 NSP analytics server parameters

Parameter	Description
Analytics Server Hostname or IP Address	The analytics server hostname or IP address that is reachable by the NSP cluster and the client browsers Default: —
Enter IP address or hostname for internal network	The analytics server internal IP address, if configured Default: —
Is NSPOS secure	Whether the internal NSP system communication is secured using TLS In a shared-mode NSP system, the value must match the "nspos secure" parameter value; otherwise, the value must match the "secure" value in the nspos section of the NFM-P main server configuration. Default: true
Use internal certificates	Whether internal service communication between NSP components is secured using internally generated TLS certificates You can set the parameter to true only if the "Is NSPOS secure" parameter is set to true. Default: true
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 • the internalAdvertisedAddress value in the primary or standalone NSP configuration file, if configured; otherwise, the advertisedAddress value Default: —
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 • the internalAdvertisedAddress value in the standby NSP configuration file, if configured; otherwise, the advertisedAddress value Default: —
Primary Oracle Data Source DB Host	The primary or standalone main database IP address or hostname Default: —
Primary Oracle Data Source DB Name	The primary or standalone main database instance name Default: —
Primary Oracle Data Source DB Port	The TCP port on the primary or standalone main database station that receives database requests Default: 1523

Table 14-2 NSP analytics server parameters (continued)

Parameter	Description
Secondary Oracle Data Source DB Host	In a redundant system, the standby main database IP address or hostname Default: —
Secondary Oracle Data Source DB Name	In a redundant system, the standby main database instance name Default: —
Secondary Oracle Data Source DB Port	In a redundant system, the TCP port on the standby main database station that receives database requests Default: 1523
PKI Server IP Address or Hostname	The PKI server IP address or hostname Regardless of whether you are using the manual or automated TLS configuration method, you must specify the PKI server address. Default: —
PKI Server Port	The PKI server port Default: 2391
Zookeeper Connection String	The IP address or hostname, and port of each ZooKeeper host, in the following format: `server1_address:port;server2_address:port` where *server1_address* and *server2_address* are the IP addresses or hostnames of the ZooKeeper hosts *port* is a port number based on the **Is NSPOS secure** setting: • 2181, if false • 2281, if true **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** • **the advertisedAddress of each cluster from the NSP configuration file** Default: —
Use NFM-P-only mode? (true/false)	Specifies how the Analytics server communicates with the NSP system The parameter must be set to true if the deployment includes only the NFM-P and has no NSP cluster. Default: false

24

Start the PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 4.10 “To configure and enable a PKI server” (p. 113).

Note: The PKI server is required for internal system configuration purposes.

25

Enter the following to install the analytics server software:

```
bash$ ./AnalyticsAdmin.sh install ↵
```

Note: The analytics server starts automatically after the installation.

The following prompt is displayed if the Use NFM-P-only mode parameter in Step 23 is set to false.

```
Enter NSP user name:
```

26

If the prompt is displayed, perform the following steps.

1. Enter admin ↵.

   The following prompt is displayed:

   ```
   Enter NSP user password (hidden):
   ```
2. Enter the password of the NSP admin user.

27

The following messages and prompt are displayed:

```
Access token retrieved successfully

date time Analytics App is UP and Running

Version check passed. NSP version = RR.r; Analytics server version =
RR.r

date time Installing Analytics Server...

Do you have existing TLS certificates?(yes/no)
```

28

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 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 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 messages and prompt are displayed:

```
Verifying TLS Keystore...

Certificate loading...

Verified TLS Certificate

Enter TLS Truststore Password:
```

5. Enter the truststore password.

   The following messages and prompt are displayed:

   ```
   Verifying TLS Truststore...

   Certificate loading...

   Verified TLS Certificate

   TLS Config has been updated
   ```

29

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
   (directory must be owned by nsp user):
   ```

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

   Modified JIRoles Table
   ```

30

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...
Start Deploying report
.
.
.
All reports successfully tracked
Analytics Server configured successfully
date time Analytics Server successfully installed
```

31

Enter the following to view the analytics server status; ensure that the server is running:

```
bash$ ./AnalyticsAdmin.sh status ↵
```

The following is displayed if the analytics server is running:

```
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
TLS TrustStore File Path : path
```

32

If no other components are to be deployed, stop the PKI server by entering Ctrl+C in the console window.

33

Close the open console window.

END OF STEPS

WS-RC installation

14.5 To install the WS-RC

14.5.1 Purpose

Use this procedure to install the WS-RC product as an NSP system component. The WS-RC shares a host server with the WS-NOC.

14.5.2 Before you begin

Prior to installing an WS-RC server, ensure that the following criteria are met:

- An WS-NOC server running Release 20.11.0-55 or later has been deployed
- A directory entitled *NFMT-<release_load>* exists within the */DEPOT* directory
- The WS-NOC release software is available from the */DEPOT/NFMT-<release_load>* directory

14.5.3 Steps

1

Login to the server that will host the WS-RC software as the root user.

2

Download the WSRC_<*software_load*>.tar.gz file to the /DEPOT/WSNOC-<*release_load*> directory.

where

<*software_load*> is the numbered WS-RC software release, such as 20.11.0-26.

<*release_load*> is the numbered WS-NOC software release, such as 20.11.0-55.

3

Verify the *cksum*.

4

Extract the WS-RC software bundle. Execute the following command:

```
cd /DEPOT/WSNOC-<release_load>;tar -xvzy WSRC_<software_load>.tar.gz
```

where

<*release_load*> is the numbered WS-NOC software release, such as 20.11.0-55.

<*software_load*> is the numbered WS-RC software release, such as 20.11.0-26.

5

Start the PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 4.10 “To configure and enable a PKI server” (p. 113).

Note: The PKI server is required for internal system configuration purposes.

6

Install the latest mnc-setup*.rpm. Execute:

```
rpm -Uvh mnc-setup-<release_load>.noarch.rpm
```

Where <*release_load*> is the numbered mnc version, such as 20.11.0-114.

7

Enable the WS-RC option in the Autoinstall configurator (AI-C). Execute:

```
touch /var/autoinstall/NRCT
```

8

Ensure that WS-RC is selected as an optional component within the General Options of the AI-C.

9

Upgrade the bench as required according to the bench upgrade document.

10

If no other components are to be deployed, stop the PKI server by entering Ctrl+C in the console window.

11

Perform 11.8 “To integrate a containerized Release 21.12, 22.6, 22.12, 23.6, or 23.12 WS-NOC and the NSP” (p. 345).

END OF STEPS

VSR-NRC installation

14.6 VSR-NRC installation overview

14.6.1 VSR-NRC installation instructions

The *Virtualized Service Router (VSR) Installation and Setup Guide* installation instructions are to be used for the VSR-NRC. Information such as the installation and configuration workflow, the host machine requirements, and the creation of a VSR-NRC VM, are valid.

Note: If you are upgrading from NSP 22.11 or earlier, you must perform a special procedure in order to migrate the VSR-NRC to VSRi architecture. See the SR OS 23.3.R1 Release Notes for more information.

14.6.2 Software license

For a VSR-NRC to be fully functional, the system must load a valid license file at bootup. The license file encodes the allowed capabilities and features of the VSR-NRC system and is generated automatically when an NSP PCE license is purchased. Contact your Nokia account representative to obtain license file associated with an NSP PCE/VSR-NRC purchase order or trial request. For information about software installation and verification, see the *Virtualized Service Router (VSR) Installation and Setup Guide*.

14.6.3 Managing VSRi through MDM

VSRi can be managed through MDM when deployed in model-driven mode.

14.7 To commission the VSR-NRC for NSP management

14.7.1 Purpose

Perform this procedure after VSR-NRC installation to configure the VSR-NRC connection to the managed network, and to prepare the VSR-NRC for NSP management. Managing the VSR-NRC using NFM-P only applies if NFM-P is running the same software version as the rest of NSP.

Note: When the VSR-NRC will be integrated with a containerized NSP system for the purposes of using the NSP's PCE functionality, users must also configure the sros section of the nsp-config.yml file. See 6.6 “Configuring SROS” (p. 185) for more information.

14.7.2 Steps

Commission the VSR-NRC for management

1

Open a CLI session on the VSR-NRC VM.

2

If required, configure a static route on the VSR-NRC:

bof static-route *networkIP/mm* next-hop *nextHopIP* ↵

where

networkIP is the destination network IP address

mm is the subnet mask

nextHopIP is the IP address of the next hop in the static route

3

Enter the following commands in sequence to complete the BOF configuration:

bof persist on ↵

bof save ↵

4

Configure the VSR-NRC system address:

configure router interface system address *systemInterfaceIP/mm* ↵

where

systemInterfaceIP is the VSR-NRC system interface IP address

mm is the system interface subnet mask

5

Enter the following commands in sequence to complete the device commissioning:

Note: The commands used in this step must be altered to align with the VSR-NRC chassis, card, and MDA types configured in the VSR-NRC *domain.xml* file.

```
card 1
     card-type iom-v
     mda 1
         mda-type m20-v
         no shutdown
     exit
     no shutdown
exit
```

The VSR-NRC reboots. After the reboot, the NFM-P can discover the VSR-NRC.

Connect the VSR-NRC to the managed network

6

For managed network connectivity, and to establish peering sessions, the VSR-NRC VM requires network interfaces, or vNICs. Depending on your network architecture, you may need to provision multiple vNICs, create an additional network bridge, and bind the vNICs to the bridge.

The first vNIC must be mapped to the CFM-A management port. The second vNIC is reserved for CFM-B. Additional vNICs that you create are sequentially assigned as network ports 1/1/1, 1/1/2, and so on.

Perform the following to create vNICs:

Note: It is recommended that “virtio” is chosen as the device model of each interface. See the RHEL OS documentation for more information.

1. Open the RHEL Virtual Machine Manager, or virt-manager, tool.
2. Use the tool to add virtual network interfaces, as required.
3. When the creation of all interfaces is complete, restart the VSR-NRC VM.

After the VM restarts, the interfaces are shown as ports in the VSR-NRC configuration.

To configure the VSR-NRC for IP topology discovery

7

Connect the VSR-NRC to one or more ABRs in the network, ensuring that visibility to each area is possible.

8

Configure an interface for each area of the network connected to the ABRs. See the *7450 ESS, 7750 SR, 7950 XRS, and VSR Unicast Routing Protocols Guide* for more information.

9

Configure OSPF or IS-IS for each link. See the *7450 ESS, 7750 SR, 7950 XRS, and VSR Unicast Routing Protocols Guide* for more information.

10

Configure the router protocol to export the topology database to NSP. Enter the following commands on the VSR-NRC:

```
configure router ospf traffic-engineering ↵
```

```
configure router ospf database-export ↵
```

Note: To discover multiple IS-IS Level-1 topologies via IGP discovery, the VSR-NRC must be configured with multiple IS-IS instances that are each connected to one portion of the topology. Because the definition of a domain includes the instance number, each instance will appear as a separate domain within NSP. To prevent this, configure each instance with identical database-export identifier values. For example, execute this command on each instance: **`configure router isis database-export identifier 1 ↵`**

To configure the VSR-NRC for BGP-LS topology discovery

11

Connect the VSR-NRC to one or more routers (preferably ABRs) in the network.

> **Note:** To perform BGP-LS topology discovery, the VSR-NRC requires BGP peering (direct or via BGP Route Reflector) with at least one router in each IGP area.

12

Configure one or more interfaces to the selected router. See the *7450 ESS, 7750 SR, 7950 XRS, and VSR Unicast Routing Protocols Guide* for more information.

13

Configure OSPF or IS-IS on the link to achieve full IP reachability to the selected router. See the *7450 ESS, 7750 SR, 7950 XRS, and VSR Unicast Routing Protocols Guide* for more information.

14

Configure the VSR-NRC to peer with the selected router. See the *7450 ESS, 7750 SR, 7950 XRS, and VSR Unicast Routing Protocols Guide* for more information.

15

Configure the VSR-NRC to export BGP-LS to the NSP. Execute the following commands on the VSR-NRC:

```
configure router ospf traffic-engineering ↵

configure router ospf no database-export ↵

configure router bgp link-state-export-enable ↵

configure router bgp family ivp4 bgp-ls ↵
```

16

On each ABR peering with the VSR-NRC, execute the following commands:

```
configure router ospf traffic-engineering ↵

configure router ospf database-export identifier bgp-ls-identifier
bgpLspID ↵

configure router bgp link-state-import-enable ↵

configure router bgp family ipv4 bgp-ls ↵
```

where

- *identifier* specifies an entry ID to export

- *bgpLspID* specifies a BGP LS ID to export

To configure the VSR-NRC as a PCE

17

Enable PCE on the VSR-NRC. Execute the following commands:

```
configure router pcep pce local-address pcepIP ↵
configure router pcep pce no shutdown ↵
```

where *pcepIP* is the IPv4 or IPv6 address of the system interface, or any loopback interface, of the VSR-NRC

Note: The configuration of the PCE local address is only required if the user wants to establish a PCEP session from the PCC inband via the network interfaces. When a PCC establishes a PCEP session out-of-band, PCE uses the VSR-NRC management IP interface address as the local address and the above configuration is ignored.

To configure PCCs

18

Execute the following commands on all 7750 SR routers that will peer with the VSR-NRC (PCE):

```
configure router pcep local-address pcepIP no shutdown ↵
configure router pcep pcc peer VSR-NRCpcepIP no shutdown ↵
configure router pcep pcc no shutdown ↵
```

Where

pcepIP is the IPv4 or IPv6 address of the system interface - or any loopback interface - of the router. The configured local address is only used for establishing the PCEP session to the PCE inband via the network interfaces. When establishing PCEP out-of-band, the router’s management IP address is used, and the local address configuration is ignored. The user can configure three modes for the establishment of the PCEP session by the PCC: out-of-band with fallback to inband (default), inband only, or out-of-band only using the command ‘**`configure router pcep pcc peer route-preference {both | inband | outband}`**’

VSR-NRCpcepIP is the PCEP PCE IPv4 or IPv6 address of the VSR-NRC with which the routers will peer. When PCC establishes the PCEP session to PCE out-of-band, the VSR-NRC management IP interface address should be entered. Otherwise, the local address configured on the VSR-NRC PCE should be entered as explained in Step 17.

End of steps

NFM-P installation

14.8 Installing the NFM-P

14.8.1 Description

CAUTION

Service Disruption

An NFM-P system installation 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 Planning Guide, and the NSP 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 NSP professional services 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.

CAUTION

Support Liability

Failure to comply with the requirements and restrictions that apply to NFM-P system deployment may violate a support agreement.

NFM-P software installation is supported only under the conditions described in this guide.

Note: NFM-P installation is supported only for shared-mode NSP deployments. You cannot install an independent Release 22 NFM-P system. See 14.8.2 “Greenfield installations of independent NFM-P deployments” (p. 432) for more information.

Note: It is strongly recommended that you verify the message digest of each NSP image file or software bundle that you download from the Nokia Support portal. The download page includes the MD5, SHA256, and SHA512 checksums for comparison with the output of the RHEL md5sum, sha256sum, or sha512sum command. See the associated RHEL man page for command usage information.

Component configuration

Most NFM-P component configuration is performed using the samconfig utility. See 14.9 “NFM-P samconfig utility” (p. 432) for information.

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

14.8.2 Greenfield installations of independent NFM-P deployments

Greenfield installations of independent Release 22 NFM-P systems are not supported under normal circumstances; only installations in shared mode with an NSP cluster are supported. However, such a system installation may be required, for example, to rebuild a Release 22 system after a catastrophic failure.

In such a scenario, contact technical support to obtain the required installation procedure.

14.9 NFM-P samconfig utility

14.9.1 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

Note: The following NFM-P main server **aux** parameters remain in the samconfig utility, but are obsolete and not to be configured:

- calltrace
- pcmd
- webdav
- disable-cn-check
- custom-http-headers
- calltrace-pairs
- pcmd-pairs

Note: The following NFM-P auxiliary server **service** parameters remain in the samconfig utility, but are obsolete and not to be configured:

- pcmd
- calltrace

Note: The following NFM-P auxiliary server **tls** parameter remains in the samconfig utility, but is obsolete and not to be configured:

- disable-cn-check

14.9.2 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] nspos            + nspOs Configuration

   [no] remote-syslog    + Configuration of Remote Syslog Location for
Activity Logging

   [no] server-logs-to-remote-syslog +Configuration of logging the NFM-P
server logs to remote syslog server

   [no] hsm              + HSM Configuration

   [no] server-logs-to-opensearch + Configuration of logging the NFM-P
server logs to OpenSearch running at containerized NSP
```

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 14-3 Special characters in samconfig menus

Character	Meaning
+	The object has child objects or parameters.
-	The object does not have child objects or parameters.
*	The object has one or more mandatory parameters that are not configured.

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>

  FORMAT:              where IP is a valid Local IPv4 (xxx.xxx.xxx.xxx) or
IPv6 formatted address.

  VALID VALUES:        nnn.nnn.nnn.nnn

  MANDATORY:           true
```

14.9.3 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.

14.10 Using an NFM-P disk image

14.10.1 Description

You can deploy a collocated standalone NFM-P system in a lab or trial environment using a disk image. The image is available for deployment in a KVM or RHEL OpenStack environment.

Note: NFM-P system deployment using the image is not supported in a live network environment.

Note: NFM-P system deployment using the image supports only IPv4 addressing.

After you deploy the image, as described in 14.11 “To deploy a trial NFM-P system using a qcow2 disk image” (p. 435), the NFM-P system is operational.

14.11 To deploy a trial NFM-P system using a qcow2 disk image

14.11.1 Description

The following steps describe how to deploy a collocated standalone NFM-P system in a lab or trial environment using a disk-image.

Note: NFM-P system deployment as described in the procedure is not supported in a live network environment; the image is provided for testing or trial purposes only.

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

14.11.2 Steps

1

Check the *Host Environment Compatibility Reference for NSP and CLM* to ensure that the OS version of the host station supports the creation of VMs at the RHEL version that the NSP requires.

2

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

3

If the host station OS version supports NSP VM creation, enter the following; otherwise, update the host OS version as required:

```
# osinfo-query os | grep rhel | grep -v - ↲
```

A list of supported RHEL variants is listed, for example:

```
rhel7.8 | Red Hat Enterprise Linux 7.8 | 7.8 | http://redhat.
com/rhel/7.8
```

```
rhel7.9 | Red Hat Enterprise Linux 7.9 | 7.9 | http://redhat.
com/rhel/7.9
```

```
rhel8.0 | Red Hat Enterprise Linux 8.0 | 8.0 | http://redhat.
com/rhel/8.0

rhel8.1 | Red Hat Enterprise Linux 8.1 | 8.1 | http://redhat.
com/rhel/8.1

rhel8.2 | Red Hat Enterprise Linux 8.2 | 8.2 | http://redhat.
com/rhel/8.2
```

4

Record the appropriate RHEL version number in the left column, which is one of the following:

- the version that matches the NSP RHEL version, if supported
- the version that is less than but closest to the supported NSP RHEL version; in the output example, the version to record is 8.2, as the NSP supports a higher RHEL version that is not listed

5

Download the following files from the NSP downloads page on the Nokia Support portal to an empty local directory on the station:

- NSP_NFM-P_*R_r*_COLLOCATED_OS.qcow2
- each file named NSP_NFM-P_*R_r*_COLLOCATED_STANDALONE.qcow2.part*n*
- QCOW2_Images.cksum

where

n is the partial file ID

R_r is the NFM-P release identifier

6

Open a console window.

7

Navigate to the directory that contains the downloaded files.

8

An NFM-P product image is divided among a set of partial image files that you must concatenate to create one complete image file.

Enter the following to create the complete image file:

```
# cat NSP_NFM-P_R_r_COLLOCATED_STANDALONE.qcow2.part* >NSP_NFM-P_R_r_
COLLOCATED_STANDALONE.qcow2 ↵
```

9

It is strongly recommended that you verify the message digest of each NSP image file or software bundle that you download from the Nokia Support portal. The download page includes checksums for comparison with the output of the RHEL md5sum, sha256sum, or sha512sum command.

To verify a file checksum, perform the following steps.

1. Enter the following:

   ```
   # command file ↵
   ```

   where

   command is md5sum, sha256sum, or sha512sum

   file is the name of the file to check

   A file checksum is displayed.

2. Compare the checksum value and the value in the .cksum file.
3. If the values do not match, the file download has failed. Download a new copy of the file, and then repeat this step.

10

Convert the image files to raw format.

1. Enter the following:

   ```
   # qemu-img convert -f qcow2 NSP_NFM-P_R_r_COLLOCATED_OS.qcow2 -O
   raw -S 0 raw_OS.img ↵
   ```

2. 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

11

Resize the raw software image.

1. Navigate to the directory that contains the raw software image file created in Step 10.
2. Enter the following:

   ```
   # qemu-img resize raw_software.img sizeG ↵
   ```

   where

   raw_software.img is the file to resize

   size is the required size value in the response to your Platform Sizing Request

12

Convert the raw image 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 11

non-sparse_software.img is the name to assign to the non-sparse software image file

13

Enter the following to deploy the VM:

```
# virt-install --connect qemu:///system --ram RAM --vcpus=vCPUs -n instance --os-type=linux --os-variant=variant --disk path=raw_OS.img,device=disk,bus=virtio,format=raw,io=native,cache=directsync --disk path=non-sparse_software.img,device=disk,bus=virtio,format=raw,io=native,cache=directsync --network bridge=bridge_name --import ↵
```

where

bridge_name is the name assigned to the VM network bridge

vCPUs is the required number of vCPU threads in the response to your Platform Sizing Request

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 12

RAM is the required amount of VM RAM in the response to your Platform Sizing Request, in Mbytes; for example, 64 Gbytes is expressed as 65536, which is 64 x 1024 Mbytes

raw_OS.img is the name of the OS image file created in Step 10

variant is the OS version recorded in Step 4; for example, 8.2

14

When the NFM-P VM is instantiated, log in as the root user on the VM; the default password is available from technical support.

15

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.

16

Enter the following:

```
# pvresize /dev/vdb ↵
```

17

Enter the following:

```
# lsblk ↵
```

Basic disk partition information is displayed; the value in the SIZE column is the partition size in Gbytes.

18

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 required partition size in the response to your Platform Sizing Request.

Note: The lvextend command does nothing if a partition size is equal to or greater than the associated value in the response to your Platform Sizing Request. In such a case, the command returns a failure message that you can ignore.

```
# lvextend -L sizeG /dev/vg2/lv_nsp ↵
# lvextend -L sizeG /dev/vg2/lv_nspos ↵
# lvextend -L sizeG /dev/vg2/lv_log ↵
# lvextend -L sizeG /dev/vg2/lv_xmloutput ↵
# lvextend -L sizeG /dev/vg2/lv_db ↵
# lvextend -L sizeG /dev/vg2/lv_archivelog ↵
# lvextend -L sizeG /dev/vg2/lv_dbbackup ↵
```

`# lvextend -L sizeG /dev/vg2/lv_nebackup ↵` (required only if *size* is greater than 1 Gbyte)

```
# lvextend -L sizeG /dev/vg2/lv_var_log ↵
# lvextend -L sizeG /dev/vg2/lv_var_log_audit ↵
# lvextend -L sizeG /dev/vg2/lv_extra ↵
```

where *size* is the required partition size in the response to your Platform Sizing Request, in Gbytes

19

For each partition modified in Step 18, 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_dbbackup ↵
# 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 ↵
```

20

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.

21

Plumb each required network interface with an IPv4 address, network mask, and gateway address. See the OS documentation for configuration information.

22

Enter the following to set the station hostname:

```
# hostnamectl set-hostname hostname
```

where *hostname* is a short hostname or FQDN, depending on your requirement

23

Update the /etc/hosts file to map the station hostname to the IP address of an interface, as described in 13.9 “Using hostnames in the management network” (p. 379).

24

Enter the following to configure and create the main database:

```
# samconfig -m db ↵
```

The following is displayed:

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

25

Verify the database configuration.

1. Enter the following:

```
<db> 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 14.9 “NFM-P samconfig utility” (p. 432) 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>.

26

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.
```

27

When the database creation is complete, enter the following:

```
<db> exit ↵
```

The samconfig utility closes.

28

Enter the following to configure and enable the main server:

```
# samconfig -m main ↵
```

The following is displayed:

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

29

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.

Note: The NFM-P uses the database backup settings to initialize the database during installation only. To change the backup settings after installation, you must use the Database Manager form in the NFM-P client GUI, as described in the *NSP System Administrator Guide*.

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

```
<main configure> back ↵
```

The prompt changes to `<main>`.

30

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

31

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

32

Optionally, for greater system security, you can remove the world permissions from RHEL compiler executable files; see A.1 “Resetting GCC-compiler file permissions” (p. 1093) for information.

33

Enter the following to switch to the nsp user:

```
# su - nsp ↵
```

34

Enter the following:

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

35

Enter the following to start the main server:

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

36

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.
```

37

When the server is fully initialized, close the console window.

End of steps

Standalone NFM-P system installation

14.12 Standalone system installation workflow

14.12.1 Description

The following is the sequence of high-level actions required to install a standalone NFM-P system.

14.12.2 Stages

ℹ **Note:** The link in each stage leads to a section in 14.13 “To install a standalone NFM-P system” (p. 446).

1

Configure firewalls between components, as required; see “Check and configure firewalls” (p. 447).

2

Download the required NFM-P installation files; see “Download installation files” (p. 447).

3

Install the standalone database; see “Install standalone database” (p. 448).

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. 454).

1. Install the main server packages.
2. Create and apply the main server configuration.

5

If required, enable Windows Active Directory for client access; see “Enable Windows Active Directory access” (p. 469).

6

If required, configure ADFS to enable Common Access Card, or CAC, client access; see “Enable CAC access” (p. 471).

7

Start the main server; see “Start standalone main server” (p. 473).

8

Install one or more of the following optional components, as required; see “Install optional components” (p. 475):

- auxiliary server
- auxiliary database

9

Install one or more single-user GUI clients or client delegate servers; see “Install GUI clients” (p. 475).

10

Stop the PKI server; see “Stop PKI server” (p. 475).

11

If any required firewalls between components are disabled, enable the firewalls, as required; see “Configure and enable firewalls” (p. 475).

14.13 To install a standalone NFM-P system

14.13.1 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

14.13.2 Steps

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 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 Planning Guide*, which describes using NFM-P templates for rule creation.

b. Disable each firewall; see the external firewall documentation, or perform 3.19 “To disable the RHEL firewalld service” (p. 91).

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
- nsp-nfmp-nodeexporter-*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:
   - nsp-nfmp-oracle-*R.r.p*-rel.*v*.rpm
   - nsp-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:
    - 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
    - nsp-nfmp-nodeexporter-*R*.*r*.*p*-rel.*v*.rpm

    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 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 ↵
```

ℹ **Note:** A default value is displayed in brackets []. To accept the default, press ↵.

ℹ **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]:
```

10

Enter Yes. The following prompt is displayed:

```
Enter the Oracle dba group name [group]:
```

11

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:
```

12

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/oracle19].

Checking or Creating the Oracle user home directory
/opt/nsp/nfmp/oracle19...

Checking user username...

Adding username...

Changing ownership of the directory /opt/nsp/nfmp/oracle19 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:
```

13

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.

20

Enter the following:

```
# chmod +x * ↵
```

21

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

22

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

23

Enter the following:

```
# samconfig -m db ↵
```

The following is displayed:

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

24

Enter the following:

```
<db> show-detail ↵
```

The database configuration is displayed.

25

To configure one or more parameters, enter the following; otherwise, go to Step 31:

```
<db> configure ↵
```

The prompt changes to `<db configure>`.

26

As required, configure the general parameters in the following table.

ℹ **Note:** The `instance` parameter is configurable only during database creation.

Table 14-4 Standalone database parameters, general

Parameter	Description
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

27

If required, configure one or more `passwords` parameters in the following table, and then enter **`back`** ↵.

ℹ **Note:** After you save the configuration, you cannot use samconfig to change a database password; you must use the method described in the *NSP System Administrator Guide*.

Table 14-5 Standalone database parameters — passwords

Parameter	Description
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

28

To enable IP validation, which restricts the server components that have access to the main database; configure the parameters in the following table, and then enter **`back`** ↵.

ℹ **Note:** For security reasons, it is strongly recommended that you enable IP validation.

ℹ **Note:** When you enable IP validation on an NFM-P system that includes auxiliary servers, NSP Flow Collectors, or NSP analytics servers, you must configure the `remote-servers` parameter; otherwise, the servers cannot reach the database.

Table 14-6 Standalone database parameters — ip-validation

Parameter	Description
main-one	IP address of main server Configuring the parameter enables IP validation. Default: —
remote-servers	Comma-separated list of the IP address of each of the following components that must connect to the database: • auxiliary servers • NSP Flow Collectors • NSP analytics servers Default: —

29

To enable the forwarding of NFM-P system metrics to the NSP; configure the parameters in the following table, and then enter **`back`** ↵.

ℹ **Note:** The parameters are required only for a distributed main database, so are not shown or configurable if the main server and database are collocated.

Table 14-7 Standalone main server parameters — tls

Parameter	Description
keystore-pass	The TLS keystore password Default: available from technical support
pki-server	The PKI server IP address or hostname You must configure the parameter. Default: —
pki-server-port	The TCP port on which the PKI server listens for and services requests Default: 2391

30

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 14.9 “NFM-P samconfig utility” (p. 432) 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>`.

31

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.
```

32

When the database creation is complete, enter the following:

`<db>` **`exit`** ↵

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 the NFM-P database management procedures in the *NSP System Administrator Guide* for more information.

Install standalone main server

34

Log in as the root user on the main server station.

35

Open a console window.

36

Navigate to the NFM-P software directory.

Note: Ensure that the directory contains only the installation files.

37

Enter the following:

```
# chmod +x * ↵
```

38

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

39

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

40

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 an NFM-P main or auxiliary server on the station, change the nsp password.

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.

41

Start the PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 4.10 “To configure and enable a PKI server” (p. 113).

ℹ **Note:** The PKI server is required for internal system configuration purposes.

42

If you are using the manual TLS deployment method, generate and distribute the required TLS files for the system, as described in 4.9 “To generate custom TLS certificate files for the NSP” (p. 108).

43

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

44

Enter the following:

```
<main> configure ↵
```

The prompt changes to `<main configure>`.

45

Enter the following:

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

The main server configuration is displayed.

46

As required, configure the general parameters in the following table.

Table 14-8 Standalone main server parameters, general

Parameter	Description
ip	The main server IP address Default: IP address of primary network interface

Table 14-8 Standalone main server parameters, general (continued)

Parameter	Description
domain	The NFM-P system identifier Default: NFM-P
initial-admin-passwd	The NSP admin user password It is strongly recommended that you change the password from the default; if you choose not to configure the parameter, the default password remains in effect The parameter is configurable only during a main server installation. A password must: • be a minimum of 8 characters • 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 more than three consecutive instances of the same character
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 the *NSP System Administrator Guide*. Default: —
fips	Whether FIPS security is enabled for network management See 13.11 “Enabling FIPS security for NFM-P network management” (p. 384) for information about using FIPS security. Default: false

47

As required, configure the `client` parameters in the following table, and then enter **`back`** ↵.

Table 14-9 Standalone main server parameters — client

Parameter	Description
nat	Whether NAT is used between the main server and the GUI and XML API clients Default: false

Table 14-9 Standalone main server parameters — client (continued)

Parameter	Description
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 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:** The installation location cannot include a space character. **Note:** Before you can install a client delegate server, the main server configuration must include the client delegate server address and file path. Default: —

48

As required, configure the `database` parameters in the following table, and then enter **`back`** ↵.

Note: The NFM-P uses the database backup settings to initialize the database during installation only. To change the backup settings after installation, you must use the Database Manager form in the NFM-P client GUI, as described in the *NSP System Administrator Guide*.

Table 14-10 Standalone main server parameters — database

Parameter	Description
ip	The IP address that the main server must use to reach the database; mandatory Default: —
instance	Database instance name Default: maindb1
user-password	Database user password Default: available from technical support
backup-dest	The backup directory on the main database station 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. Default: /opt/nsp/nfmp/dbbackup
backup-interval	How frequently, in hours, to back up the main database Default: 24
backup-sets	The number of main database backup sets to retain Default: 3

49

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 14-11 Standalone main server parameters — aux

Parameter	Description
stats	If enabled, specifies that one or more auxiliary servers are to be used for statistics collection Default: false
ip-to-auxes	The main server IP address that the auxiliary servers must use to reach the main server Default: —

Table 14-11 Standalone main server parameters — aux (continued)

Parameter	Description
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 Standby auxiliary server IP addresses Default: —

50

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 14-12 Standalone main server parameters — mediation

Parameter	Description
nat	Whether NAT is used between the main server and the managed NEs Default: false
snmp-ipv4	The IPv4 address that the managed NEs must use to reach the main server Default: IPv4 address of primary network interface
snmp-ipv6	The IPv6 address that the managed NEs must use to reach the main server Default: IPv6 address of primary network interface
snmp-port	The TCP port on the main server station that the managed NEs must use to reach the main server Default: 162
traplog-id	The SNMP trap log ID associated with the main server Default: 98

51

Configure the `tls` parameters in the following table, and then enter **`back`** ↵.

Table 14-13 Standalone main server parameters — tls

Parameter	Description
keystore-file	The absolute path of the TLS keystore file To enable automated TLS deployment, enter `no keystore-file`. Default: /opt/nsp/os/tls/nsp.keystore
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: /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	The PKI server IP address or hostname Default: —
pki-server-port	The TCP port on which the PKI server listens for and services requests Default: 2391
regenerate-certs	Whether to regenerate the internal TLS certificates Certificate regeneration is required when the current certificates are about to expire, or a new internal root certificate is available. A new internal root certificate is available when the root certificate is reset, or when the PKI server is run on a station other than the station used for the previous certificate deployment. Default: false
hsts-enabled	Whether HSTS browser security is enabled Default: false

52

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 49. Otherwise, OSS access is restricted to the auxiliary servers, which require the configuration of OSS access parameters during installation.

Table 14-14 Standalone main server parameters — oss

Parameter	Description
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 main server Default: IP address of primary network interface
xml-output	The directory that is to contain the output of XML APIfile export operations Default: /opt/nsp/nfmp/server/xml_output

53

If the NFM-P includes an auxiliary database, configure the `auxdb` parameters in the following table, and then enter **`back`** ↵.

Table 14-15 Standalone main server parameters — auxdb

Parameter	Description
enabled	Whether the auxiliary database is enabled in the main server configuration
secure	Whether TLS is enabled on the auxiliary database If TLS is enabled on the main server, you must set the parameter to true, and enable TLS during the auxiliary database installation. Default: true
ip-list	A list of the auxiliary database station IP addresses that are accessible to the main server, in the following format: **Note:** For a geo-redundant auxiliary database, the order of the IP addresses must be the same on each main server in the geo-redundant system. ***`cluster_1_IP1,cluster_1_IP2,cluster_1_IPn;cluster_2_IP1,cluster_2_IP2,cluster_2_IPn`*** ↵ where *cluster_1_IP1*, *cluster_1_IP2*,*cluster_1_IPn* are the external IP addresses of the auxiliary database stations in one data center *cluster_2_IP1*, *cluster_2_IP2*,*cluster_2_IPn* are the external IP addresses of the stations in the other data center; required only for geo-redundant auxiliary database Default: —
oam-test-results	Whether the auxiliary database is to store OAM test results Default: false

Table 14-15 Standalone main server parameters — auxdb (continued)

Parameter	Description
redundancy-level	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

54

As required, configure the `aa-stats` parameters in the following table, and then enter **`back`** ↵.

Table 14-16 Standalone main server parameters — aa-stats

Parameter	Description
enabled	Whether the NFM-P is to collect AA accounting statistics Default: false
formats	AA accounting statistics file formats; the options are the following: • ipdr—IPDR format • ram—format for NSP Analytics reporting • ipdr,ram—both formats The parameter is configurable when the enabled parameter is set to true. Default: ram
aux-db storage	Whether the NFM-P is to store the statistics in an auxiliary database The parameter is configurable when the enabled parameter is set to true. Default: false

55

Configure the `nspos` parameters in the following table, and then enter **`back`** ↵.

Table 14-17 Standalone main server parameters — nspos

Parameter	Description
ip-list	The NSP cluster IP addresses, separated by a semicolon *`cluster1_address`*;*`cluster2_address`* where *cluster1_address* and *cluster2_address* are the NSP cluster advertised addresses Specify only one IP address for a standalone NSP system. Default: —
address-to-nspos	The main server IP address that is reachable by the nspOS server Default: —
internal-certs	Whether internal certificates are used to secure nspOS communication between components; the parameter is configurable when the **secure** parameter is set to true. The parameter is deprecated, and must be set to the same value as the **secure** parameter. Default: false
secure	Whether communication with the nspOs servers is secured using TLS It is strongly recommended to enable the parameter in an NFM-P-only deployment. Default: false
dc-name	The nspOS DR data center name for aligning NSP components with the local NFM-P main server; must match the dcName value in the NSP configuration file The parameter is required only in a redundant deployment; however, it is recommended that you configure the parameter, regardless of the NFM-P deployment type. Default: —
mtls-kafka-enabled	Specifies whether mTLS is enabled for Kafka communication with the NSP The parameter is displayed only: • if the ip-list parameter is set to a remote address • after the configuration is initially applied in a subsequent step **Note:** The parameter is configurable only if the **secure** and **internal-certs** parameters are set to true. **Note:** The function is supported only in an NSP system that uses separate interfaces for internal and client communication. Default: false

Table 14-17 Standalone main server parameters — nspos (continued)

Parameter	Description
authMode	NSP authentication mode, which is one of the following: • oauth2—OAUTH2 user authentication • cas—CAS user authentication (deprecated) The parameter is configurable only in a shared-mode NSP deployment. The parameter setting must match the authMode setting in the NSP cluster configuration. Default: oauth2

56

Configure the `remote-syslog` parameters in the following table, and then enter **`back`** ↵.

Table 14-18 Standalone main server parameters — remote-syslog

Parameter	Description
enabled	Enable the forwarding of the NFM-P User Activity logs in syslog format to a remote server Default: disabled
syslog-host	Remote syslog server hostname or IP address Default: —
syslog-port	Remote server TCP port Default: —
ca-cert-path	Absolute local path of public CA TLS certificate copied from remote server

57

Configure the `server-logs-to-remote-syslog` parameters in the following table, and then enter **`back`** ↵.

Table 14-19 Standalone main server parameters — server-logs-to-remote-syslog

Parameter	Description
enabled	Enable the forwarding of the NFM-P server logs in syslog format to a remote server Default: disabled
secured	Whether the communication with the remote server is TLS-secured Default: disabled

Table 14-19 Standalone main server parameters — server-logs-to-remote-syslog (continued)

Parameter	Description
syslog-host	Remote syslog server hostname or IP address Default: —
syslog-port	Remote server TCP port Default: —
ca-cert-path	Absolute local path of public CA TLS certificate copied from remote server

58

If the NFM-P deployment includes the 1830 SMS netHSM, configure the `hsm` parameters in the following table; otherwise, go to Step 60.

Table 14-20 Standalone main server parameters — hsm

Parameter	Description
enabled	Whether HSM is enabled Default: false
server-certs	The location of the 1830 SMS netHSM TLS client certificate for NFM-P access Specify a client certificate location in the following format: ***address#file_path*** where *address* is the 1830 SMS netHSM IP address or hostname *file_path* is the absolute path and file name of the certificate file on the 1830 SMS netHSM Default: —
mode	Operation mode; 0 specifies one HSM instance with load balancing disabled, and 2 specifies load balancing among multiple instances Default: 0
client-key	The auto-generated TLS key file that the NFM-P provides to the 1830 SMS netHSM for two-way web-client authentication Default: client.key
client-cert	The auto-generated TLS certificate file that the NFM-P provides to the 1830 SMS netHSM for two-way web-client authentication Default: client.cert

59

By default, the NFM-P generates TLS authentication files for web-client access to the NFM-P HSM server.

If you want to provide your own TLS authentication files, configure the `twoway` HSM parameters in the following table, and then enter **back** ↵.

Table 14-21 Standalone main server parameters — hsm, twoway

Parameter	Description
keystore-file	The absolute path and name of the TLS keystore file for web-client access to the NFM-P HSM server Default: —
keystore-pass	The keystore password Default: —
keystore-alias	The keystore alias Default: NSP
truststore-file	The absolute path and name of the TLS truststore file for web-client access to the NFM-P HSM server Default: —
truststore-pass	The truststore password Default: —
truststore-alias	The truststore alias Default: NSP

60

If the NFM-P is not integrated with an NSP cluster, you must skip this step..

If required, enable the forwarding of the EmsServer.log and server_console.log entries from the main server to NSP OpenSearch.

Enter the following:

```
<main configure> server-logs-to-opensearch enabled ↵
```

The prompt changes to `<main configure server-logs-to-opensearch>`.

61

Enter **back** ↵.

The prompt changes to `<main configure>`.

62

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>`.

63

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

64

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

65

If you want to enable mTLS for internal Kafka authentication using two-way TLS, perform the following steps.

Note: Enabling mTLS for internal Kafka authentication is supported only in an NSP deployment that uses separate interfaces for internal and client communication.

Note: The parameter you must configure is displayed only if the ip-list parameter is set to a remote address.

Note: The parameter is configurable only if the **secure** and **internal-certs** parameters in the **nspos** section are set to true.

1. Enter the following:

   ```
   # samconfig -m main ↵
   ```

   The following is displayed:

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

2. Enter the following:

   ```
   # configure nspos mtls-kafka-enabled back ↵
   ```

3. Enter the following:

   ```
   <main> apply ↵
   ```

   The configuration is applied.

4. Enter the following:

   ```
   <main> exit ↵
   ```

The samconfig utility closes.

Enable Windows Active Directory access

66

If you intend to use Windows Active Directory, or AD, for single-sign-on client access, you must configure LDAP remote authentication for AD; otherwise, go to Step 85.

Open the following file as a reference for use in subsequent steps:

/opt/nsp/os/install/examples/config.yml

ℹ **Note:** Consider the following.

- The NFM-P does not assign a default user group to users of a remote authentication source that you define for Windows AD; the authentication source must provide the user group attributes.
- Windows AD supports the following LDAP server types for remote authentication:

  AD—The user group of an AD user is derived from the group_base_dn attribute in the server configuration; group search filters are not supported.

  AUTHENTICATED—The server configuration must include bind credentials; group search filters are supported. After NFM-P initialization, you add the AD server bind credentials to the NSP password vault using the NSP Session Manager REST API.

67

Locate the section that begins with the following lines:

```
#   ldap:
#     enabled: true
#     servers:
#       - type: AUTHENTICATED/AD/ANONYMOUS
#         url: ldaps://ldap.example.com:636
#         security: SSL/STARTTLS/NONE
```

68

Open the following file using a plain-text editor such as vi:

/opt/nsp/os/install/config.json

69

Locate the section that begins with the following line:

```
"sso": {
```

The section has one subsection for each type of SSO access.

ℹ **Note:** You can enable multiple remote authentication methods such as LDAP and RADIUS in the config.json file, or by using the NFM-P GUI. Using the GUI also allows you to specify the order in which the methods are tried during login attempts; however, no ordering is applied to multiple methods enabled in the config.json file.

70

In the **sso** section, create an **ldap** subsection as shown below using the parameter names from the **ldap** section of config.yml and the required values for your configuration.

The following example shows the LDAP configuration for two AD servers:

```
"ldap": {
"enabled": true,
"servers": [
{
"type": "auth_type",
"url": "ldaps://server1:port",
"server1_parameter_1": "value",
"server1_parameter_2": "value",
.
.
"server1_parameter_n": "value",
},
{
"type": "auth_type",
"url": "ldaps://server2:port",
"server2_parameter_1": "value",
"server2_parameter_2": "value",
.
.
"server2_parameter_n": "value",
},
}]
}
```

where *auth_type* is AD or AUTHENTICATED

71

Save and close the files.

72

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

73

Enter the following:

```
<main> apply ↵
```

The AD LDAP configuration is applied.

74

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Enable CAC access

75

If you do not intend to enable Common Access Card, or CAC, technology for NFM-P client access, go to Step 85.

76

Download the federationmetadata.xml from the following ADFS link:

https://*ADFS_server_name*/FederationMetadata/2007-06/federationmetadata.xml

where *ADFS_server_name* is the ADFS server FQDN

77

Add an ADFS server entry to the /etc/hosts file on the main server.

1. Open the /etc/hosts file using a plain-text editor such as vi.
2. Add the following line below the line that contains the main server IP address:

   ```
   IP_address FQDN
   ```

   where

   IP_address is the IP address of the ADFS server

   FQDN is the FQDN of the ADFS server
3. Save and close the file.

78

In order to enable CAC for client access, you must configure Active Directory Federation Services, or ADFS.

Open the following file using a plain-text editor such as vi:

/opt/nsp/os/install/config.json

79

In the **sso** section, create an **saml2** subsection as shown below using the parameter names from the **saml2** section of config.yml and the required values for your configuration.

The following example shows the ADFS configuration.

Note: You must preserve the lead spacing of each line.

```
  "sso" : {
    "saml2": {
       "enabled": true,
       "service_provider_entity_id": "NFM-P_identifier",
       "service_provider_metadata_filename": "casmetadata.xml",
       "maximum_authentication_lifetime": 3600,
       "accepted_skew": 300,
       "destination_binding": "urn:oasis:names:tc:SAML:2.0:bindings:
HTTP-Redirect",
       "identity_provider_metadata_path": "ADFS_metadata_file",
       "authn_context_class_ref": "urn:oasis:names:tc:SAML:2.0:ac:
classes:TLSClient",
       "authn_context_comparison_type": "minimum",
       "name_id_policy_format": "urn:oasis:names:tc:SAML:1.1:
nameid-format:unspecified",
       "force_auth": true,
       "passive": false,
       "wants_assertions_signed": false,
       "wants_responses_signed": false,
       "all_signature_validation_disabled": false,
       "sign_service_provider_metadata": false,
       "principal_id_attribute": "UPN",
       "use_name_qualifier": false,
       "provider_name": "ADFS_server_URI",
       "requested_attributes": [{
         "name": "http://schemas.xmlsoap.
org/ws/2005/05/identity/claims/emailaddress",
          "friendly_name": "E-Mail Address",
          "name_format": "urn:oasis:names:tc:SAML:2.0:attrname-format:
uri",
          "required": false
      } ],
       "mapped_attributes": [{
           "name": "http://schemas.xmlsoap.org/claims/Group",
           "mapped_to": "authorizationProfile"
      }, {
           "name": "http://schemas.xmlsoap.
org/ws/2005/05/identity/claims/upn",
           "mapped_to": "upn"
      } ]
    },
```

80

Configure the following parameters; leave all other parameters at the default:

- "service_provider_entity_id": "*NFM-P_identifier*"
- "identity_provider_metadata_path": "*ADFS_metadata_file*"
- "provider_name": "*ADFS_server_name*"

NFM-P_identifier is the unique ADFS Relying Trust Party identifier

*ADFS_metadata_fil*e is the absolute path of the ADFS metadata XML file, for example, /opt/federationmetadata.xml

ADFS_server_name is the ADFS server FQDN

81

Save and close the files.

82

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

83

Enter the following:

```
<main> apply ↵
```

The ADFS configuration is applied.

84

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Start standalone main server

85

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 the *NSP 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.

86

If you have enabled CAC for NFM-P client access, download the casmetadata.xml file from the following URL, and then import the file into the ADFS server relying-trust-party:

https://*server*/cas/sp/metadata

where *server* is the main server IP address or hostname

After the download, the casmetadata.xml file is available in the following directory on the main server:

/opt/nsp/os/tomcat/conf/cas/saml

87

If you have enabled Windows Active Directory access using the AUTHENTICATED type of LDAP server, you must add the LDAP server bind credentials to the NSP security configuration.

Use the NSP Session Manager REST API to add the bind credentials; see the Network Developer Portal for information.

88

Specify the memory requirement for GUI clients based on the type of network that the NFM-P is to manage.

1. Enter the following:

```
bash$ ./nmsdeploytool.bash clientmem -option ↵
```

where *option* is one of the following:

- m—medium, for management of limited-scale network
- l—large, for a network of 15 000 or more NEs

2. Record the setting, which is not preserved through an upgrade, for future use.

3. Enter the following to commit the configuration change:

```
bash$ ./nmsdeploytool.bash deploy ↵
```

89

Close the console window.

Install optional components

90

Install and enable one or more auxiliary servers, if required; see “Auxiliary server installation” (p. 544).

91

Install and enable an auxiliary database, if required; see “Auxiliary database installation” (p. 556).

Install GUI clients

92

Install NFM-P single-user GUI clients or client delegate servers, as required; see the following for information:

- “NFM-P single-user GUI client installation” (p. 585)
- “NFM-P client delegate server installation” (p. 591)

See the *NSP NFM-P User Guide* for information about using the NFM-P GUI.

Stop PKI server

93

If no other components are to be deployed, stop the PKI server by entering Ctrl+C in the console window.

Configure and enable firewalls

94

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 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 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

14.14 Redundant system installation workflow

14.14.1 Description

The following is the sequence of high-level actions required to install a redundant NFM-P system.

i **Note:** The link in each stage leads to a section in 14.15 “To install a redundant NFM-P system” (p. 479).

14.14.2 Stages

1

Configure firewalls between components, as required; see “Check and configure firewalls” (p. 479).

2

Download the required NFM-P installation files; see “Download installation files” (p. 480).

3

Install the primary database; see “Install primary database” (p. 480).

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. 488).

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. 494).

1. Install the main server packages.
2. Create and apply the primary main server configuration.

6

If required, enable Windows Active Directory for client access on the primary main server; see “Enable Windows Active Directory access” (p. 511).

7

If required, configure ADFS to enable Common Access Card, or CAC, client access; see "Enable CAC access" (p. 513).

8

Start the primary main server; see "Start primary main server" (p. 516).

9

Install a single-user GUI client or client delegate server; see "Install GUI client" (p. 517).

10

Instantiate the standby database; see "Instantiate standby database" (p. 518).

11

Install the standby main server; see "Install standby main server" (p. 518).

1. Install the main server packages.
2. Create and apply the standby main server configuration.

12

If required, enable Windows Active Directory for client access on the standby main server; see "Enable Windows Active Directory access" (p. 536).

13

If required, configure ADFS to enable Common Access Card, or CAC, client access; see "Enable CAC access" (p. 538).

14

Start the standby main server; see "Start standby main server" (p. 540).

15

Install one or more of the following optional components, as required; see "Install optional components" (p. 542):

- auxiliary server
- auxiliary database

16

Stop the PKI server; see "Stop PKI server" (p. 542).

17

Install additional single-user GUI clients and client delegate servers, as required; see "Install additional GUI clients" (p. 542) .

18

If any required firewalls between components are disabled, enable the firewalls, as required; see “Configure and enable firewalls” (p. 542).

14.15 To install a redundant NFM-P system

14.15.1 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:

- on each main database station—*Oracle management*
- on each 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

14.15.2 Steps

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 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 Planning Guide*, which describes using NFM-P templates for rule creation.

b. Disable each firewall; see the external firewall documentation, or perform 3.19 “To disable the RHEL firewalld service” (p. 91).

Download installation files

2

Download the following installation files to an empty directory on each 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
- nsp-nfmp-nodeexporter-*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

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-*R*.*r*.*p*-rel.*v*.rpm
   - nsp-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 each 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
   - nsp-nfmp-nodeexporter-*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 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.

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]:
```

10

Enter Yes. The following prompt is displayed:

```
Enter the Oracle dba group name [group]:
```

11

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:
```

12

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/oracle19].

Checking or Creating the Oracle user home directory
/opt/nsp/nfmp/oracle19...

Checking user username...

Adding username...

Changing ownership of the directory /opt/nsp/nfmp/oracle19 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:
```

13

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 primary main database station:

```
# 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.

Note: Ensure that the directory contains only the installation files.

20

Enter the following:

```
# chmod +x * ↵
```

21

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

22

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
```

```
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

23

Enter the following:

`#` **`samconfig -m db`** ↵

The following is displayed:

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

24

Enter the following:

`<db>` **`show-detail`** ↵

The primary database configuration is displayed.

25

Enter the following:

`<db>` **`configure`** ↵

The prompt changes to `<db configure>`.

26

As required, configure the general parameters in the following table.

Note: The `instance` parameter is configurable only during database creation.

Table 14-22 Primary database parameters, general

Parameter	Description
ip	Primary database IP address Default: IP address of primary network interface
instance	Primary database instance name, which must: • contain 8 or fewer characters • consist of ASCII characters only • have a letter as the first character Default: maindb1

27

Configure the `redundant` parameters in the following table, and then enter **`back`** ↵.

Note: The `instance` parameter is configurable only during database creation.

Table 14-23 Primary database parameters — redundant

Parameter	Description
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

28

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 System Administrator Guide*.

Table 14-24 Primary database parameters — passwords

Parameter	Description
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

29

To enable IP validation, which restricts the server components that have access to the main database; configure the parameters in the following table, and then enter **`back`** ↵.

Note: For security reasons, it is strongly recommended that you enable IP validation.

Note: When you enable IP validation on an NFM-P system that includes auxiliary servers, NSP Flow Collectors, or NSP analytics servers, you must configure the `remote-servers` parameter; otherwise, the servers cannot reach the database.

Table 14-25 Primary database parameters — ip-validation

Parameter	Description
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: —

30

To enable the forwarding of NFM-P system metrics to the NSP; configure the parameters in the following table, and then enter **`back`** ↵.

Note: The parameters are required only for a distributed main database, so are not shown or configurable if the main server and database are collocated.

Table 14-26 Primary database parameters — tls

Parameter	Description
keystore-pass	The TLS keystore password Default: available from technical support
pki-server	The PKI server IP address or hostname You must configure the parameter. Default: —

Table 14-26 Primary database parameters — tls (continued)

Parameter	Description
pki-server-port	The TCP port on which the PKI server listens for and services requests Default: 2391

31

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 14.9 “NFM-P samconfig utility” (p. 432) 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>`.

32

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.
```

33

When the database creation is complete, enter the following:

`<db>` **`exit`** ↵

The samconfig utility closes.

34

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 the *NSP System Administrator Guide* for information.

Install standby database

35

Log in as the root user on the standby main database station.

36

Open a console window.

37

Navigate to the directory that contains the OracleSw_PreInstall.sh file.

38

Enter the following:

```
# chmod +x OracleSw_PreInstall.sh ↵
```

39

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]:
```

40

Enter Yes. The following prompt is displayed:

```
Enter the Oracle dba group name [group]:
```

41

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:
```

42

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/oracle19].

Checking or Creating the Oracle user home directory
/opt/nsp/nfmp/oracle19...

Checking user username...

Adding username...

Changing ownership of the directory /opt/nsp/nfmp/oracle19 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:
```

43

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:
```

44

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]:
```

45

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
```

46

When the script execution is complete, enter the following to reboot the standby main database station:

```
# systemctl reboot ↵
```

The station reboots.

47

When the reboot is complete, log in as the root user on the standby main database station.

48

Open a console window.

49

Navigate to the NFM-P software directory.

Note: Ensure that the directory contains only the installation files.

50

Enter the following:

```
# chmod +x * ↵
```

51

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf 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
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

53

Enter the following:

```
# samconfig -m db ↵
```

The following is displayed:

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

54

Enter the following:

```
<db> configure type standby ↵
```

The prompt changes to `<db configure>`.

55

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

56

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>`.

57

Enter the following, and then enter **back** ↵:

```
<db configure redundant> instance instance_name ↵
```

where *instance_name* is the primary database instance name

58

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 System Administrator Guide*.

Table 14-27 Standby database parameters — passwords

Parameter	Description
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

59

To enable IP validation, which restricts the server components that have access to the main database; configure the parameters in the following table, and then enter **`back`** ↵.

Note: For security reasons, it is strongly recommended that you enable IP validation.

Note: When you enable IP validation on an NFM-P system that includes auxiliary servers, NSP Flow Collectors, or NSP analytics servers, you must configure the `remote-servers` parameter; otherwise, the servers cannot reach the database.

Table 14-28 Standby database parameters — ip-validation

Parameter	Description
main-one	IP address of primary main server Configuring the parameter enables IP validation. Default: —
main-two	IP address of standby main server Default: —

Table 14-28 Standby database parameters — ip-validation (continued)

Parameter	Description
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: —

60

To enable the forwarding of NFM-P system metrics to the NSP; configure the parameters in the following table, and then enter **`back`** ↵.

Note: The parameters are required only for a distributed main database, so are not shown or configurable if the main server and database are collocated.

Table 14-29 Standby database parameters — tls

Parameter	Description
keystore-pass	The TLS keystore password Default: available from technical support
pki-server	The PKI server IP address or hostname You must configure the parameter. Default: —
pki-server-port	The TCP port on which the PKI server listens for and services requests Default: 2391

61

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 reinstantiated later in the procedure.

2. Review each parameter to ensure that the value is correct.
3. Configure one or more parameters, if required; see 14.9 “NFM-P samconfig utility” (p. 432) 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>`.

62

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.
```

63

When the database creation is complete, enter the following:

```
<db> exit ↵
```

The samconfig utility closes.

Install primary main server

64

Log in as the root user on the primary main server station.

65

Open a console window.

66

Navigate to the NFM-P software directory.

Note: Ensure that the directory contains only the installation files.

67

Enter the following:

```
# chmod +x * ↵
```

68

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

69

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

70

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 an NFM-P main or auxiliary server on the station, change the nsp password.

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.

71

Start the PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 4.10 “To configure and enable a PKI server” (p. 113).

Note: The PKI server is required for internal system configuration purposes.

72

If you are using the manual TLS deployment method, generate and distribute the required TLS files for the system, as described in 4.10 “To configure and enable a PKI server” (p. 113).

73

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

74

Enter the following:

```
<main> configure ↵
```

The prompt changes to `<main configure>`.

75

As required, configure the general parameters in the following table.

Table 14-30 Primary main server parameters, general

Parameter	Description
ip	The primary main server IP address Default: IP address of primary network interface
domain	The NFM-P system identifier Default: NFM-P
initial-admin-passwd	The NSP admin user password It is strongly recommended that you change the password from the default; if you choose not to configure the parameter, the default password remains in effect The parameter is configurable only during a main server installation. **Note:** The NFM-P uses the password configured on the first main server that initializes after the installation. A password must: • be a minimum of 8 characters • 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 more than three consecutive instances of the same character

Table 14-30 Primary main server parameters, general (continued)

Parameter	Description
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 the *NSP System Administrator Guide*. Default: —
fips	Whether FIPS security is enabled for network management See 13.11 "Enabling FIPS security for NFM-P network management" (p. 384) for information about using FIPS security. Default: false

76

As required, configure the `client` parameters in the following table, and then enter **`back`** ↵.

Table 14-31 Primary main server parameters — client

Parameter	Description
nat	Whether NAT is used between the main servers and the GUI and XML API clients Default: false
hostname	The primary 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 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 primary main server The parameter is configurable when the hostname parameter is unconfigured. Default: —

Table 14-31 Primary main server parameters — client (continued)

Parameter	Description
jndi-port	The TCP port on the primary main server station to use for EJB JNDI messaging to GUI clients 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. 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:** The installation location cannot include a space character. **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: —

77

Configure the `database` parameters in the following table, and then enter **`back`** ↵.

Note: The NFM-P uses the database backup settings to initialize the database during installation only. To change the backup settings after installation, you must use the Database Manager form in the NFM-P client GUI, as described in the *NSP System Administrator Guide*.

Table 14-32 Primary main server parameters — database

Parameter	Description
ip	The IP address that the primary main server must use to reach the primary database Default: —
instance	Primary database instance name Default: maindb1
user-password	Primary database user password Default: available from technical support
backup-dest	The backup directory on the primary main database station 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. Default: /opt/nsp/nfmp/dbbackup

Table 14-32 Primary main server parameters — database (continued)

Parameter	Description
backup-interval	How frequently, in hours, to back up the main database Default: 24
backup-sets	The number of main database backup sets to retain Default: 3

78

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 14-33 Primary main server parameters — aux

Parameter	Description
stats	If enabled, specifies that one or more auxiliary servers are to be used for statistics collection Default: false
ip-to-auxes	The primary main server IP address that the auxiliary servers must use to reach the primary 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: —

79

Enter the following:

```
<main> configure redundancy enabled ↵
```

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

80

Configure the general `redundancy` parameters in the following table.

Table 14-34 Primary main server parameters — redundancy

Parameter	Description
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

81

Configure the `database` redundancy parameters in the following table, and then enter **`back`** ↵.

Table 14-35 Primary main server parameters — redundancy, database

Parameter	Description
ip	The IP address that the primary main server must use to reach the standby database Default: —
instance	The standby database instance name Default: —
backup-sync	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 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
alignment	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 *NSP System Administrator Guide*. Default: false

Table 14-35 Primary main server parameters — redundancy, database (continued)

Parameter	Description
preferred-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: —
reinstantiation-delay	The delay, in minutes, between the completion of a database failover and the automatic reinstantiation of the standby database A value of 0 disables automatic database reinstantiation. Default: 60

82

Configure the `peer-server` redundancy parameters in the following table, and then enter **`back`** ↵.

Table 14-36 Primary main server parameters — redundancy, peer-server

Parameter	Description
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 The parameter is configurable and mandatory when the `hostname` parameter in Step 76 is configured. If the TLS certificate contains the FQDN, you must specify the FQDN as the parameter value. 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 14-36 Primary main server parameters — redundancy, peer-server (continued)

Parameter	Description
ip-to-auxes	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: —
snmp-ipv4	The IPv4 address that the managed NEs must use to reach the standby main server
snmp-ipv6	The IPv6 address that the managed NEs must use to reach the standby main server
snmp-port	The TCP port on the standby main server station used for SNMP communication with the managed NEs Default: 162
traplog-id	The SNMP trap log ID associated with the standby main server Default: 98

83

Enter **`back`** ↵.

The prompt changes to `<main configure>`.

84

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 14-37 Primary main server parameters — mediation

Parameter	Description
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 primary main server Default: IPv4 address of primary network interface

Table 14-37 Primary main server parameters — mediation (continued)

Parameter	Description
snmp-ipv6	The IPv6 address that the managed NEs must use to reach the primary main server Default: IPv6 address of primary network interface
snmp-port	The TCP port on the primary main server station that the managed NEs must use to reach the primary main server Default: 162
traplog-id	The SNMP trap log ID associated with the primary main server Default: 98

85

If required, configure the `tls` parameters in the following table, and then enter **`back`** ↵.

Table 14-38 Primary main server parameters — tls

Parameter	Description
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
alias	The alias specified during keystore generation You must configure the parameter. Default: —
pki-server	The PKI server IP address or hostname Default: —
pki-server-port	The TCP port on which the PKI server listens for and services requests Default: 2391

Table 14-38 Primary main server parameters — tls (continued)

Parameter	Description
regenerate-certs	Whether to regenerate the internal TLS certificates Certificate regeneration is required when the current certificates are about to expire, or a new internal root certificate is available. A new internal root certificate is available when the root certificate is reset, or when the PKI server is run on a station other than the station used for the previous certificate deployment. Default: false
hsts-enabled	Whether HSTS browser security is enabled Default: false

86

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 78. Otherwise, OSS access is restricted to the auxiliary servers, which require the configuration of OSS access parameters during installation.

Table 14-39 Primary main server parameters — oss

Parameter	Description
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 primary main server Default: IP address of primary network interface
xml-output	The directory in which to store the output of XML API file export operations Default: /opt/nsp/nfmp/server/xml_output

87

If the NFM-P includes an auxiliary database, configure the `auxdb` parameters in the following table, and then enter **`back`** ↵.

Table 14-40 Primary main server parameters — auxdb

Parameter	Description
enabled	Whether the auxiliary database is enabled in the main server configuration

Table 14-40 Primary main server parameters — auxdb (continued)

Parameter	Description
secure	Whether TLS is enabled on the auxiliary database If TLS is enabled on the main server, you must set the parameter to true, and enable TLS during the auxiliary database installation. Default: true
ip-list	A list of the auxiliary database station IP addresses that are accessible to the main server, in the following format: **Note:** For a geo-redundant auxiliary database, the order of the IP addresses must be the same on each main server in the geo-redundant system. ***cluster_1_IP1,cluster_1_IP2,cluster_1_IPn;cluster_2_IP1,cluster_2_IP2,cluster_2_IPn*** ↵ where *cluster_1_IP1*, *cluster_1_IP2*,*cluster_1_IPn* are the external IP addresses of the auxiliary database stations in one data center *cluster_2_IP1*, *cluster_2_IP2*,*cluster_2_IPn* are the external IP addresses of the stations in the other data center; required only for geo-redundant auxiliary database Default: —
oam-test-results	Whether the auxiliary database is to store OAM test results Default: false
redundancy-level	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

88

As required, configure the `aa-stats` parameters in the following table, and then enter **`back`** ↵.

Table 14-41 Primary main server parameters — aa-stats

Parameter	Description
enabled	Whether the NFM-P is to collect AA accounting statistics Default: false

Table 14-41 Primary main server parameters — aa-stats (continued)

Parameter	Description
formats	AA accounting statistics file formats; the options are the following: • ipdr—IPDR format • ram—format for NSP Analytics reporting • ipdr,ram—both formats The parameter is configurable when the enabled parameter is set to true. Default: ram
aux-db storage	Whether the NFM-P is to store the statistics in an auxiliary database The parameter is configurable when the enabled parameter is set to true. Default: false

89

Configure the `nspos` parameters in the following table, and then enter **`back`** ↵.

Table 14-42 Primary main server parameters — nspos

Parameter	Description
ip-list	The NSP cluster IP addresses, separated by a semicolon *`cluster1_address`*;*`cluster2_address`* where *cluster1_address* and *cluster2_address* are the NSP cluster advertised addresses Specify only one IP address for a standalone NSP system. Default: —
address-to-nspos	The main server IP address that is reachable by the nspOS server Default: —
secure	Whether communication with the nspOs servers is secured using TLS It is strongly recommended to enable the parameter in an NFM-P-only deployment. Default: false
internal-certs	Whether internal certificates are used to secure nspOS communication between components; the parameter is configurable when the **secure** parameter is set to true. The parameter is deprecated, and must be set to the same value as the **secure** parameter. Default: false

Table 14-42 Primary main server parameters — nspos (continued)

Parameter	Description
dc-name	The nspOS DR data center name for aligning NSP components with the local NFM-P main server; must match the dcName value in the NSP configuration file The parameter is required only in a redundant deployment; however, it is recommended that you configure the parameter, regardless of the NFM-P deployment type. Default: —
mtls-kafka-enabled	Specifies whether mTLS is enabled for Kafka communication with the NSP The parameter is displayed only: • if the ip-list parameter is set to a remote address • after the configuration is initially applied in a subsequent step **Note:** The parameter is configurable only if the **secure** and **internal-certs** parameters are set to true. **Note:** The function is supported only in an NSP system that uses separate interfaces for internal and client communication. Default: false
authMode	NSP authentication mode, which is one of the following: • oauth2—OAUTH2 user authentication • cas—CAS user authentication (deprecated) The parameter is configurable only in a shared-mode NSP deployment. The parameter setting must match the authMode setting in the NSP cluster configuration. Default: oauth2

90

Configure the `remote-syslog` parameters in the following table, and then enter **`back`** ↵.

Table 14-43 Primary main server parameters — remote-syslog

Parameter	Description
enabled	Enable the forwarding of the NFM-P User Activity logs in syslog format to a remote server Default: disabled
syslog-host	Remote syslog server hostname or IP address Default: —

Table 14-43 Primary main server parameters — remote-syslog (continued)

Parameter	Description
syslog-port	Remote server TCP port Default: —
ca-cert-path	Absolute local path of public CA TLS certificate copied from remote server

91

Configure the `server-logs-to-remote-syslog` parameters in the following table, and then enter **`back`** ↵.

Table 14-44 Primary main server parameters — server-logs-to-remote-syslog

Parameter	Description
enabled	Enable the forwarding of the NFM-P server logs in syslog format to a remote server Default: disabled
secured	Whether the communication with the remote server is TLS-secured Default: disabled
syslog-host	Remote syslog server hostname or IP address Default: —
syslog-port	Remote server TCP port Default: —
ca-cert-path	Absolute local path of public CA TLS certificate copied from remote server

92

If the NFM-P deployment includes the 1830 SMS netHSM, configure the `hsm` parameters in the following table; otherwise, go to Step 94.

Table 14-45 Primary main server parameters — hsm

Parameter	Description
enabled	Whether HSM is enabled Default: false

Table 14-45 Primary main server parameters — hsm (continued)

Parameter	Description
server-certs	The location of the 1830 SMS netHSM TLS client certificate for NFM-P access Specify a client certificate location in the following format: ***address#file_path*** where *address* is the 1830 SMS netHSM IP address or hostname *file_path* is the absolute path and file name of the certificate file on the 1830 SMS netHSM Default: —
mode	Operation mode; 0 specifies one HSM instance with load balancing disabled, and 2 specifies load balancing among multiple instances Default: 0
client-key	The auto-generated TLS key file that the NFM-P provides to the 1830 SMS netHSM for two-way web-client authentication Default: client.key
client-cert	The auto-generated TLS certificate file that the NFM-P provides to the 1830 SMS netHSM for two-way web-client authentication Default: client.cert

93

By default, the NFM-P generates TLS authentication files for web-client access to the NFM-P HSM server.

If you want to provide your own TLS authentication files, configure the `twoway` HSM parameters in the following table, and then enter **back** ↵.

Table 14-46 Primary main server parameters — hsm, twoway

Parameter	Description
keystore-file	The absolute path and name of the TLS keystore file for web-client access to the NFM-P HSM server Default: —
keystore-pass	The keystore password Default: —
keystore-alias	The keystore alias Default: NSP
truststore-file	The absolute path and name of the TLS truststore file for web-client access to the NFM-P HSM server Default: —

Table 14-46 Primary main server parameters — hsm, twoway (continued)

Parameter	Description
truststore-pass	The truststore password Default: —
truststore-alias	The truststore alias Default: NSP

94

If the NFM-P is not integrated with an NSP cluster, you must skip this step..

If required, enable the forwarding of the EmsServer.log and server_console.log entries from the main server to NSP OpenSearch.

Enter the following:

```
<main configure> server-logs-to-opensearch enabled ↵
```

The prompt changes to `<main configure server-logs-to-opensearch>`.

95

Enter **back** ↵.

The prompt changes to `<main configure>`.

96

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>`.

97

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

98

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

99

If you want to enable mTLS for internal Kafka authentication using two-way TLS, perform the following steps.

Note: Enabling mTLS for internal Kafka authentication is supported only in an NSP deployment that uses separate interfaces for internal and client communication.

Note: The parameter you must configure is displayed only if the ip-list parameter is set to a remote address.

Note: The parameter is configurable only if the **secure** and **internal-certs** parameters in the **nspos** section are set to true.

1. Enter the following:

   ```
   # samconfig -m main ↵
   ```

   The following is displayed:

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

2. Enter the following:

   ```
   # configure nspos mtls-kafka-enabled back ↵
   ```

3. Enter the following:

   ```
   <main> apply ↵
   ```

   The configuration is applied.

4. Enter the following:

   ```
   <main> exit ↵
   ```

   The samconfig utility closes.

Enable Windows Active Directory access

100

If you intend to use Windows Active Directory, or AD, for single-sign-on client access, you must configure LDAP remote authentication for AD; otherwise, go to Step 119.

Open the following file as a reference for use in subsequent steps:

/opt/nsp/os/install/examples/config.yml

Note: Consider the following.

- The NFM-P does not assign a default user group to users of a remote authentication source that you define for Windows AD; the authentication source must provide the user group attributes.
- Windows AD supports the following LDAP server types for remote authentication:

AD—The user group of an AD user is derived from the group_base_dn attribute in the server configuration; group search filters are not supported.

AUTHENTICATED—The server configuration must include bind credentials; group search filters are supported. After NFM-P initialization, you add the AD server bind credentials to the NSP password vault using the NSP Session Manager REST API.

101

Locate the section that begins with the following lines:

```
#   ldap:
#     enabled: true
#     servers:
#       - type: AUTHENTICATED/AD/ANONYMOUS
#         url: ldaps://ldap.example.com:636
#         security: SSL/STARTTLS/NONE
```

102

Open the following file using a plain-text editor such as vi:

/opt/nsp/os/install/config.json

103

Locate the section that begins with the following line:

```
"sso": {
```

The section has one subsection for each type of SSO access.

Note: You can enable multiple remote authentication methods such as LDAP and RADIUS in the config.json file, or by using the NFM-P GUI. Using the GUI also allows you to specify the order in which the methods are tried during login attempts; however, no ordering is applied to multiple methods enabled in the config.json file.

104

In the **sso** section, create an **ldap** subsection as shown below using the parameter names from the **ldap** section of config.yml and the required values for your configuration.

The following example shows the LDAP configuration for two AD servers:

```
"ldap": {
"enabled": true,
"servers": [
{
"type": "auth_type",
"url": "ldaps://server1:port",
"server1_parameter_1": "value",
"server1_parameter_2": "value",
.
.
"server1_parameter_n": "value",
},
{
"type": "auth_type",
"url": "ldaps://server2:port",
"server2_parameter_1": "value",
"server2_parameter_2": "value",
.
.
"server2_parameter_n": "value",
},
}]
}
```

where *auth_type* is AD or AUTHENTICATED

105

Save and close the files.

106

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

107

Enter the following:

```
<main> apply ↵
```

The AD LDAP configuration is applied.

108

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Enable CAC access

109

If you do not intend to enable Common Access Card, or CAC, technology for NFM-P client access, go to Step 119.

110

Download the federationmetadata.xml from the following ADFS link:

https://*ADFS_server_name*/FederationMetadata/2007-06/federationmetadata.xml

where *ADFS_server_name* is the ADFS server FQDN

111

Add an ADFS server entry to the /etc/hosts file on the main server.

1. Open the /etc/hosts file using a plain-text editor such as vi.
2. Add the following line below the line that contains the main server IP address:

   ```
   IP_address FQDN
   ```

   where

   IP_address is the IP address of the ADFS server

   FQDN is the FQDN of the ADFS server
3. Save and close the file.

112

In order to enable CAC for client access, you must configure Active Directory Federation Services, or ADFS.

Open the following file using a plain-text editor such as vi:

/opt/nsp/os/install/config.json

113

In the **sso** section, create an **saml2** subsection as shown below using the parameter names from the **saml2** section of config.yml and the required values for your configuration.

The following example shows the ADFS configuration.

Note: You must preserve the lead spacing of each line.

```
  "sso" : {
    "saml2": {
       "enabled": true,
       "service_provider_entity_id": "NFM-P_identifier",
       "service_provider_metadata_filename": "casmetadata.xml",
       "maximum_authentication_lifetime": 3600,
       "accepted_skew": 300,
       "destination_binding": "urn:oasis:names:tc:SAML:2.0:bindings:
HTTP-Redirect",
       "identity_provider_metadata_path": "ADFS_metadata_file",
       "authn_context_class_ref": "urn:oasis:names:tc:SAML:2.0:ac:
classes:TLSClient",
       "authn_context_comparison_type": "minimum",
```

```
       "name_id_policy_format": "urn:oasis:names:tc:SAML:1.1:
nameid-format:unspecified",
       "force_auth": true,
       "passive": false,
       "wants_assertions_signed": false,
       "wants_responses_signed": false,
       "all_signature_validation_disabled": false,
       "sign_service_provider_metadata": false,
       "principal_id_attribute": "UPN",
       "use_name_qualifier": false,
       "provider_name": "ADFS_server_URI",
       "requested_attributes": [{
         "name": "http://schemas.xmlsoap.
org/ws/2005/05/identity/claims/emailaddress",
          "friendly_name": "E-Mail Address",
          "name_format": "urn:oasis:names:tc:SAML:2.0:attrname-format:
uri",
          "required": false
      } ],
       "mapped_attributes": [{
           "name": "http://schemas.xmlsoap.org/claims/Group",
           "mapped_to": "authorizationProfile"
      }, {
           "name": "http://schemas.xmlsoap.
org/ws/2005/05/identity/claims/upn",
           "mapped_to": "upn"
      } ]
    },
```

114

Configure the following parameters; leave all other parameters at the default:

- "service_provider_entity_id": "*NFM-P_identifier*"
- "identity_provider_metadata_path": "*ADFS_metadata_file*"
- "provider_name": "*ADFS_server_name*"

NFM-P_identifier is the unique ADFS Relying Trust Party identifier

*ADFS_metadata_fil*e is the absolute path of the ADFS metadata XML file, for example, /opt/federationmetadata.xml

ADFS_server_name is the ADFS server FQDN

115

Save and close the files.

116

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

117

Enter the following:

```
<main> apply ↵
```

The ADFS configuration is applied.

118

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Start primary main server

119

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 the *NSP 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.

120

If you have enabled CAC for NFM-P client access, download the casmetadata.xml file from the following URL, and then import the file into the ADFS server relying-trust-party:

https://*server*/cas/sp/metadata

where *server* is the main server IP address or hostname

After the download, the casmetadata.xml file is available in the following directory on the main server:

/opt/nsp/os/tomcat/conf/cas/saml

121

If you have enabled Windows Active Directory access using the AUTHENTICATED type of LDAP server, you must add the LDAP server bind credentials to the NSP security configuration.

Use the NSP Session Manager REST API to add the bind credentials; see the Network Developer Portal for information.

122

Specify the memory requirement for GUI clients based on the type of network that the NFM-P is to manage.

1. Enter the following:

   ```
   bash$ ./nmsdeploytool.bash clientmem -option ↵
   ```

   where *option* is one of the following:
   - m—medium, for management of limited-scale network
   - l—large, for a network of 15 000 or more NEs
2. Record the setting, which is not preserved through an upgrade, for future use.
3. Enter the following to commit the configuration change:

   ```
   bash$ ./nmsdeploytool.bash deploy ↵
   ```

123

Close the console window.

Install GUI client

124

You require an NFM-P GUI client to complete the procedure; see the following for information:

Note: Single-user GUI client installation takes less time, so may be the preferred option if your maintenance period is limited; you can uninstall an unused single-user client after you complete the procedure.

- “NFM-P single-user GUI client installation” (p. 585)

- “NFM-P client delegate server installation” (p. 591)

See the *NSP NFM-P User Guide* for information about using the NFM-P GUI to view and manage objects.

Instantiate standby database

125

Open an NFM-P GUI client as the admin user.

126

Choose Administration→System Information from the main menu. The System Information form opens.

127

Click Re-Instantiate Standby.

128

Click Yes to confirm the action. The instantiation begins, and the GUI status bar displays the current phase of the operation.

i **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.

129

When the instantiation is complete, close the System Information form.

Install standby main server

130

Log in as the root user on the standby main server station.

131

Open a console window.

132

Navigate to the NFM-P software directory.

i **Note:** Ensure that the directory contains only the installation files.

133

Enter the following:

```
# chmod +x * ↵
```

134

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

135

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

136

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 an NFM-P main or auxiliary server on the station, change the nsp password.

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.

137

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

138

Enter the following:

```
<main> configure ↵
```

The prompt changes to `<main configure>`.

139

As required, configure the general parameters in the following table.

Table 14-47 Standby main server parameters, general

Parameter	Description
ip	The standby main server IP address Default: IP address of primary network interface
domain	The NFM-P system identifier Default: NFM-P
initial-admin-passwd	The NSP admin user password; which must match the password specified in the primary main server configuration It is strongly recommended that you change the password from the default; if you choose not to configure the parameter, the default password remains in effect The parameter is configurable only during a main server installation. **Note:** The NFM-P uses the password configured on the first main server that initializes after the installation. A password must: • be a minimum of 8 characters • 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 more than three consecutive instances of the same character

Table 14-47 Standby main server parameters, general (continued)

Parameter	Description
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 the *NSP System Administrator Guide*. Default: —
fips	Whether FIPS security is enabled for network management See 13.11 “Enabling FIPS security for NFM-P network management” (p. 384) for information about using FIPS security. Default: false

140

As required, configure the `client` parameters in the following table, and then enter **`back`** ↵.

Table 14-48 Standby main server parameters — client

Parameter	Description
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 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: —

Table 14-48 Standby main server parameters — client (continued)

Parameter	Description
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: —

141

Configure the `database` parameters in the following table, and then enter **`back`** ↵.

Note: The NFM-P uses the database backup settings to initialize the database during installation only. To change the backup settings after installation, you must use the Database Manager form in the NFM-P client GUI, as described in the *NSP System Administrator Guide*.

Table 14-49 Standby main server parameters — database

Parameter	Description
ip	The IP address that the standby main server must use to reach the standby database Default: —
instance	Standby database instance name You must set this parameter to the same value as the instance parameter in step Step 81. Default: maindb1
user-password	Standby database user password Default: available from technical support

Table 14-49 Standby main server parameters — database (continued)

Parameter	Description
backup-dest	The backup directory on the primary main database station 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. Default: /opt/nsp/nfmp/dbbackup
backup-interval	How frequently, in hours, to back up the main database Default: 24
backup-sets	The number of main database backup sets to retain Default: 3

142

If the NFM-P system is to include auxiliary servers, configure the `aux` parameters in the following table, and then enter **`back`** ↵.

ℹ **Note:** At least one auxiliary server that you specify must be a Preferred auxiliary server.

Table 14-50 Standby main server parameters — aux

Parameter	Description
stats	If enabled, specifies that one or more auxiliary servers are to be used for statistics collection Default: false
ip-to-auxes	The standby main server IP address that the auxiliary servers must use to reach the standby 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: —

143

Enter the following:

```
<main> configure redundancy enabled ↵
```

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

144

Configure the general `redundancy` parameters in the following table.

Table 14-51 Standby main server parameters — redundancy

Parameter	Description
ip-to-peer	The standby main server IP address that the primary main server must use for general communication Default: IP address of primary network interface
rsync-ip	The standby main server IP address that the primary main server must use for data synchronization Default: IP address of primary network interface

145

Configure the `database` redundancy parameters in the following table, and then enter **`back`** ↵.

Table 14-52 Standby main server parameters — redundancy, database

Parameter	Description
ip	The IP address that the standby main server must use to reach the primary database Default: —
instance	Primary database instance name Default: —
backup-sync	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 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

Table 14-52 Standby main server parameters — redundancy, database (continued)

Parameter	Description
alignment	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 *NSP System Administrator Guide* Default: false
preferred-instance	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: —
reinstantiation-delay	The delay, in minutes, between the completion of a database failover and the automatic reinstantiation of the standby database A value of 0 disables automatic database reinstantiation. Default: 60

146

Configure the `peer-server` redundancy parameters in the following table, and then enter **`back`** ↵.

Table 14-53 Standby main server parameters — redundancy, peer-server

Parameter	Description
ip	The primary main server IP address that the standby main server must use for general communication Default: —
hostname	The primary main server hostname that the standby main server must use for general communication The parameter is configurable and mandatory when the `hostname` parameter in Step 140 is configured. If the TLS certificate contains the FQDN, you must specify the FQDN as the parameter value. Default: —

Table 14-53 Standby main server parameters — redundancy, peer-server (continued)

Parameter	Description
rsync-ip	The primary main server IP address that the standby main server must use for data synchronization Default: —
public-ip	The IP address that the GUI clients, XML API clients, and auxiliary servers must use to reach the primary 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

147

Enter **`back`** ↵.

The prompt changes to `<main configure>`.

148

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 14-54 Standby main server parameters — mediation

Parameter	Description
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

149

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.

150

If required, configure the `tls` parameters in the following table, and then enter **`back`** ↲.

Table 14-55 Standby main server parameters — tls

Parameter	Description
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 14-55 Standby main server parameters — tls (continued)

Parameter	Description
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	The PKI server IP address or hostname Default: —
pki-server-port	The TCP port on which the PKI server listens for and services requests Default: 2391
regenerate-certs	Whether to regenerate the internal TLS certificates Certificate regeneration is required when the current certificates are about to expire, or a new internal root certificate is available. A new internal root certificate is available when the root certificate is reset, or when the PKI server is run on a station other than the station used for the previous certificate deployment. Default: false
hsts-enabled	Whether HSTS browser security is enabled Default: false

151

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 142. Otherwise, OSS access is restricted to the auxiliary servers, which require the configuration of OSS access parameters during installation.

Table 14-56 Standby main server parameters — oss

Parameter	Description
secure	Whether communication between the main servers and the XML API clients is secured using TLS Default: secure

Table 14-56 Standby main server parameters — oss (continued)

Parameter	Description
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
xml-output	The directory in which to store the output of XML API file export operations Default: /opt/nsp/nfmp/server/xml_output

152

If the NFM-P includes an auxiliary database, configure the `auxdb` parameters in the following table, and then enter **`back`** ↵.

Table 14-57 Standby main server parameters — auxdb

Parameter	Description
enabled	Whether the auxiliary database is enabled in the main server configuration
secure	Whether TLS is enabled on the auxiliary database If TLS is enabled on the main server, you must set the parameter to true, and enable TLS during the auxiliary database installation. Default: true
ip-list	A list of the auxiliary database station IP addresses that are accessible to the main server, in the following format: **Note:** For a geo-redundant auxiliary database, the order of the IP addresses must be the same on each main server in the geo-redundant system. ***`cluster_1_IP1,cluster_1_IP2,cluster_1_IPn;cluster_2_IP1,cluster_2_IP2,cluster_2_IPn`*** ↵ where *cluster_1_IP1*, *cluster_1_IP2*,*cluster_1_IPn* are the external IP addresses of the auxiliary database stations in one data center *cluster_2_IP1*, *cluster_2_IP2*,*cluster_2_IPn* are the external IP addresses of the stations in the other data center; required only for geo-redundant auxiliary database Default: —
oam-test-results	Whether the auxiliary database is to store OAM test results Default: false

Table 14-57 Standby main server parameters — auxdb (continued)

Parameter	Description
redundancy-level	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

153

As required, configure the `aa-stats` parameters in the following table, and then enter **`back`** ↵.

Table 14-58 Standby main server parameters — aa-stats

Parameter	Description
enabled	Whether the NFM-P is to collect AA accounting statistics Default: false
formats	AA accounting statistics file formats; the options are the following: • ipdr—IPDR format • ram—format for NSP Analytics reporting • ipdr,ram—both formats The parameter is configurable when the enabled parameter is set to true. Default: ram
aux-db storage	Whether the NFM-P is to store the statistics in an auxiliary database The parameter is configurable when the enabled parameter is set to true. Default: false

154

Configure the `nspos` parameters in the following table, and then enter **`back`** ↵.

Table 14-59 Standby main server parameters — nspos

Parameter	Description
ip-list	The NSP cluster IP addresses, separated by a semicolon `cluster1_address;cluster2_address` where *cluster1_address* and *cluster2_address* are the NSP cluster advertised addresses Specify only one IP address for a standalone NSP system. Default: —
address-to-nspos	The main server IP address that is reachable by the nspOS server Default: —
secure	Whether communication with the nspOs servers is secured using TLS It is strongly recommended to enable the parameter in an NFM-P-only deployment. Default: false
internal-certs	Whether internal certificates are used to secure nspOS communication between components; the parameter is configurable when the **secure** parameter is set to true. The parameter is deprecated, and must be set to the same value as the **secure** parameter. Default: false
dc-name	The nspOS DR data center name for aligning NSP components with the local NFM-P main server; must match the dcName value in the NSP configuration file The parameter is required only in a redundant deployment; however, it is recommended that you configure the parameter, regardless of the NFM-P deployment type. Default: —
mtls-kafka-enabled	Specifies whether mTLS is enabled for Kafka communication with the NSP The parameter is displayed only: • if the ip-list parameter is set to a remote address • after the configuration is initially applied in a subsequent step **Note:** The parameter is configurable only if the **secure** and **internal-certs** parameters are set to true. **Note:** The function is supported only in an NSP system that uses separate interfaces for internal and client communication. Default: false

Table 14-59 Standby main server parameters — nspos (continued)

Parameter	Description
authMode	NSP authentication mode, which is one of the following: • oauth2—OAUTH2 user authentication • cas—CAS user authentication (deprecated) The parameter is configurable only in a shared-mode NSP deployment. The parameter setting must match the authMode setting in the NSP cluster configuration. Default: oauth2

155

Configure the `remote-syslog` parameters in the following table, and then enter **`back`** ↵.

Table 14-60 Standby main server parameters — remote-syslog

Parameter	Description
enabled	Enable the forwarding of the NFM-P User Activity logs in syslog format to a remote server Default: disabled
syslog-host	Remote syslog server hostname or IP address Default: —
syslog-port	Remote server TCP port Default: —
ca-cert-path	Absolute local path of public CA TLS certificate copied from remote server

156

Configure the `server-logs-to-remote-syslog` parameters in the following table, and then enter **`back`** ↵.

Table 14-61 Standby main server parameters — server-logs-to-remote-syslog

Parameter	Description
enabled	Enable the forwarding of the NFM-P server logs in syslog format to a remote server Default: disabled
secured	Whether the communication with the remote server is TLS-secured Default: disabled

Table 14-61 Standby main server parameters — server-logs-to-remote-syslog (continued)

Parameter	Description
syslog-host	Remote syslog server hostname or IP address Default: —
syslog-port	Remote server TCP port Default: —
ca-cert-path	Absolute local path of public CA TLS certificate copied from remote server

157

If the NFM-P deployment includes the 1830 SMS netHSM, configure the `hsm` parameters in the following table; otherwise, go to Step 159.

Table 14-62 Standby main server parameters — hsm

Parameter	Description
enabled	Whether HSM is enabled Default: false
server-certs	The location of the 1830 SMS netHSM TLS client certificate for NFM-P access Specify a client certificate location in the following format: ***address#file_path*** where *address* is the 1830 SMS netHSM IP address or hostname *file_path* is the absolute path and file name of the certificate file on the 1830 SMS netHSM Default: —
mode	Operation mode; 0 specifies one HSM instance with load balancing disabled, and 2 specifies load balancing among multiple instances Default: 0
client-key	The auto-generated TLS key file that the NFM-P provides to the 1830 SMS netHSM for two-way web-client authentication Default: client.key
client-cert	The auto-generated TLS certificate file that the NFM-P provides to the 1830 SMS netHSM for two-way web-client authentication Default: client.cert

158

By default, the NFM-P generates TLS authentication files for web-client access to the NFM-P HSM server.

If you want to provide your own TLS authentication files, configure the `twoway` HSM parameters in the following table, and then enter **`back`** ↵.

Table 14-63 Standby main server parameters — hsm, twoway

Parameter	Description
keystore-file	The absolute path and name of the TLS keystore file for web-client access to the NFM-P HSM server Default: —
keystore-pass	The keystore password Default: —
keystore-alias	The keystore alias Default: NSP
truststore-file	The absolute path and name of the TLS truststore file for web-client access to the NFM-P HSM server Default: —
truststore-pass	The truststore password Default: —
truststore-alias	The truststore alias Default: NSP

159

If the NFM-P is not integrated with an NSP cluster, you must skip this step..

If required, enable the forwarding of the EmsServer.log and server_console.log entries from the main server to NSP OpenSearch.

Enter the following:

```
<main configure> server-logs-to-opensearch enabled ↵
```

The prompt changes to `<main configure server-logs-to-opensearch>`.

160

Enter **`back`** ↵.

The prompt changes to `<main configure>`.

161

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>`.

162

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

163

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

164

If you want to enable mTLS for internal Kafka authentication using two-way TLS, perform the following steps.

Note: Enabling mTLS for internal Kafka authentication is supported only in an NSP deployment that uses separate interfaces for internal and client communication.

Note: The parameter you must configure is displayed only if the ip-list parameter is set to a remote address.

Note: The parameter is configurable only if the **secure** and **internal-certs** parameters in the **nspos** section are set to true.

1. Enter the following:

   ```
   # samconfig -m main ↵
   ```

   The following is displayed:

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

2. Enter the following:

   ```
   # configure nspos mtls-kafka-enabled back ↵
   ```

3. Enter the following:

   ```
   <main> apply ↵
   ```

   The configuration is applied.

4. Enter the following:

   ```
   <main> exit ↵
   ```

   The samconfig utility closes.

Enable Windows Active Directory access

165

If you intend to use Windows Active Directory, or AD, for single-sign-on client access, you must configure LDAP remote authentication for AD; otherwise, go to Step 184.

Open the following file as a reference for use in subsequent steps:

/opt/nsp/os/install/examples/config.yml

Note: Consider the following.

- The NFM-P does not assign a default user group to users of a remote authentication source that you define for Windows AD; the authentication source must provide the user group attributes.
- Windows AD supports the following LDAP server types for remote authentication:

  AD—The user group of an AD user is derived from the group_base_dn attribute in the server configuration; group search filters are not supported.

  AUTHENTICATED—The server configuration must include bind credentials; group search filters are supported. After NFM-P initialization, you add the AD server bind credentials to the NSP password vault using the NSP Session Manager REST API.

166

Locate the section that begins with the following lines:

```
#   ldap:
#     enabled: true
#     servers:
#       - type: AUTHENTICATED/AD/ANONYMOUS
#         url: ldaps://ldap.example.com:636
#         security: SSL/STARTTLS/NONE
```

167

Open the following file using a plain-text editor such as vi:

/opt/nsp/os/install/config.json

168

Locate the section that begins with the following line:

```
"sso": {
```

The section has one subsection for each type of SSO access.

Note: You can enable multiple remote authentication methods such as LDAP and RADIUS in the config.json file, or by using the NFM-P GUI. Using the GUI also allows you to specify the order in which the methods are tried during login attempts; however, no ordering is applied to multiple methods enabled in the config.json file.

169

In the **sso** section, create an **ldap** subsection as shown below using the parameter names from the **ldap** section of config.yml and the required values for your configuration.

The following example shows the LDAP configuration for two AD servers:

```
"ldap": {
"enabled": true,
"servers": [
{
"type": "auth_type",
"url": "ldaps://server1:port",
"server1_parameter_1": "value",
"server1_parameter_2": "value",
.
.
"server1_parameter_n": "value",
},
{
"type": "auth_type",
"url": "ldaps://server2:port",
"server2_parameter_1": "value",
"server2_parameter_2": "value",
.
.
"server2_parameter_n": "value",
},
}]
}
```

where *auth_type* is AD or AUTHENTICATED

170

Save and close the files.

171

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

172

Enter the following:

```
<main> apply ↵
```

The AD LDAP configuration is applied.

173

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Enable CAC access

174

If you do not intend to enable Common Access Card, or CAC, technology for NFM-P client access, go to Step 184.

175

Download the federationmetadata.xml from the following ADFS link:

https://*ADFS_server_name*/FederationMetadata/2007-06/federationmetadata.xml

where *ADFS_server_name* is the ADFS server FQDN

176

Add an ADFS server entry to the /etc/hosts file on the main server.

1. Open the /etc/hosts file using a plain-text editor such as vi.
2. Add the following line below the line that contains the main server IP address:

   ```
   IP_address FQDN
   ```

   where

   IP_address is the IP address of the ADFS server

   FQDN is the FQDN of the ADFS server
3. Save and close the file.

177

In order to enable CAC for client access, you must configure Active Directory Federation Services, or ADFS.

Open the following file using a plain-text editor such as vi:

/opt/nsp/os/install/config.json

178

In the **sso** section, create an **saml2** subsection as shown below using the parameter names from the **saml2** section of config.yml and the required values for your configuration.

The following example shows the ADFS configuration.

Note: You must preserve the lead spacing of each line.

```
"sso" : {
  "saml2": {
```

```
       "enabled": true,
       "service_provider_entity_id": "NFM-P_identifier",
       "service_provider_metadata_filename": "casmetadata.xml",
       "maximum_authentication_lifetime": 3600,
       "accepted_skew": 300,
       "destination_binding": "urn:oasis:names:tc:SAML:2.0:bindings:
HTTP-Redirect",
       "identity_provider_metadata_path": "ADFS_metadata_file",
       "authn_context_class_ref": "urn:oasis:names:tc:SAML:2.0:ac:
classes:TLSClient",
       "authn_context_comparison_type": "minimum",
       "name_id_policy_format": "urn:oasis:names:tc:SAML:1.1:
nameid-format:unspecified",
       "force_auth": true,
       "passive": false,
       "wants_assertions_signed": false,
       "wants_responses_signed": false,
       "all_signature_validation_disabled": false,
       "sign_service_provider_metadata": false,
       "principal_id_attribute": "UPN",
       "use_name_qualifier": false,
       "provider_name": "ADFS_server_URI",
       "requested_attributes": [{
         "name": "http://schemas.xmlsoap.
org/ws/2005/05/identity/claims/emailaddress",
          "friendly_name": "E-Mail Address",
          "name_format": "urn:oasis:names:tc:SAML:2.0:attrname-format:
uri",
          "required": false
      } ],
       "mapped_attributes": [{
           "name": "http://schemas.xmlsoap.org/claims/Group",
           "mapped_to": "authorizationProfile"
      }, {
           "name": "http://schemas.xmlsoap.
org/ws/2005/05/identity/claims/upn",
           "mapped_to": "upn"
      } ]
```

```
    },
```

179

Configure the following parameters; leave all other parameters at the default:

- "service_provider_entity_id": "*NFM-P_identifier*"
- "identity_provider_metadata_path": "*ADFS_metadata_file*"
- "provider_name": "*ADFS_server_name*"

NFM-P_identifier is the unique ADFS Relying Trust Party identifier

*ADFS_metadata_fil*e is the absolute path of the ADFS metadata XML file, for example, /opt/federationmetadata.xml

ADFS_server_name is the ADFS server FQDN

180

Save and close the files.

181

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

182

Enter the following:

```
<main> apply ↵
```

The ADFS configuration is applied.

183

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Start standby main server

184

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 the *NSP 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.

185

If you have enabled CAC for NFM-P client access, download the casmetadata.xml file from the following URL, and then import the file into the ADFS server relying-trust-party:

https://*server*/cas/sp/metadata

where *server* is the main server IP address or hostname

After the download, the casmetadata.xml file is available in the following directory on the main server:

/opt/nsp/os/tomcat/conf/cas/saml

186

If you have enabled Windows Active Directory access using the AUTHENTICATED type of LDAP server, you must add the LDAP server bind credentials to the NSP security configuration.

Use the NSP Session Manager REST API to add the bind credentials; see the Network Developer Portal for information.

187

Specify the memory requirement for GUI clients based on the type of network that the NFM-P is to manage.

1. Enter the following:

   ```
   bash$ ./nmsdeploytool.bash clientmem -option ↵
   ```

   where *option* is one of the following:
   - m—medium, for management of limited-scale network
   - l—large, for a network of 15 000 or more NEs
2. Record the setting, which is not preserved through an upgrade, for future use.
3. Enter the following to commit the configuration change:

   ```
   bash$ ./nmsdeploytool.bash deploy ↵
   ```

188

Close the console window.

Install optional components

189

Install and enable one or more auxiliary servers, if required; see "Auxiliary server installation" (p. 544).

190

Install and enable an auxiliary database, if required; see "Auxiliary database installation" (p. 556).

191

Install and enable one or more NSP analytics servers, if required; see "NSP analytics server installation" (p. 414) for information.

Stop PKI server

192

If no other components are to be deployed, stop the PKI server by entering Ctrl+C in the console window.

Install additional GUI clients

193

Install additional NFM-P GUI clients or client delegate servers, as required; see the following for information:

- "NFM-P single-user GUI client installation" (p. 585)
- "NFM-P client delegate server installation" (p. 591)

Configure and enable firewalls

194

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 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 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 installation

14.16 Auxiliary server installation workflow

14.16.1 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 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.

14.16.2 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 14.17 “To install an NFM-P auxiliary server” (p. 545) on the auxiliary server station.

2

Perform 14.18 “To add auxiliary servers to an NFM-P system” (p. 550) 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 the *NSP NFM-P User Guide* for information about configuring an additional management interface on an auxiliary server.

14.17 To install an NFM-P auxiliary server

14.17.1 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 SNMP statistics 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

14.17.2 Steps

1

Start the PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 4.10 “To configure and enable a PKI server” (p. 113).

Note: The PKI server is required for internal system configuration purposes.

2

Log in as the root user on the auxiliary server station.

3

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
- nsp-nfmp-nodeexporter-*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.

4

Navigate to the NFM-P software directory.

Note: Ensure that the directory contains only the installation files.

5

Enter the following:

```
# chmod +x * ↵
```

6

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf 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
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

8

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 an NFM-P main or auxiliary server on the station, change the nsp password.

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.

9

Enter the following:

```
# samconfig -m aux ↵
```

The following is displayed:

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

10

Enter the following:

```
<aux> configure ↵
```

The prompt changes to `<aux configure>`.

11

Enter the following:

```
<aux configure> show-detail ↵
```

The auxiliary server configuration is displayed.

12

If the default `ip` value is not the correct IP address of the auxiliary server, configure the `ip` parameter.

13

Configure the `fips` parameter to specify whether FIPS security is enabled for network management.

See 13.11 “Enabling FIPS security for NFM-P network management” (p. 384) for information about using FIPS security.

14

Configure the `main-server` parameters in the following table, and then enter **back** ↵.

Table 14-64 Auxiliary server parameters — main-server

Parameter	Description
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: —

Table 14-64 Auxiliary server parameters — main-server (continued)

Parameter	Description
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 14-65 Auxiliary server parameters — data-sync

Parameter	Description
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 14-66 Auxiliary server parameters — tls

Parameter	Description
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
pki-server	The PKI server IP address or hostname Default: —
pki-server-port	The TCP port on which the PKI server listens for and services requests Default: 2391

Table 14-66 Auxiliary server parameters — tls (continued)

Parameter	Description
regenerate-certs	Whether to regenerate the internal TLS certificates Certificate regeneration is required when the current certificates are about to expire, or a new internal root certificate is available. A new internal root certificate is available when the root certificate is reset, or when the PKI server is run on a station other than the station used for the previous certificate deployment. Default: false

17

As required, configure the `oss` parameters in the following table, and then enter **`back`** ↵.

Table 14-67 Auxiliary server parameters — oss

Parameter	Description
public-ip	The IP address that the XML API clients must use to reach the auxiliary server Default: IP address of primary network interface
xml-output	The directory that is to contain the output of XML API file export operations Default: /opt/nsp/nfmp/server/xml_output

18

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:

   ```
   bash$ /opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash auxstart ↵
   ```

   The auxiliary server starts.

22

Close the open console windows.

END OF STEPS

14.18 To add auxiliary servers to an NFM-P system

14.18.1 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*

14.18.2 Steps

1

Start the PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 4.10 “To configure and enable a PKI server” (p. 113).

Note: The PKI server is required for internal system configuration purposes.

2

If you are using the manual TLS deployment method, generate and distribute the required TLS files for the system, as described in 4.9 “To generate custom TLS certificate files for the NSP” (p. 108).

3

If the NFM-P is deployed in a standalone configuration, go to Step 7.

4

Perform Step 7 to Step 17 on the standby main server, which is called Server B.

5

Perform Step 7 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 in Step 18.

6

Go to Step 19.

7

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

8

Open a console window.

9

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.

5. Enter the following to switch back to the root user:

```
bash$ su ↵
```

6. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to display the nspOS service status:

```
# nspdctl status ↵
```

Information like the following is displayed.

```
Mode:      redundancy_mode
Role:      redundancy_role
DC-Role:   dc_role
DC-Name:   dc_name
Registry:  IP_address:port
State:     stopped
Uptime:    0s
SERVICE            STATUS
service_a          inactive
service_b          inactive
service_c          inactive
```

You must not proceed to the next step until all NSP services are stopped; if the State is not ‘stopped’, or the STATUS indicator of each listed service is not ‘inactive’, repeat this substep.

10

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

11

Enter the following:

```
<main> configure aux ↵
```

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 14-68 Main server aux parameters

Parameter	Description
stats	If enabled, specifies that one or more auxiliary servers are to be used for statistics collection Default: false
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: —

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.

15

If the configuration is correct, enter the following:

```
<main> apply ↵
```

The configuration is applied.

16

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

17

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.

18

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.

19

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/oracle19/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/oracle19/bin/lsnrctl stop ↵
   ```
10. Enter the following to start the Oracle database listener:

    ```
    bash$ /opt/nsp/nfmp/oracle19/bin/lsnrctl start ↵
    ```

20

Close the open console windows.

END OF STEPS

Auxiliary database installation

14.19 Installing an auxiliary database

14.19.1 Description

This section describes standalone and geographically redundant, or geo-redundant, auxiliary database installation.

Note: An auxiliary database must be deployed as part of an NFM-P system, and cannot function in an NSP system that does not include the NFM-P.

Conversion to geo-redundancy

14.25 “To convert a standalone auxiliary database to geo-redundancy” (p. 583) describes how to convert a standalone auxiliary database to a geo-redundant auxiliary database by adding a new auxiliary database cluster in a standby data center.

14.20 Auxiliary database installation workflow

14.20.1 Description

CAUTION

Deployment Requirement

An auxiliary database requires one or more dedicated stations.

You cannot install the auxiliary database software on a station if another NSP system component is installed on the station.

CAUTION

Service Disruption

If a firewall is in place, you must ensure that the firewall allows the required traffic to pass between the auxiliary database and other components in the deployment before you attempt to install the auxiliary database.

See the NSP Planning Guide for port assignment and firewall configuration information.

CAUTION

Performance Degradation Risk

If the internal communication among the stations in an auxiliary database cluster is not confined to an isolated private network, management network congestion may result.

The internal communication among the stations in an auxiliary database cluster requires a dedicated private network. Each station IP address used for internal communication must be associated with an interface connected to the private network, and must be the only IP address of the interface.

This section describes how to:

- Install and enable an auxiliary database in a new or existing NSP deployment; see 14.20.2 “Workflow for auxiliary database installation” (p. 556).
- Add a new station to an existing auxiliary database; see 14.24 “To add a station to an auxiliary database” (p. 571).

Note: You must set CPU frequency scaling 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” CPU frequency scaling governor on a station.

Setting CPU frequency scaling to “performance” effectively disables the function, so may result in greater energy consumption by a station.

14.20.2 Workflow for auxiliary database installation

The following is the sequence of high-level actions required to install and enable an auxiliary database. You can use the workflow and associated procedures to deploy a standalone auxiliary database cluster in one data center, or geo-redundant auxiliary database clusters in separate data centers.

Stages

1

Perform the following sequence of procedures in the standalone or primary data center.

1. Perform procedure 14.21 “To prepare a station for auxiliary database installation” (p. 558) on each auxiliary database station.
2. Perform procedure 14.22 “To install the auxiliary database software” (p. 561).
3. Perform procedure 14.23 “To add an auxiliary database to a deployment” (p. 564).

2

If you are deploying a geo-redundant auxiliary database, perform the following sequence of actions in the standby data center.

1. Stop the standby auxiliary database cluster.

2. Perform procedure 14.21 “To prepare a station for auxiliary database installation” (p. 557) on each auxiliary database station.
3. Perform procedure 14.22 “To install the auxiliary database software” (p. 561).
4. Perform procedure 14.23 “To add an auxiliary database to a deployment” (p. 564).

14.21 To prepare a station for auxiliary database installation

14.21.1 Purpose

The following steps describe how to configure a station in advance of 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.

14.21.2 Steps

1

Log in as the root user on the auxiliary database station.

2

Open a console window.

3

Add a hostname entry for the new station to the /etc/hosts file on the new station using the following criteria:

- The first entry for the station hostname in the file must be the station IP address that is reachable by each main server.
- The hostname must be the fully qualified hostname, and not the short hostname.
- The hostname must:
  - contain only ASCII alphanumeric and hyphen characters.
  - not begin or end with a hyphen.
  - not begin with a number.
  - comply with the format defined in IETF RFC 1034.
  - use period characters delimit the FQDN components.
  - not exceed 63 characters.

Note: Hostnames are case-sensitive.

4

Perform 3.3 “To apply the RHEL 8 swappiness workaround” (p. 66) on the station.

5

Download the following installation files to an empty local directory:

Note: You must ensure that the directory is empty.

Note: In subsequent steps, the directory is called the software directory.

- nspos-auxdb-*R.r.p*-rel.*v*.rpm
- VerticaSw_PreInstall.sh
- nspos-jre-*R.r.p*-rel.*v*.rpm
- vertica-*R.r.p*-rel.tar

where

R.r.p is the NSP release identifier, in the form *MAJOR.minor.patch*

v is a version number

6

Navigate to the software directory.

Note: The directory must contain only the installation files.

7

Enter the following:

```
# chmod +x * ↵
```

8

Enter the following:

```
# ./VerticaSw_PreInstall.sh ↵
```

The script displays configuration messages like the following, and a prompt:

```
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 samauxdb...
Set password for samauxdb...
```

```
New password:
```

9

Enter a password that conforms to the RHEL password criteria.

The following prompt is displayed:

```
Retype new password:
```

10

Re-enter the password.

Messages like the following are displayed:

```
Changing password for user samauxdb.

passwd: all authentication tokens updated successfully.

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...
```

11

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 software directory.

12

Enter the following:

```
# tar xvf vertica-R.r.p-rel.tar $(tar tf vertica-R.r.p-rel.tar | sort
-V | tail -1) ↵
```

13

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt for each package:

```
Total size: nn G
```

```
Installed size: nn G
Is this ok [y/d/N]:
```

14

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

15

When the package installation is complete, close the console window.

END OF STEPS

14.22 To install the auxiliary database software

14.22.1 Purpose

The following steps describe how to install and initialize the auxiliary database software.

ℹ **Note:** You must perform the procedure on each auxiliary database cluster in a geo-redundant deployment.

ℹ **Note:** You require root user privileges on each auxiliary database station.

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

14.22.2 Steps

1

Start the PKI server, if the server is not running; perform 4.10 “To configure and enable a PKI server” (p. 113).

ℹ **Note:** The PKI server is required for internal system configuration purposes.

2

Log in to any auxiliary database station as the root user.

3

Open a console window.

4

Enter the following:

```
# cp /opt/nsp/nfmp/auxdb/install/config/install.config.default
/opt/nsp/nfmp/auxdb/install/config/install.config ↵
```

5

Open the /opt/nsp/nfmp/auxdb/install/config/install.config file using a plain-text editor such as vi.

6

CAUTION

Service disruption

Changing a parameter in the auxiliary database install.config file can have serious consequences that include service disruption.

Do not change any parameter in the install.config file, other than the parameters described in the step, without guidance from technical support.

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 for communication with other components in the deployment

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]
```

Note: If required, for a single-station auxiliary database you can specify the same address for internal communication and for communication with other components. In such a scenario, you must specify the same address as the *internal_IP* value and the *export_IP* value.

7

To enable TLS, edit the following lines in the file to read as shown below:

Note: The **secure** value must match the **secure** value in the **auxdb** section of the NSP and NFM-P system configurations.

```
secure=true
pki_server=server
pki_server_port=port
```

where

server is the PKI server IP address or hostname

port is the PKI server port number

8

Save and close the install.config file.

9

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.

10

Enter the required password at each prompt. The script installs the software on the station.

11

When the script execution is complete, if you are deploying a geo-redundant auxiliary database, perform the following steps on each auxiliary database station in the current cluster.

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following:

   ```
   bash$ su - samauxdb ↵
   ```

4. Enter the following for each station in the geo-redundant cluster:

   ```
   bash$ ssh-copy-id station_IP ↵
   ```

   where *station_IP* is the IP address of a station in the geo-redundant cluster

12

Perform the following steps on each auxiliary database station in the current cluster.

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following:

   ```
   # systemctl start nspos-auxdbproxy.service ↵
   ```

   The auxiliary database proxy starts.

13

If no other components are to be deployed, stop the PKI server by entering Ctrl+C in the console window.

14

Close the open console windows.

End of steps

14.23 To add an auxiliary database to a deployment

14.23.1 Purpose

The following steps describe how to enable an auxiliary database in an NSP deployment and configure communication between the database and the NSP clusters and NFM-P main servers in the deployment.

CAUTION

Service Disruption

This procedure requires a restart of each NFM-P main server, so is service-affecting.

Perform this procedure only during a scheduled maintenance period.

Note: You must perform the procedure in each data center.

Note: In a redundant deployment, you must perform the procedure first in the standby data center.

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.

14.23.2 Steps

Verify auxiliary database operation

1

Ensure that the auxiliary database is operational.

Note: After you add an auxiliary database to an NFM-P 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:

   ```
   # /opt/nsp/nfmp/auxdb/install/bin/auxdbAdmin.sh status ↵
   ```

   The script displays the following:

   ```
   Database status
   Node       | Host           | State | Version | DB
   ------------+---------------+-------+---------+-------
   node_1 | internal_IP_1 | STATE | version | db_name
   node_2 | internal_IP_2 | STATE | version | db_name
   .
   .
   .
   node_n | internal_IP_n | STATE | version | db_name
         Output captured in log_file
   ```
4. If each *STATE* is not UP, contact technical support for assistance.

Configure TLS on auxiliary database station

2

Open the following file using a plain-text editor such as vi:

/opt/nsp/nfmp/auxdb/install/config/install.config

3

CAUTION

Service disruption

Changing a parameter in the auxiliary database install.config file can have serious consequences that include service disruption.

Do not change any parameter in the install.config file, other than the parameters described in the step, without guidance from technical support.

Edit the following lines in the file to read as shown below:

Note: If you set the secure parameter to false, you do not need to configure the PKI-server parameters.

```
secure=value
```

```
pki_server=server
```

```
pki_server_port=port
```

where

value is true or false, and indicates whether TLS is enabled

server is the PKI server IP address or hostname

port is the PKI server port number

4

Save and close the install.config file.

Configure NFM-P main server

5

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

6

Open a console window.

7

Stop the main server.

1. Enter the following:

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

2. Enter the following:

   ```
   bash$ ./nmsserver.bash stop ↵
   ```

3. 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.

4. Enter the following to switch to the root user:

```
bash$ su ↵
```

5. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to display the nspOS service status:

```
# nspdctl status ↵
```

Information like the following is displayed.

```
Mode:      redundancy_mode
Role:      redundancy_role
DC-Role:   dc_role
DC-Name:   dc_name
Registry:  IP_address:port
State:     stopped
Uptime:    0s
SERVICE           STATUS
service_a         inactive
service_b         inactive
service_c         inactive
```

You must not proceed to the next step until all NSP services are stopped; if the State is not ‘stopped’, or the STATUS indicator of each listed service is not ‘inactive’, repeat this substep.

8

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

9

CAUTION

Misconfiguration Risk

If the station IP-address order in each main server configuration is not identical, the auxiliary database addition fails.

Ensure that the auxiliary database station addresses are listed in the same order in each main server configuration.

In a geo-redundant auxiliary database deployment, the order of the IP addresses must match in each main server configuration in each data center.

Enter the following:

```
<main> configure auxdb enabled ip-list cluster_1_IP1,cluster_1_IP2,
cluster_1_IPn;cluster_2_IP1,cluster_2_IP2,cluster_2_IPn ↵
```

where

cluster_1_IP1, *cluster_1_IP2*,*cluster_1_IPn* are the external IP addresses of the stations in one cluster

cluster_2_IP1, *cluster_2_IP2*,*cluster_2_IPn* are the external IP addresses of the stations in the geo-redundant cluster; required only for geo-redundant auxiliary database

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

10

CAUTION

Misconfiguration Risk

After you configure any `auxdb` *parameter on a main server and start the main server, you cannot modify the* `redundancy-level` *parameter.*

Ensure that you are certain of the `redundancy-level` *setting before you save the configuration.*

Perform one of the following.

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 ↵
```

11

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

12

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

13

Enter the following to switch back to the nsp user:

```
# exit ↵
```

Start main server, verify statistics migration

14

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.

15

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.

16

Close the console window.

Configure NSP cluster

17

If the NFM-P is in a shared-mode deployment, log in as the root user on the NSP deployer host in the local NSP cluster.

Otherwise, go to Step 23.

18

Open the following file using a plain-text editor such as vi:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

19

Locate the following section:

```
auxDb:
  secure: "value"
  ipList: ""
  standbyIpList: ""
```

20

Edit the section to read as follows:

Note: For a geo-redundant auxiliary database, ensure that you record the following, which must be correctly specified in the local NFM-P main server configuration:

- ip_list addresses, which must be specified as the *cluster_1* addresses on the main server
- standby_ip_list addresses, which must be specified as the *cluster_2* addresses on the main server

Note: You must preserve the leading spaces in each line.

```
auxDb:
  secure: "value"
  ipList: "cluster_1_IP1,cluster_1_IP2...cluster_1_IPn"
  standbyIpList: "cluster_2_IP1,cluster_2_IP2...cluster_2_IPn"
```

where

cluster_1_IP1, *cluster_1_IP2*...*cluster_1_IPn* are the external IP addresses of the stations in the local cluster

value is true or false, and specifies whether TLS is enabled

cluster_2_IP1, *cluster_2_IP2*...*cluster_2_IPn* are the external IP addresses of the stations in the peer cluster; required only for geo-redundant deployment

21

Save and close the nsp-config.yml file.

22

Enter the following to start the NSP cluster:

```
# /opt/nsp/NSP-CN-DEP-release-ID/bin/nspdeployerctl install --config
--deploy ↵
```

The NSP configuration is updated to include the auxiliary database.

Verify backup configuration

23

Regular auxiliary database backups are strongly recommended. Ensure that scheduled database backups are enabled to ensure minimal data loss in the event of a failure. See the *NSP System Administrator Guide* for information.

END OF STEPS

14.24 To add a station to an auxiliary database

14.24.1 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 NFM-P main server, so is service-affecting.

Perform this procedure only during a scheduled maintenance period.

Note: You cannot add a station to a one-station auxiliary database.

Note: The primary and standby auxiliary database clusters in a geo-redundant deployment require the same number of stations.

14.24.2 Steps

Install software

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 using the following criteria.

- The first entry for the station hostname in the file must be the station IP address that is reachable by each main server.
- The hostname must be the fully qualified hostname, and not the short hostname.
- The hostname must:
  - contain only ASCII alphanumeric and hyphen characters.
  - not begin or end with a hyphen.
  - not begin with a number.
  - comply with the format defined in IETF RFC 1034.
  - use period characters delimit the FQDN components.
  - not exceed 63 characters.

ℹ **Note:** Hostnames are case-sensitive.

4

Perform 3.3 “To apply the RHEL 8 swappiness workaround” (p. 66) on the station.

5

Download the following installation files to an empty local directory:

ℹ **Note:** You must ensure that the directory is empty.

ℹ **Note:** The software release must match the software release of the existing auxiliary database.

- nspos-auxdb-*R*.*r*.*p*-rel.*v*.rpm
- VerticaSw_PreInstall.sh
- nspos-jre-*R*.*r*.*p*-rel.*v*.rpm
- vertica-*R*.*r*.*p*-rel.tar

where

R.*r*.*p* is the NSP release identifier, in the form *MAJOR*.*minor*.*patch*

v is a version number

ℹ **Note:** In subsequent steps, the directory is called the software directory.

6

Open a console window.

7

Navigate to the software directory.

ℹ **Note:** The directory must contain only the installation files.

8

Enter the following:

```
# chmod +x * ↵
```

9

Enter the following:

```
# ./VerticaSw_PreInstall.sh ↵
```

The script displays configuration messages like the following, and a prompt:

```
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 samauxdb...
Set password for samauxdb...
New password:
```

10

Enter a password that conforms to the RHEL password criteria.

The following prompt is displayed:

```
Retype new password:
```

11

Re-enter the password.

Messages like the following are displayed:

```
Changing password for user samauxdb.
passwd: all authentication tokens updated successfully.
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...
```

12

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 software directory.

13

Enter the following:

```
# tar xvf vertica-R.r.p-rel.tar $(tar tf vertica-R.r.p-rel.tar | sort
-V | tail -1) ↵
```

14

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

15

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

Add new station to auxiliary database configuration

16

When the package installation is complete, perform the folowing steps on each auxiliary database station to stop the database proxy.

Note: If the auxiliary database is geo-redundant, you must stop the database proxy on each station in each auxiliary database cluster.

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following:

   ```
   # systemctl stop nspos-auxdbproxy.service ↵
   ```
4. Verify that the proxy is stopped; enter the following:

   ```
   # systemctl status nspos-auxdbproxy ↵
   ```

17

Log in to an existing auxiliary database station as the root user.

Note: If the auxiliary database is geo-redundant, the station must be in the primary auxiliary database cluster.

18

Open a console window.

19

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 other components in the deployment

The script displays the following:

```
Adding hosts(s) hostname to auxiliary database cluster ...
```

20

You are prompted to enter the auxiliary database dba password.

Enter the samauxdb database administrator password.

21

You are prompted to enter the root user password for the new station.

Enter the password of the root user account on the new station.

22

CAUTION

Installation Failure

If the addition of the station to the auxiliary database is interrupted, the operation 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.

23

When the script execution is complete, open the /opt/nsp/nfmp/auxdb/install/config/install.config file using a plain-text editor such as vi.

24

CAUTION

Service Disruption

Changing a parameter in the auxiliary database install.config file can have serious consequences that include service disruption.

Do not change any parameter in the install.config file, other than the parameters described in the step, without guidance from technical support.

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

25

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

26

Save and close the install.config file.

27

Enter the following:

```
# ./auxdbAdmin.sh distributeConfig ↵
```

The updated auxiliary database configuration is distributed to each auxiliary database station.

Start auxiliary database proxies

28

Perform the following steps on the existing and new auxiliary database stations to start the database proxy.

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following:

   ```
   # systemctl start nspos-auxdbproxy.service ↵
   ```

   The auxiliary database proxy starts.

Rebalance cluster

29

Return to the existing auxiliary database station that you configured in Step 17 to Step 27.

30

Enter the following:

```
# ./auxdbAdmin.sh rebalance ↵
```

The following prompt is displayed:

```
Please enter auxiliary database dba password [if you are doing initial
setup for auxiliary database, press enter]:
```

31

Enter the database user password.

The following messages and prompt are displayed:

```
KSAFE factor of 1 detected

Rebalance was started in the background. Please don't reboot system
until rebalance is completed.

You can track the rebalance process by typing 'ps -fe | grep
rebalance'. Rebalance can take a very long time on large databases.
Please be patient.

Type YES to continue
```

32

CAUTION

Data corruption

Interrupting the rebalance operation can cause data corruption.

Do not interrupt the operation by, for example, rebooting the station.

Enter YES.

The rebalance operation begins, and the following is displayed:

```
Output captured in /opt/nsp/nfmp/auxdb/install/log/auxdbAdmin.sh.
timestamp.log
```

where *timestamp* is the start time of the rebalance operation

33

Monitor the rebalance operation; do not proceed to the next step until the operation is complete.

Note: A rebalance operation on a large database may take several hours.

Enter the following periodically to identify whether the rebalance process is active:

```
# ps -ef | grep rebalance ↵
```

If the rebalance process is active, two lines of output are displayed. If the rebalance is complete, only one line like the following is displayed:

```
root    nnnnn  nnnn 0 hh:mm pts/0   00:00:00 grep --color=auto
rebalance
```

34

When the rebalance is complete, if the auxiliary database is not geo-redundant, go to Step 40.

Update standby auxiliary database configuration

35

Log in to an existing standby auxiliary database station as the root user.

36

Open a console window.

37

Perform Step 19 to Step 33.

38

Stop the standby auxiliary database; enter the following on an existing standby auxiliary database station:

```
# ./auxdbAdmin.sh stop ↵
```

39

Enter the following on each standby auxiliary database station to start the database proxy:

```
# systemctl start nspos-auxdbproxy.service ↵
```

Configure NFM-P main servers

40

CAUTION

Misconfiguration Risk

If you alter the original IP-address assignments, or the order of the IP addresses, the station addition fails.

Do not change any of the original auxiliary database station IP address assignments, or the address order, in the main server configuration.

In a geo-redundant auxiliary database deployment, the order of the IP addresses must match in each main server configuration in each data center.

Perform the following steps on each main server station.

Note: In a geo-redundant system, you must perform the steps on the main servers in each data center.

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. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to display the nspOS service status:

   ```
   # nspdctl status ↵
   ```

   Information like the following is displayed.

   ```
   Mode:     redundancy_mode
   Role:     redundancy_role
   DC-Role:  dc_role
   DC-Name:  dc_name
   Registry: IP_address:port
   State:    stopped
   Uptime:   0s
   SERVICE            STATUS
   service_a          inactive
   service_b          inactive
   service_c          inactive
   ```

   You must not proceed to the next step until all NSP services are stopped; if the State is not ‘stopped’, or the STATUS indicator of each listed service is not ‘inactive’, repeat this substep.

8. Enter the following:

   ```
   # samconfig -m main ↵
   ```

   The following is displayed:

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

9. Enter the following:

   Note: For a geo-redundant auxiliary database, the order of the IP addresses must be the same on each main server in each data center.

   ```
   <main> configure auxdb ip-list IP_list exit ↵
   ```

   where

   IP_list is a list of the IP addresses in the following format:

```
cluster_1_IP1,cluster_1_IP2,cluster_1_IPn,cluster_1_new_IP;cluster_
2_IP1,cluster_2_IP2,cluster_2_IPn,cluster_2_new_IP
```

where *new_IP* is the external IP address of the new station

Note: The format example shows the new address added to cluster_1; cluster_2 addresses are present only for a geo-redundant auxiliary database. Ensure that you add *new_IP* to the address list for the appropriate cluster.

10. Enter the following:

    ```
    <main> apply ↵
    ```

    The configuration is applied.

11. Enter the following:

    ```
    <main> exit ↵
    ```

    The samconfig utility closes.

12. Enter the following to switch back to the nsp user:

    ```
    # exit ↵
    ```

Start NFM-P main servers

41

On the standalone or primary main server station, enter the following to start the main server:

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

The main server starts, and the station is added to the auxiliary database.

42

If the NFM-P system is redundant, enter the following on the standby main server station to start the main server:

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

The main server starts.

Configure NSP clusters

43

If the NFM-P is in a shared-mode deployment, perform Step 44 to Step 52 on the NSP cluster in each data center.

Otherwise, go to Step 53.

44

Log in as the root user on the NSP deployer host.

45

Open the following file using a plain-text editor such as vi:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/nsp-config.yml

46

Locate the following section:

```
auxDb:
  secure: "value"
  ipList: ""
  standbyIpList: ""
```

47

Edit the section to include the new auxiliary database station address, and to specify whether TLS is enabled, as shown below:

Note: You must preserve the leading spaces in each line.

```
auxDb:
  secure: "value"
  ipList: "cluster_1_IP1,cluster_1_IP2,cluster_1_IPn"
  standbyIpList: "cluster_2_IP1,cluster_2_IP2,cluster_2_IPn"
```

where

cluster_1_IP1, *cluster_1_IP2*...*cluster_1_IPn* are the external IP addresses of the stations in the local cluster, including the new station address

cluster_2_IP1, *cluster_2_IP2*,*cluster_2_IPn* are the external IP addresses of the stations in the peer cluster, including the new station address; required only for geo-redundant deployment

48

Save and close the nsp-config.yml file.

49

Enter the following to put the changes into effect:

```
# /opt/nsp/NSP-CN-DEP-release-ID/bin/nspdeployerctl install --config
--deploy ↵
```

The NSP configuration is updated.

50

Enter the following:

```
# kubectl get pods -A ↵
```

The pods are listed.

51

Locate the auxiliary database pod entry, which resembles the following:

```
nsp-psa-restricted     nspos-auxdb-agent-pod_ID     1/1
Running      0         uptime
```

52

Enter the following:

`# kubectl delete pod nspos-auxdb-agent-pod_ID -n namespace ↵`

where

namespace is the namespace of the pod entry in Step 51

pod_ID is the pod ID of the auxiliary database pod entry in Step 51

The pod is deleted and recreated to include the new station.

53

Close the open console windows.

End of steps

14.25 To convert a standalone auxiliary database to geo-redundancy

14.25.1 Purpose

Perform this procedure to add a new auxiliary database cluster of one or more stations to an existing standalone deployment in order to create a disaster-recovery, or DR, deployment in redundant data centers.

Note: The new auxiliary database cluster must have the same number of stations as the existing standalone cluster.

14.25.2 Steps

1

Perform 14.21 “To prepare a station for auxiliary database installation” (p. 558) on each station in the new auxiliary database cluster.

2

Perform 14.22 “To install the auxiliary database software” (p. 561) on the auxiliary database cluster in each data center.

Note: You must perform the steps first on the new cluster, which is the standby cluster after the conversion.

3

Perform 14.23 “To add an auxiliary database to a deployment” (p. 564) to add the new auxiliary database cluster to the configuration of each NFM-P main server and NSP cluster in each data center.

END OF STEPS

NFM-P single-user GUI client installation

14.26 Installing an NFM-P single-user GUI client

14.26.1 Description

The following procedures describe single-user GUI client installation in a standalone or redundant NFM-P system. You must comply with the general requirements in 14.8 “Installing the NFM-P” (p. 431), and any specific requirements in this section , before you attempt to deploy a single-user GUI client.

Supported deployments

You can install multiple single-user GUI clients on one station, or on separate stations. The multiple clients installed on one station can be at various releases and associated with the different NFM-P systems.

You can also configure one single-user client to connect to multiple NFM-P systems. For information , see 13.19 “To configure a GUI client login form to list multiple NFM-P systems” (p. 394).

14.26.2 Platform requirements

Single-user GUI client installation is supported on the following platforms:

- Mac OS X
- Microsoft Windows
- RHEL

See the *NSP Planning Guide* for OS-version support information.

Common to all OS

The following are the security requirements for single-user client deployment:

- Installation 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 deployment requires a supported web browser on the client station. See the *NSP Planning Guide* for browser support information.

Mac OS

See the *NSP Planning Guide* for the Mac OS single-user client deployment requirements.

Microsoft Windows

See the *NSP Planning Guide* for the Microsoft Windows single-user client deployment requirements.

RHEL

A RHEL single-user GUI client station must have:

- a supported OS release and patch level, as described in the *NSP Planning Guide*
- the required RHEL OS configuration and packages, as described in Chapter 3, “RHEL OS deployment for the NSP”

Optionally, for greater system security, you can remove the world permissions from RHEL compiler executable files; see A.1 “Resetting GCC-compiler file permissions” (p. 1093) for information.

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

14.27 To install an NFM-P single-user GUI client

14.27.1 Purpose

The following steps describe how to install the single-user GUI client software on a station.

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.

Note: A leading `bash$` in a CLI command line represents the RHEL prompt, and is not to be included in the command.

14.27.2 Steps

1

Create a local folder to hold the client installation software.

2

Use a browser on the client station to open one of the following URLs:

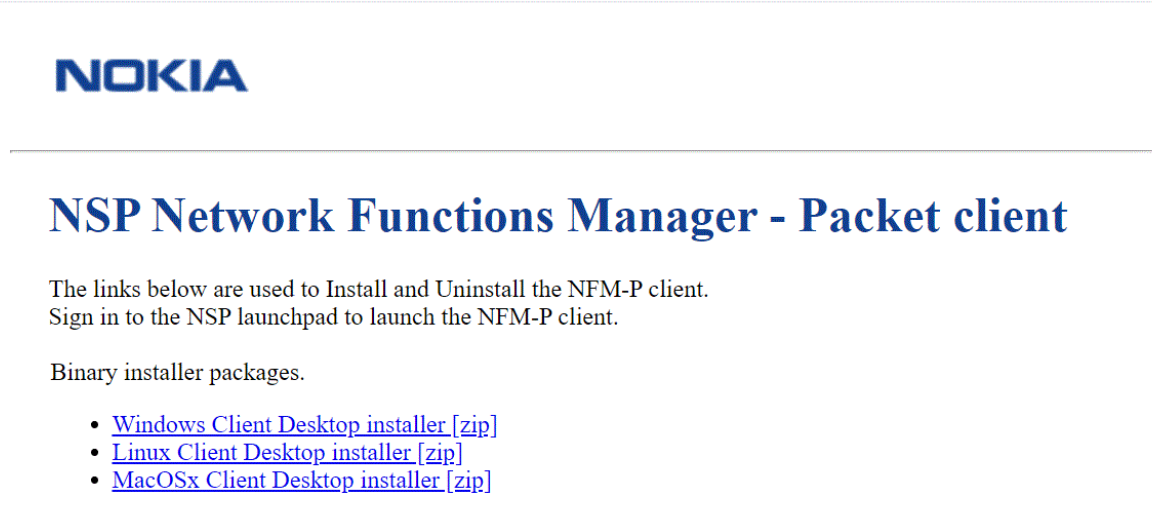
- http://*server*:8085/client, if TLS for client access is disabled
- https://*server*:8444/client, if TLS for client access is enabled

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 14-1, “NSP Network Functions Manager - Packet client” (p. 587) opens.

Figure 14-1 NSP Network Functions Manager - Packet client



NSP Network Functions Manager - Packet client

The links below are used to Install and Uninstall the NFM-P client.
Sign in to the NSP launchpad to launch the NFM-P client.

Binary installer packages.

- Windows Client Desktop installer [zip]
- Linux Client Desktop installer [zip]
- MacOSx Client Desktop installer [zip]

3

Click on the appropriate Binary installer packages link for your client station OS to download the installer zip file.

4

Fully unzip the contents of the downloaded file to the temporary folder created at the beginning of the procedure.

Note: Do not run the installer from a zip-file preview window.

5

If you are installing a single-user client on Windows, open the nfmp_win_client executable file in the temporary folder. An installation wizard is displayed.

Note: You may need to unquarantine the file if your virus scanner identifies the file as unknown.

6

If you are installing a single-user client on RHEL, perform the following steps.

1. Open a console window.

2. Navigate to the temporary folder.
3. Enter the following:

   ```
   bash$ ./install_nfmp_linux_client.sh ↵
   ```

   A Network Functions Manager - Packet icon is created in the Desktop folder. The icon is automatically renamed to include the client software version as part of the installation.
4. Open the Desktop folder.
5. Double-click on the Network Functions Manager - Packet icon, and acknowledge any prompt about allowing a security exemption.

7

If you are installing a single-user client on Mac OS, perform the following steps.

Note: Each client package has a different name that corresponds to the server IP address. Multiple client installations on one station are supported, but only one client installation per server is allowed.

1. A package called NFMPclient.*IP_address* is displayed, where *IP_address* is the main server IP address. Mac OS security prevents the application from being renamed.
2. Drag the package to move it to your desktop or application folders.
3. Right-click on the package and choose Open. You are prompted to accept a security exemption.
4. Accept the security exemption.

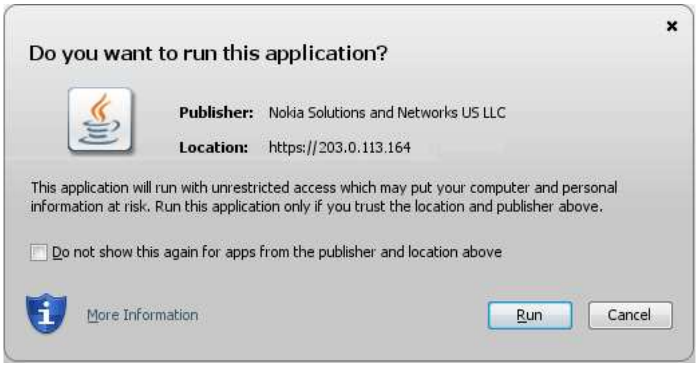
8

Follow the prompts to specify the client installation directory, whether you want a desktop shortcut created, and whether to run the client when the installation is complete, as required.

Note: Depending on the OS type, one or more prompts may not be present.

After you click Finish, a form like the following is displayed.

Figure 14-2 Do you want to run this application?



Do you want to run this application?

Publisher: Nokia Solutions and Networks US LLC

Location: https://203.0.113.164

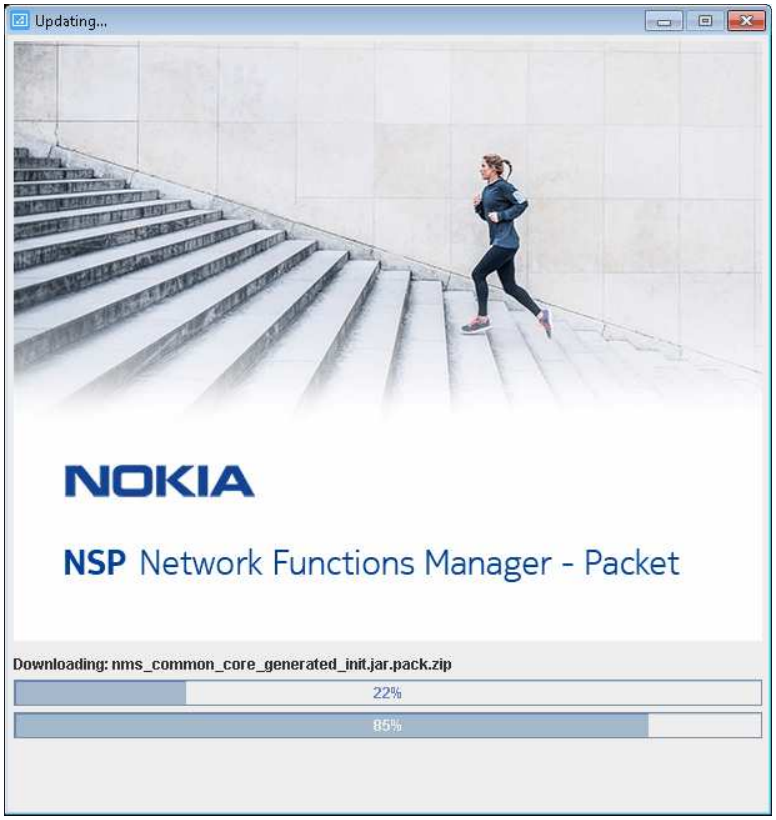
This application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the location and publisher above.

□ Do not show this again for apps from the publisher and location above

9

Click Run. The client installation begins, and the panel shown in Figure 14-3, “Updating...” (p. 588) is displayed. The panel uses separate bars to indicate the overall and current task progress.

Figure 14-3 Updating...



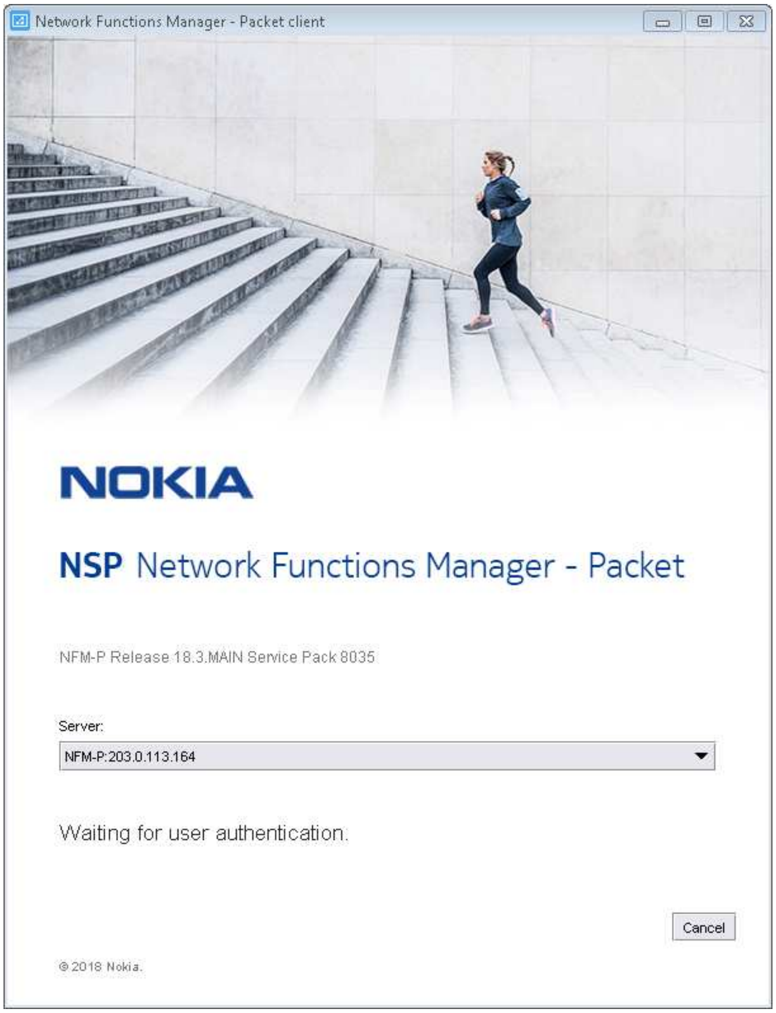
Downloading: nms_common_core_generated_init.jar.pack.zip

10

If you are not currently logged in, the splash screen shown in Figure 14-4, “Waiting for user authentication” (p. 590) opens, and the NSP sign-in page is displayed.

Enter the required login credentials on the NSP sign-in page and click SIGN IN. The NSP UI is displayed, and the client GUI opens.

Figure 14-4 Waiting for user authentication



Network Functions Manager - Packet client
NOKIA
NSP Network Functions Manager - Packet

NFM-P Release 18.3.MAIN Service Pack 8035

Server:
NFM-P:203.0.113.164

Waiting for user authentication.

End of steps

NFM-P client delegate server installation

14.28 Installing an NFM-P client delegate server

14.28.1 Description

This section describes client delegate server installation in a standalone or redundant NFM-P system. You must comply with the general requirements in “NFM-P deployment configuration” (p. 370) and the specific requirements in this section before you attempt to deploy a client delegate server.

14.28.2 Platform requirements

Client delegate server deployment is supported on the following platforms:

- 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 Planning Guide* for a list of the ports that must be open on each component.

Note: Adding a client delegate server to an existing NFM-P system requires root and nsp user privileges on each main server station.

Note: Client delegate server deployment requires a supported web browser on the client delegate server station. See the *NSP Planning Guide* for browser support information.

Microsoft Windows

See the *NSP Planning Guide* for the supported Microsoft Windows versions for client delegate server deployment.

Note: Client delegate server deployment on Windows requires local Administrator privileges.

RHEL

A RHEL client delegate server station must have:

- a supported OS release and patch level, as described in the *NSP Planning Guide*
- the required RHEL OS configuration and packages, as described in Chapter 3, “RHEL OS deployment for the NSP”
- the required Oracle JRE version; see the *NSP Planning Guide* for information

Optionally, for greater system security, you can remove the world permissions from RHEL compiler executable files; see A.1 “Resetting GCC-compiler file permissions” (p. 1093) for information.

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.

14.29 To add a client delegate server to an NFM-P system

14.29.1 Purpose

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: In order to install a client delegate server, you must specify the client delegate server address and installation location in each main server configuration, as described in the procedure.

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.

14.29.2 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.

3

Perform Step 7 to Step 19 on the primary main server.

4

Perform Step 20 on the primary main server station.

5

When the primary main server is fully operational, perform Step 20 on the standby main server station.

6

Go to Step 21.

7

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

8

Open a console window.

9

If you plan to use a hostname rather than an IP address for the client delegate server, add an entry to the /etc/hosts file on the main server that maps the client delegate server hostname to the IP address.

10

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.

5. Enter the following to switch to the root user:

```
bash$ su ↵
```

6. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to display the nspOS service status:

```
# nspdctl status ↵
```

   Information like the following is displayed.

```
Mode:      redundancy_mode
Role:      redundancy_role
```

```
DC-Role:  dc_role
DC-Name:  dc_name
Registry: IP_address:port
State:    stopped
Uptime:   0s
SERVICE            STATUS
service_a          inactive
service_b          inactive
service_c          inactive
```

You must not proceed to the next step until all NSP services are stopped; if the State is not ‘stopped’, or the STATUS indicator of each listed service is not ‘inactive’, repeat this substep.

11

Enter the following:

```
# 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>`.

18

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

19

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

20

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.

21

Close the open console windows.

END OF STEPS

14.30 To install an NFM-P client delegate server

14.30.1 Purpose

The following steps describe how to install the client delegate server software on a RHEL or Microsoft Windows station.

ℹ **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 14.29 “To add a client delegate server to an NFM-P system” (p. 592).

ℹ **Note:** The main server to which the client delegate server connects must be running and operational when you perform the procedure.

ℹ **Note:** You require the following user privileges on the client delegate server station:

- Microsoft Windows—local Administrator
- RHEL—root

ℹ **Note:** A leading # in a CLI command line represents the RHEL prompt, and is not to be included in the command.

14.30.2 Description

1

If you are installing the client delegate server on RHEL, you must create a RHEL user group called nsp, and a RHEL user called nsp as a member of the nsp group; perform the following steps.

1. Log in as the root user on the client delegate server station.
2. Open a console window.
3. Enter the following:

```
# groupadd nsp; useradd -d home_dir -g nsp nsp ↵
```

where *home_dir* is the user home directory, for example, /opt/nsp

The nsp user group is created with the nsp user as a member.

2

Create a local folder to hold the client installation software.

3

Use a browser on the client delegate server station to open one of the following URLs:

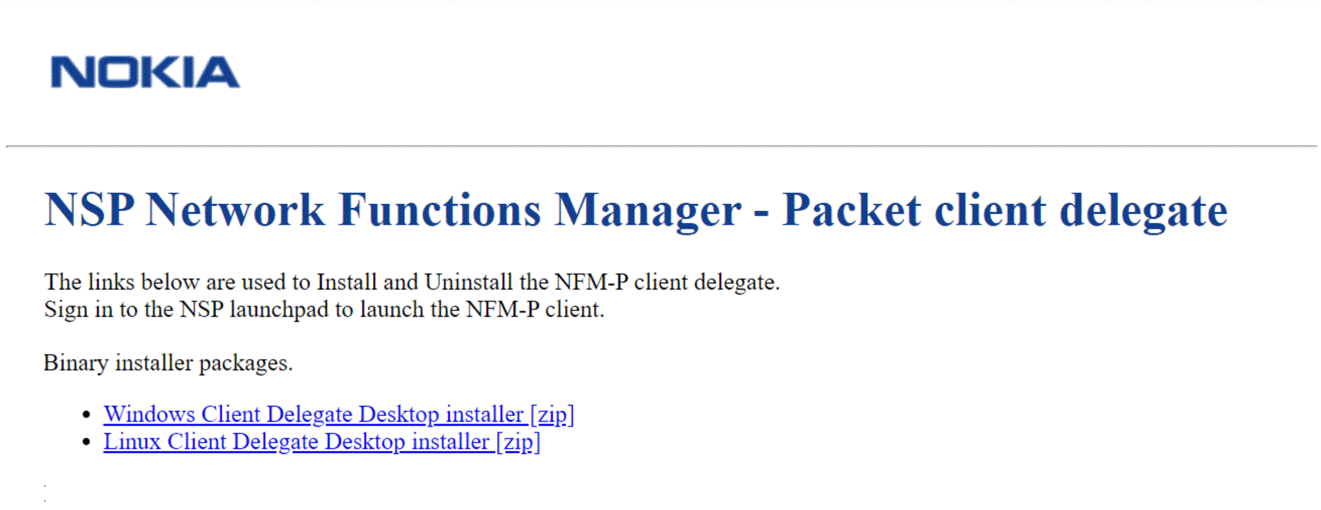
- http://*server*:8085/clientdelegate, if TLS for client access is disabled
- https://*server*:8444/clientdelegate, if TLS for client access is enabled

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 14-5, “NSP Network Functions Manager - Packet client” (p. 596) opens.

Figure 14-5 NSP Network Functions Manager - Packet client



NOKIA

NSP Network Functions Manager - Packet client delegate

The links below are used to Install and Uninstall the NFM-P client delegate.
Sign in to the NSP launchpad to launch the NFM-P client.

Binary installer packages.

- Windows Client Delegate Desktop installer [zip]
- Linux Client Delegate Desktop installer [zip]

4

Click on the appropriate Binary installer packages link for the client delegate server OS to download the installer zip file.

5

Fully unzip the contents of the downloaded file to the temporary folder created at the beginning of the procedure.

Note: Do not run the installer from a zip-file preview window.

6

If you are installing a client delegate server on Windows 2012, right-click on the nfmp_win_delegate file and choose Run as administrator. An installation wizard is displayed.

ℹ **Note:** You may need to unquarantine the file if your virus scanner identifies the file as unknown.

7

If you are installing a client delegate server on Windows 2016, open the nfmp_win_delegate executable file in the temporary folder. An installation wizard is displayed.

ℹ **Note:** You may need to unquarantine the file if your virus scanner identifies the file as unknown.

8

If you are installing a client delegate server on RHEL, perform the following steps.

1. Log in as the root user on the client delegate server station.
2. Open a console window.
3. Navigate to the temporary folder.
4. Enter the following:

   ```
   # ./install_nfmp_linux_delegate.sh ↵
   ```

   A Network Functions Manager - Packet icon is created in the Desktop folder. The icon is automatically renamed to include the client software version as part of the installation.
5. Open the Desktop folder.
6. Double-click on the Network Functions Manager - Packet icon, and acknowledge any prompt about allowing a security exemption.

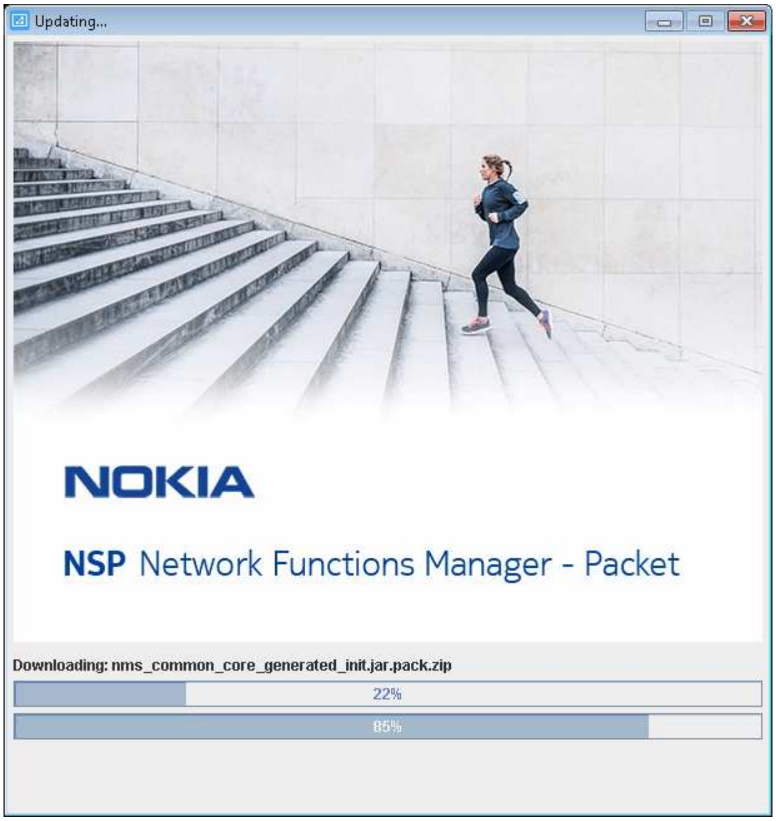
9

Follow the prompts to specify the client delegate server type, whether you want a desktop shortcut created, and whether to run the client when the installation is complete, as required.

ℹ **Note:** Depending on the OS type, one or more prompts may not be displayed.

After you click Finish, the client installation begins, and the panel shown in Figure 14-6, “Updating...” (p. 599) is displayed. The panel uses separate bars to indicate the overall and current task progress.

Figure 14-6 Updating...



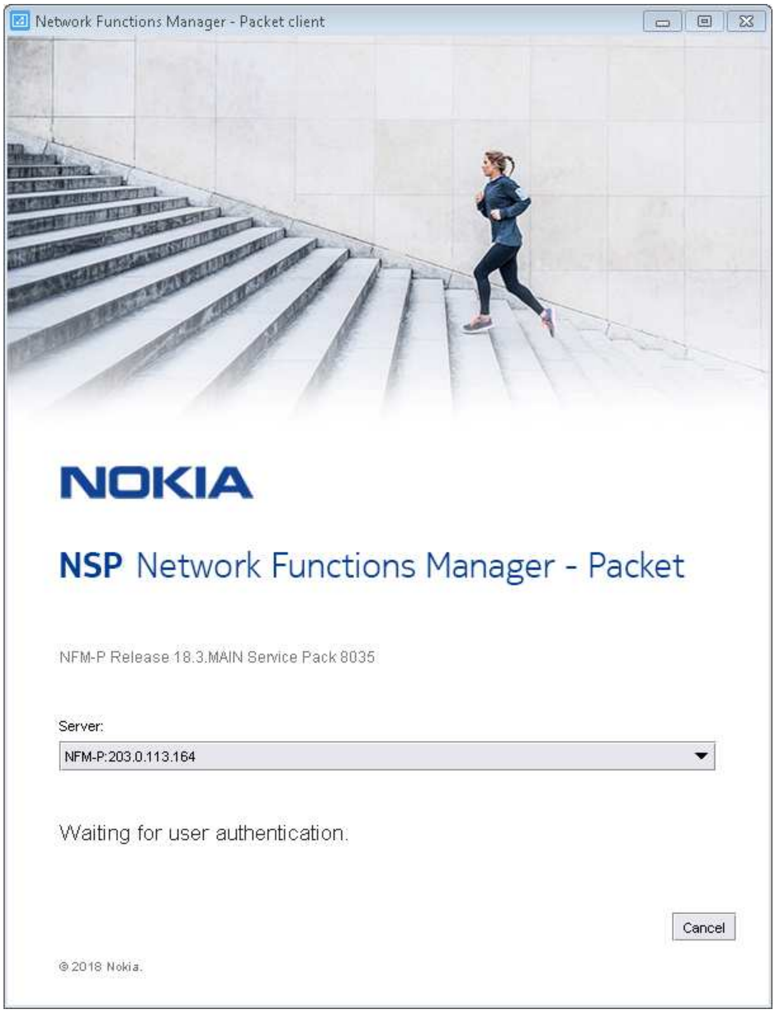
Downloading: nms_common_core_generated_init.jar.pack.zip

10

If you are not currently logged in, the splash screen shown in Figure 14-7, “Waiting for user authentication” (p. 600) opens, and the NSP sign-in page is displayed.

Enter the required login credentials on the NSP sign-in page and click SIGN IN. The NSP UI is displayed, and the client GUI opens.

Figure 14-7 Waiting for user authentication


Network Functions Manager - Packet client
NOKIA
NSP Network Functions Manager - Packet

NFM-P Release 18.3.MAIN Service Pack 8035

Server: NFM-P:203.0.113.164

Waiting for user authentication.

11

If you are installing on Windows, you must enable the Modify access privilege on the installation folder for each Windows-authenticated user of the client delegate server.

Perform the following steps as a user with local administrative privileges.

Note: The steps may vary, depending on the Windows version, and may need to be repeated for multiple users or user groups.

1. Right click on the client delegate server installation folder and choose Properties. The folder properties form opens.
2. Click the Security tab.
3. Click Advanced.

4. Select the required user or user group, for example the Authenticated Users group.
5. Click Add and select the Modify attribute.
6. Save your changes and close the open forms.

12

If required, enable local client access for other users on the client delegate server station.

1. Move the client desktop shortcut to the local public desktop folder, for example, C:\Users\Public\Desktop on a Windows PC.
2. Enable Read and Execute privileges on the shortcut for specific users or all users, as required.

END OF STEPS

15 NSP component upgrade from Release 22.6 or earlier

15.1 Overview

15.1.1 Purpose

This chapter describes the upgrade of Release 22.6 or earlier NSP components that are deployed outside the NSP cluster.

15.1.2 Contents

Auxiliary server upgrade from Release 22.6 or earlier 760

Auxiliary database upgrade from Release 22.6 or earlier 767

NFM-P single-user GUI client upgrade from Release 22.6 or earlier 782

NFM-P client delegate server upgrade from Release 22.6 or earlier 790

Upgrading NSP components

15.2 NSP component upgrade overview

15.2.1 Component upgrade support

CAUTION

Service Disruption

An NFM-P system upgrade 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 Planning Guide, and the NSP 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 NSP professional services 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.

CAUTION

Deployment failure

You cannot successfully upgrade an NSP component that has never initialized.

Before you attempt an NSP component upgrade, ensure that the component has successfully initialized.

Before you attempt to perform a procedure in this chapter, you must ensure that your deployment meets the hardware and software requirements described in the *NSP Planning Guide*.

Note: When you upgrade a shared-mode NSP system that includes the NFM-P, the existing Service Supervision groups are migrated from the NFM-P to the NSP. The migration may take a few hours, depending on the number of services. During this time, you must not auto-create Service Supervision groups. You can use the Find Ungrouped members count in the Group Manager application to help determine when the upload is complete, after which you can auto-create groups.

Note: It is strongly recommended that you verify the GPG signature of each RPM file that you download from Nokia to ensure that each file has a valid Nokia signature.

Note: It is strongly recommended that you verify the message digest of each NSP image file or software bundle that you download from the Nokia Support portal. The download page includes the MD5, SHA256, and SHA512 checksums for comparison with the output of the RHEL md5sum, sha256sum, or sha512sum command. See the associated RHEL man page for command usage information.

Note: If you have modified any NFM-P template files, contact technical support before you attempt an NSP or NFM-P system upgrade; an upgrade overwrites customized template values.

Note: NFM-P language localization files are not automatically backed up during an NSP upgrade. To preserve your language localization, you must back up your localization file before an NSP upgrade, and then redeploy the file after the upgrade.

Shared-mode upgrades

CAUTION

Upgrade Failure

If the system locales of the NFM-P and the NSP components of a shared-mode deployment do not match, a system upgrade may fail.

Ensure that the NSP system locale matches the NFM-P locale before you attempt a shared-mode system upgrade. If the locales do not match, contact technical support for assistance.

The components that comprise a shared-mode NSP deployment must be upgraded in a specific order, starting with the NSP cluster. During the upgrade, the NSP UI is unavailable, as is an NFM-P or WS-NOC that is part of the NSP system. After the NSP component upgrade, the NFM-P and WS-NOC can be upgraded in any order.

See the NSP compatibility matrix in the *NSP Release Notice* to ensure that the proposed upgrade results in a supported configuration.

NSP Flow Collector and Flow Collector Controller upgrade from Release 22.6 or earlier

15.3 To upgrade Release 22.6 or earlier NSP Flow Collector Controllers and NSP Flow Collectors

15.3.1 Purpose

Use this procedure to upgrade the Release 22.6 or earlier standalone or redundant NSP Flow Collector Controllers and NSP Flow Collectors in an NSP data center.

Note: You cannot upgrade an NSP Flow Collector or Flow Collector Controller to a collocated deployment that has both on one station.

Note: The install.sh utility requires SSH access to a target station. To enable SSH access, you must do one of the following.

- Configure the required SSH keys on the stations.
- If each remote station has the same root user password, add the --ask-pass argument to the install.sh command; for example:

  `./install.sh --ask-pass --target` ***`remote_station`***

15.3.2 Steps

Commission new stations, if required

1

If you are deploying any NSP Flow Collector or Flow Collector Controller on a new station, commission the station according to the platform specifications in this guide and in the *NSP Planning Guide*.

Note: The hostname and IP address of a replacement station must match the hostname and IP address of the station being replaced.

For information about deploying the RHEL OS using an NSP OEM disk image, see 2.2.2 “NSP disk-image deployment” (p. 28).

Stop NSP Flow Collector Controllers

2

Perform the following steps on each NSP Flow Collector Controller station to stop the NSP Flow Collector Controller.

Note: If an NSP Flow Collector is also installed on the station, the Flow Collector stops automatically.

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

2. Enter the following:

```
bash$ /opt/nsp/flow/fcc/bin/flowCollectorController.bash stop ↵
```

The NSP Flow Collector Controller stops.

Stop NSP Flow Collectors

3

Stop each NSP Flow Collector that is not collocated with an NSP Flow Collector Controller.

Note: Any NSP Flow Collector that is collocated with a Flow Collector Controller is automatically stopped earlier in the procedure.

1. Log in to the NSP Flow Collector station as the nsp user.
2. Enter the following:

```
bash$ /opt/nsp/flow/fc/bin/flowCollector.bash stop ↵
```

The NSP Flow Collector stops.

Uninstall software

4

Log in as the root user on a station that has the downloaded and extracted NSP component installer package.

5

Open a console window.

6

Enter the following:

```
# cd path/NSD_NRC_R_r/bin ↵
```

where

path is the directory path of the NSP component installer package

R_r is the NSP software release, in the form *MAJOR_minor*

7

Enter the following:

```
# ./uninstall.sh --ask-pass --target address_1,address_2,...address_n
↵
```

where *address_1, address_2,...address_n* is a comma-separated list of the local NSP Flow Collector Controller and Flow Collector IP addresses

You are prompted for the common root password of the stations.

8

Enter the password.

The NSP software is removed from each station, and the following backup directory is created:

/opt/nsp/backup_flow

Back up configurations

9

Back up the configuration of each NSP Flow Collector Controller and Flow Collector; perform the following steps on each station that hosts an NSP Flow Collector Controller, and on each station that hosts only an NSP Flow Collector.

1. Log in as the root user on the station.
2. Open a console window.
3. Enter the following:

   ```
   # cd /tmp ↵
   ```

4. Enter the following:

   ```
   # tar -czf host_backup_flow /opt/nsp/backup_flow ↵
   ```

   where *host* is a unique station identifier such as the station hostname, or a name that indicates the station role, such as FCC*n* for a Flow Collector Controller, or FCAA*n* for a Flow Collector in AA mode

   A *host*_backup_flow.tar.gz file is created in the /tmp directory.

5. Transfer the /tmp/*host*_backup_flow.tar.gz file to a secure location on a separate station that is not affected by the upgrade activity.

Recommission stations, if required

10

If you are reusing any NSP Flow Collector Controller or Flow Collector station, recommission the station according to the platform specifications in this guide and the *NSP Planning Guide*.

For information about deploying the RHEL OS using an NSP OEM disk image, see 2.2.2 “NSP disk-image deployment” (p. 28).

Note: If you are using RHEL OpenStack VMs, you must re-image each VM using the rebuild option, which preserves the current VM IP addresses, and specify the required new RHEL version.

Start PKI server

11

Start the PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 4.10 “To configure and enable a PKI server” (p. 113).

ℹ **Note:** The PKI server is required for internal system configuration purposes.

Upgrade software

12

Perform the following steps on each new or recommissioned station.

1. Log in as the root user.
2. Open a console window.
3. Transfer the appropriate *host*_backup_flow.tar.gz file created Step 9 to the /tmp directory on the station.
4. Enter the following:

   ```
   # cd /tmp ↵
   ```
5. Enter the following to extract the file content:

   ```
   # tar xvf host_backup_flow.tar.gz ↵
   ```

   The /tmp/backup_flow directory is created, and the configuration files are extracted to the directory.
6. Enter the following:

   ```
   # mv backup_flow /opt/nsp ↵
   ```

13

Download the NSP component installer package (NSP_NSD_NRC_*R_r*.tar.gz) from OLCS and extract it on any station running a supported version of RHEL. This does not have to be the station on which the NSP Flow Collector Controller or an NSP Flow Collector is installed; the installer can perform remote upgrades.

An NSD_NRC_*R_r* directory is created in the current directory, where *R_r* is the release identifier in the form *MAJOR_minor*.

ℹ **Note:** In subsequent steps, the directory is called the NSP installer directory or *NSP_installer_directory*.

14

Log in as the root user on the station that has the downloaded NSP software bundle.

15

Enter the following:

```
# cd NSP_installer_directory/NSD_NRC_R_r/bin ↵
```

16

Create a hosts file in the current directory that contains the required entries in the following sections:

- [nspos]—one entry for each ZooKeeper host; the ZooKeeper hosts are one of the following:
  - if the NSP system includes only the NFM-P, the NFM-P main servers

  - otherwise, the VIP address of each NSP cluster
- [fcc]—one line entry for each Flow Collector Controller
- [fc]—one line entry for each Flow Collector

Note: If an NSP Flow Collector Controller and Flow Collector are to be collocated on one station, specify the same address for in the [fc] and [fcc] sections; for example:

```
[fcc] 203.0.113.3 advertised_address=198.51.100.3 ansible_host=
198.51.100.3
[fc] 203.0.113.3 ansible_host=198.51.100.3 fc_mode=AA
```

See 13.3 “NSP hosts file” (p. 364) for configuration information.

Note: A sample hosts file is in the following directory; you must use a modified copy of the file for installation:

- *NSP_installer_directory*/NSD_NRC_*R_r*/examples
  where *R_r* is the NSP software release

17

Create a config.yml file in the NSP installer directory that includes the following sections; see 13.4 “NSP RPM-based configuration file” (p. 366) for information.

- multi-component deployment:
  - **sso**
  - **tls**
  - section for each component to install
- independent deployment, for example, if you are adding a Flow Collector or Flow Collector Controller to an NFM-P-only system:
  - **sso**
  - **tls**

Note: The following parameter values in the **tls** section must match the values in the NSP configuration file; otherwise, the values must match the values in the NFM-P main server configuration:

- secure
- PKI server parameters
  You can use the samconfig “show” command on a main server to display the **tls** parameters. See 14.9 “NFM-P samconfig utility” (p. 432) for information about using the samconfig utility.

Note: A sample config.yml file is in the following directory; you must use a modified copy of the file for installation:

- *NSP_installer_directory*/NSD_NRC_*R_r*/examples
  where *R_r* is the NSP software release

18

Enter the following:

Note: Include the --ask-pass option only if each target station has the same root user password.

```
# ./install.sh --ask-pass --target target_list ↵
```

where *target_list* is a comma-separated list of the NSP Flow Collector Controller and NSP Flow Collector IP addresses

The NSP Flow Collector Controller or NSP Flow Collector software is upgraded on each station.

Configure NFM-P in DR deployment

19

If the NSP cluster and NSP Flow Collector Controllers are not in a DR deployment, go to Step 25.

20

Log in as the root user on the NFM-P main server in the same data center as the NSP Flow Collector Controller.

21

Open a console window.

22

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.

5. Enter the following to switch back to the root user:

   ```
   bash$ su - ↵
   ```

6. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to display the nspOS service status:

   ```
   # nspdctl status ↵
   ```

   Information like the following is displayed.

```
Mode:     DR
Role:     redundancy_role
DC-Role:  dc_role
DC-Name:  dc_name
Registry: IP_address:port
State:    stopped
Uptime:   0s
SERVICE           STATUS
service_a         inactive
service_b         inactive
service_c         inactive
```

You must not proceed to the next step until all NSP services are stopped; if the State is not ‘stopped’, or the STATUS indicator of each listed service is not ‘inactive’, repeat this substep.

23

You must create an association between the local NSP Flow Controller and the local NFM-P main server to ensure that the Flow Collector and Controller remain in communication with the local NFM-P during NSP DR activity.

Add the local data center name to the main-server configuration.

Note: The data center name must be a name other than “default”.

1. Enter the following:

   ```
   # samconfig -m main ↵
   ```

   The samconfig utility opens, and the following is displayed:

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

2. Enter the following:

   ```
   <main> configure nspos dc-name data_center ↵
   ```

   where *data_center* is the data center name, which must match the dcName value for the local NSP cluster in the NSP configuration file

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

3. Enter the following:

   ```
   <main configure nspos> exit ↵
   ```

   The prompt changes to `<main>`.

4. Enter the following:

   ```
   <main> apply ↵
   ```

   The configuration is applied.

5. Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

24

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.

Start NSP Flow Collector Controllers

25

Perform the following steps on each NSP Flow Collector Controller station.

Note: If an NSP Flow Collector is also installed on the station, the Flow Collector starts automatically.

1. Log in to the station as the nsp user.
2. Enter the following:

   ```
   bash$ /opt/nsp/flow/fcc/bin/flowCollectorController.bash start ↵
   ```

   The NSP Flow Collector Controller starts.

3. Close the console window.

Start NSP Flow Collectors

26

Start each NSP Flow Collector that is not collocated with an NSP Flow Collector Controller.

Note: Any NSP Flow Collector that is collocated with a Flow Collector Controller is automatically started earlier in the procedure.

1. Log in to the NSP Flow Collector station as the nsp user.
2. Enter the following:

```
bash$ /opt/nsp/flow/fc/bin/flowCollector.bash start ↵
```

The NSP Flow Collector starts.

3. Close the console window.

27

Perform the following steps for each NSP Flow Collector.

1. Use a browser to open the web UI at the following URL:

   https://*server*:8443/fc/admin

   where *server* is the NSP Flow Collector IP address or hostname

   The Collection Policy configuration page opens.

2. Verify the settings on each configuration page to ensure that the settings from before the upgrade are preserved.

28

If no other components are to be deployed, stop the PKI server by entering Ctrl+C in the console window.

29

Close the open console windows.

End of steps

NSP analytics server upgrade from Release 22.6 or earlier

15.4 To upgrade Release 22.6 or earlier NSP analytics servers

15.4.1 Purpose

The following steps describe how to upgrade the Release 22.6 or earlier analytics servers in an NSP system.

Note: You cannot selectively upgrade analytics servers; all analytics servers must be upgraded in one operation, as described in the procedure.

Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

Note: Each running NSP analytics server and each running NFM-P auxiliary database in the NSP system must be at the same release.

Note: If you are replacing any analytics server stations, it is recommended that you commission the stations in advance of the upgrade to reduce the upgrade duration.

For information about deploying the RHEL OS using an NSP OEM disk image, see 2.2.2 “NSP disk-image deployment” (p. 28).

Note: After an 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 *NSP Release Notice* for limitations regarding specific reports.

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

15.4.2 Steps

Download installation files

1

Log in as the root user on a station that is reachable from each analytics server station.

2

Open a console window.

3

Download the following NSP installation files to an empty local directory:

- analyticsBackupForMigration.sh
- 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 ID, in the form *MAJOR.minor.patch*

v is a version number

Commission new stations, if required

4

If you are deploying the analytics servers on new stations, commission the stations according to the platform specifications in this guide and in the *NSP Planning Guide*.

Note: The hostname and IP address of a replacement station must match the hostname and IP address of the station being replaced.

For information about deploying the RHEL OS using an NSP OEM disk image, see 2.2.2 “NSP disk-image deployment” (p. 28).

Back up analytics report repository, security files

5

Log in as the root user on any analytics server station in the data center.

6

Transfer the downloaded analyticsBackupForMigration.sh file to the /opt/nsp directory.

7

Enter the following:

```
# chown nsp:nsp /opt/nsp/analyticsBackupForMigration.sh ↵
```

8

Enter the following:

```
# chmod +x /opt/nsp/analyticsBackupForMigration.sh ↵
```

9

Enter the following to switch to the nsp user:

```
#  su - nsp ↵
```

10

Enter the following:

```
bash$ ./analyticsBackupForMigration.sh ↵
```

The server security keys and configuration file are backed up to the following file in the current directory, /opt/nsp:

analyticsBackup.tar.gz

11

Enter the following:

```
bash$ tar -tzf analyticsBackup.tar.gz ↵
```

The backed-up files are listed.

12

Verify that the output matches the following; if any file is not listed, contact technical support:

- opt/nsp/.jrsks
- opt/nsp/.jrsksp
- opt/nsp/analytics/config/install.config
- opt/nsp/analytics/backup/analytics_backup_*version_timestamp*.zip
  where
  version is the current analytics software version
  timestamp is the current timestamp

13

Copy the /opt/nsp/analyticsBackup.tar.gz file to a secure location on a separate station that is not affected by the upgrade activity.

Stop analytics servers

14

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/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
```

Uninstall all analytics servers

15

Perform Step 1 to Step 8 of 19.2 “To uninstall an NSP analytics server” (p. 1076) on each analytics server station.

Recommission stations, if required

16

If you are reusing any analytics server stations, recommission the stations according to the platform specifications in this guide and the *NSP Planning Guide*.

For information about deploying the RHEL OS using an NSP OEM disk image, see 2.2.2 “NSP disk-image deployment” (p. 28).

Start PKI server

17

Start the PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 4.10 “To configure and enable a PKI server” (p. 113).

ℹ **Note:** The PKI server is required for internal system configuration purposes, so must be running before you continue.

ℹ **Note:** All NSP components must use TLS artifacts that are signed by the same root CA. If the NSP or NFM-P to which the analytics server connects is using TLS artifacts from a previous deployment, you must ensure that the private key file and public certificate file from the previous deployment are copied to the PKI server, as described in 4.10 “To configure and enable a PKI server” (p. 113).

18

Perform Step 20 to Step 35 on each analytics server station.

19

Go to Step 36.

Upgrade individual analytics server

20

Log in as the root user on the analytics server station.

21

Open a console window.

22

Transfer the installation files downloaded in Step 3 to an empty temporary directory on the station.

Note: You must ensure that the directory contains only the installation files.

23

Navigate to the directory that contains the installation files.

24

Enter the following:

```
# chmod +x * ↵
```

25

Enter the following:

```
# dnf install *.rpm ↵
```

For each package, the dnf 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
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

27

Perform one of the following.

a. If the analytics server is the first analytics server to be upgraded, perform the following steps.

   1. Copy the /opt/nsp/analyticsBackup.tar.gz saved in Step 13 to the /opt/nsp directory.
   2. Enter the following to switch to the nsp user:

      ```
      # su - nsp ↵
      ```
   3. Enter the following:

      ```
      bash$ cd /opt/nsp/analytics/bin ↵
      ```
   4. Enter the following:

      ```
      bash$ ./preInstallWithBackup.sh /opt/nsp/analyticsBackup.tar.gz ↵
      ```

      The configuration is restored.

b. If the analytics server is not the first analytics server to be upgraded, perform the following steps.

   1. Transfer the following files from the first upgraded analytics server to the /opt/nsp directory on the analytics server that you are currently upgrading:
      - /opt/nsp/.jrsks
      - /opt/nsp/.jrsksp
   2. Enter the following:

      ```
      # chown nsp:nsp /opt/nsp/.jrsks ↵
      ```
   3. Enter the following:

      ```
      # chown nsp:nsp /opt/nsp/.jrsksp ↵
      ```
   4. Enter the following to switch to the nsp user:

      ```
      # su - nsp ↵
      ```

28

Enter the following:

```
bash$ /opt/nsp/analytics/bin/AnalyticsAdmin.sh updateConfig ↵
```

The script displays the following message and prompt:

```
THIS ACTION UPDATES /opt/nsp/analytics/config/install.config
Please type 'YES' to continue
```

29

Enter YES.

The script displays a series of prompts.

30

At each prompt, verify the parameter value; to accept a default in brackets, press ↵.

ℹ **Note:** Accept all previous values unless they have changed.

Table 15-1, "NSP analytics server parameters" (p. 621) lists and describes each parameter.

ℹ **Note:** Ensure that you update each IP address that is changing to a new value.

Table 15-1 NSP analytics server parameters

Parameter	Description
Analytics Server Hostname or IP Address	The analytics server hostname or IP address that is reachable by the NSP cluster and the client browsers Default: —
Enter IP address or hostname for internal network	The analytics server internal IP address, if configured Default: —
Is NSPOS secure	Whether the internal NSP system communication is secured using TLS In a shared-mode NSP system, the value must match the "nspos secure" parameter value; otherwise, the value must match the "secure" value in the nspos section of the NFM-P main server configuration.
Use internal certificates	Whether internal service communication between NSP components is secured using internally generated TLS certificates You can set the parameter to true only if the "Is NSPOS secure" parameter is set to true.
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 • the internalAdvertisedAddress value in the primary or standalone NSP configuration file, if configured; otherwise, the advertisedAddress value
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 • the internalAdvertisedAddress value in the standby NSP configuration file, if configured; otherwise, the advertisedAddress value
Primary Oracle Data Source DB Host	The primary or standalone main database IP address or hostname
Primary Oracle Data Source DB Name	The primary or standalone main database instance name
Primary Oracle Data Source DB Port	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 or hostname

Table 15-1 NSP analytics server parameters (continued)

Parameter	Description
Secondary Oracle Data Source DB Name	In a redundant system, the standby main database instance name
Secondary Oracle Data Source DB Port	In a redundant system, the TCP port on the standby main database station that receives database requests
PKI Server IP Address or Hostname	The PKI server IP address or hostname Regardless of whether you are using the manual or automated TLS configuration method, you must specify the PKI server address.
PKI Server Port	The PKI server port
Zookeeper Connection String	The IP address or hostname, and port of each ZooKeeper host, in the following format: `server1_address:port;server2_address:port` where *server1_address* and *server2_address* are the IP addresses or hostnames of the ZooKeeper hosts *port* is a port number based on the **Is NSPOS secure** setting: • 2181, if false • 2281, if true **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** • **the advertisedAddress of each cluster from the NSP configuration file**
Use NFM-P-only mode? (true/false)	Specifies how the Analytics server communicates with the NSP system The parameter must be set to true if the deployment includes only the NFM-P and has no NSP cluster.

31

If you are upgrading the first analytics server, and either of the following is true, you must purge the Analytics data from the NSP PostgreSQL database, and restore critical files from the backup; otherwise, you can skip this step.

- The software version from which you are upgrading is still installed on one or more analytics servers.

  OR

- One or more analytics servers were still installed when the NSP PostgreSQL database backup was created for the NSP system upgrade.

1. Enter the following:

   ```
   bash$ ./AnalyticsAdmin.sh genCertificate ↵
   ```

   Note: The command may generate the following error message that you can safely ignore:

```
/opt/nsp/analytics/bin/vault.sh: line 46: ./eap-vault-update.sh: No
such file or directory
```

2. Enter the following:

```
bash$ ./AnalyticsAdmin.sh force_uninstall ↵
```

   The NSP PostgreSQL database is purged of analytics-server information.

3. Enter the following:

```
bash$ tar -xzf /opt/nsp/analyticsBackup.tar.gz --directory /opt/nsp
'./.jrsks*' ↵
```

32

Perform one of the following to install the analytics server software on the station.

a. If the analytics server is the first analytics server to be upgraded, enter the following:

```
bash$ /opt/nsp/analytics/bin/AnalyticsAdmin.sh installWithBackup ↵
```

b. If the analytics server is not the first analytics server to be upgraded, enter the following:

```
bash$ /opt/nsp/analytics/bin/AnalyticsAdmin.sh install ↵
```

Note: The analytics server starts automatically after the installation.

The following prompt is displayed if the Use NFM-P-only mode parameter in Step 30 is set to false.

```
Enter NSP user name:
```

33

If the prompt is displayed, perform the following steps.

1. Enter admin ↵.

   The following prompt is displayed:

```
Enter NSP user password (hidden):
```

2. Enter the password of the NSP admin user.

34

The following messages and prompt are displayed:

```
Access token retrieved successfully

date time Analytics App is UP and Running

Version check passed. NSP version = RR.r; Analytics server version =
RR.r

date time Installing Analytics Server...

Do you have existing TLS certificates?(yes/no)
```

35

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 Certificate 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 upgrade proceeds, and messages like the following are displayed:

```
Creating Analytics Repository Schema
Analytics Repository Schema creation is complete
Modified JIRoles Table
Please wait while Analytics Server is being installed...This may take
a few minutes
Restoring backup
Retrieving AUXDB Connection Configurations
AUXDB Connection Configuration successfully retrieved
date time Deploying customization zip file
date time  Analytics server upgrade is complete. Starting analytics
server
date time Starting Analytics Application
Waiting for Analytics Server to come up
date time Analytics Server is UP and Running
Oracle Redundancy Configuration Detected
Analytics Server successfully started
Importing reports for upgrade
Deploying Reports After Upgrade
Start Deploying /opt/nsp/analytics/analytics-report/domains.zip
Tracking nn reports...
Inserted nn reports into Tracker Table
All reports successfully tracked
Start Deploying /opt/nsp/analytics/analytics-report/reports.zip
Tracking nnn reports...
All reports successfully tracked
Waiting for upgrading reports...
Moving resources under Results folder to Shared folder
Updating scheduled jobs
Transferred roles to user
Deleting Analytics resources metadata...
Analytics resources metadata deleted
Updating Analytics resources metadata...
Analytics resources metadata updated
```

```
date time Analytics server upgraded successfully
```

Stop PKI server

36

If no other components are to be deployed, stop the PKI server by entering Ctrl+C in the console window.

37

Close the open console windows.

END OF STEPS

NFM-P system upgrade from Release 22.6 or earlier

15.5 Upgrade requirements

15.5.1 Primary considerations

CAUTION

Service Disruption

An NFM-P system upgrade 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 Planning Guide, and the NSP 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 NSP professional services 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.

CAUTION

Upgrade Failure

A system upgrade fails unless you strictly comply with the upgrade requirements and operate within the upgrade restrictions.

Ensure that you have a thorough understanding of the NFM-P system upgrade requirements and restrictions in “NFM-P deployment configuration” (p. 370) and in the NSP Planning Guide, and that you perform a test upgrade in advance of a live upgrade, as described in 15.5.3 “Staging your upgrade” (p. 630).

This section describes the general conditions that apply to NFM-P system upgrades. Before you attempt to upgrade an NFM-P component, you must comply with the conditions in “NFM-P deployment configuration” (p. 370) and this section.

“NFM-P single-user GUI client upgrade from Release 22.6 or earlier” (p. 782) and “NFM-P client delegate server upgrade from Release 22.6 or earlier” (p. 790) describe how to upgrade an NFM-P single-user GUI client or client delegate server.

Note: It is strongly recommended that you verify the message digest of each NSP image file or software bundle that you download from the Nokia Support portal. The download page includes the MD5, SHA256, and SHA512 checksums for comparison with the output of the RHEL md5sum, sha256sum, or sha512sum command. See the associated RHEL man page for command usage information.

Note: Before a system upgrade, you must ensure that you have sufficient time to complete a main database upgrade. The time required for the upgrade depends on the platform resources, database complexity, and tablespace configuration. Contact technical support to obtain a database upgrade duration estimate.

ℹ **Note:** The following NFM-P main server **aux** parameters remain in the samconfig utility, but are obsolete and not to be configured:

- calltrace
- pcmd
- webdav
- disable-cn-check
- custom-http-headers
- calltrace-pairs
- pcmd-pairs

ℹ **Note:** The following NFM-P auxiliary server **service** parameters remain in the samconfig utility, but are obsolete and not to be configured:

- pcmd
- calltrace

ℹ **Note:** The following NFM-P auxiliary server **tls** parameter remains in the samconfig utility, but is obsolete and not to be configured:

- disable-cn-check

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

Geo-redundant system upgrades

The upgrade of geo-redundant NFM-P sites in a DR NSP deployment is orchestrated using the NSP system upgrade procedures in Chapter 8, “NSP system upgrade from Release 22.6 or earlier”. Consequently, an NFM-P system upgrade is an operation that is independent of the NSP deployment type.

ℹ **Note:** The upgrade procedures include a limited number of conditional workflow or procedure steps for special geo-redundant considerations such as auxiliary database upgrades.

ℹ **Note:** If the main servers in a redundant NFM-P system use different time zones, as in a geo-redundant deployment, and NSP Analytics 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 an event, after both main servers are upgraded you must use the client GUI to change the Analytics aggregation time-zone setting.

See the *NSP Analytics Report Catalog* for aggregation configuration information.

15.5.2 Migration to RHEL 8

An NFM-P system upgrade from Release 22.6 or earlier requires a RHEL OS upgrade, and is essentially a platform migration that involves installing the new NFM-P software on the upgraded platform, rather than directly upgrading the existing software. The migration preserves the existing NFM-P component configurations and database content.

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.

For information about deploying the RHEL OS using an NSP OEM disk image, see 2.2.2 “NSP disk-image deployment” (p. 28).

15.5.3 Staging your upgrade

It is essential that you plan, document, and test an upgrade in advance on a lab system in a closed environment that is representative of the actual network. Contact technical support to assess the system upgrade requirements.

Note: In a large or complex network, it is strongly recommended that you engage the technical support upgrade service.

Performing a test upgrade involves the same preparation and series of actions as a live upgrade; see 15.7 “General NFM-P Release 22.6 or earlier upgrade workflow” (p. 632) for information.

15.5.4 TLS configuration

In 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.

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.

Note: TLS 1.0 and 1.1 are disabled by default. If either version is enabled before an NFM-P system upgrade and required after the upgrade, you must re-enable the version support after the upgrade.

See the *NSP System Administrator Guide* for information about using the tool.

15.5.5 XML API client compatibility

An OSS client must use the samOss.jar from the current NFM-P release. If a different samOss.jar is used, the NFM-P system may become unstable. The NFM-P release information is in the JAR manifest file.

Note: If you intend to use an existing OSS client from a previous NFM-P release, you must review the list of NFM-P schema changes in the *NSP NFM-P XML API Developer Guide* to identify modifications to packages, classes, types, methods, and properties that the OSS client uses.

See the *NSP NFM-P XML API Developer Guide* for information about how to obtain the required samOss.jar file, and how to configure and test a JMS connection.

15.6 NFM-P system upgrade restrictions

15.6.1 Description

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 a main server upgrade, specific NFM-P configuration and log files are copied to a time-stamped directory in the installation directory, and specific directories below the installation directory are deleted.

If you create or modify a file under the main server installation directory, you risk losing the file during an upgrade unless you first back up the file to a location that is unaffected by the upgrade.

CAUTION

Upgrade failure

An NFM-P main server upgrade fails if each main server in the system is not fully initialized and functional before the upgrade.

Before you attempt to upgrade a main server, you must ensure that the initialization of each main server in the NFM-P system is complete.

The following restrictions apply to an NFM-P system 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 21 or 22 NFM-P system to Release 23, but you cannot upgrade a Release 20 system directly to Release 23; you must first perform an intermediate upgrade to at least Release 21.
- After an upgrade to an intermediate release, for example, an upgrade from Release 20 to Release 21 or 22 in preparation for a final upgrade to Release 23, you must allow each main server to initialize fully before the final upgrade, or the upgrade fails.
- A redundant system upgrade requires a network-management outage and must be performed only during a scheduled maintenance period of sufficient duration.

Note: An NFM-P server upgrade applies a default set of file permissions to each directory below the main or auxiliary 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.

15.7 General NFM-P Release 22.6 or earlier upgrade workflow

15.7.1 Description

The following is the sequence of high-level actions required to upgrade an NFM-P system from Release 22.6 or earlier.

Note: The workflow applies to an upgrade in a staging environment or in a live network.

15.7.2 Stages

Pre-upgrade

1

Perform 15.8 “To prepare for an NFM-P system upgrade from Release 22.6 or earlier” (p. 634) to collect the required information and to ensure that the correct upgrade conditions are in place.

2

Perform 15.9 “To prepare an SELinux-enabled Release 22.6 or earlier NFM-P system for an upgrade” (p. 649) to ensure that SELinux is enabled and in permissive mode before the upgrade.

Upgrade

3

Perform one of the following.

a. Upgrade a standalone NFM-P system; see “Standalone NFM-P system upgrade from Release 22.6 or earlier” (p. 651).

b. Upgrade a redundant NFM-P system; see “Redundant NFM-P system upgrade from Release 22.6 or earlier” (p. 686).

Post-upgrade

4

If SELinux was enabled in the NFM-P before the system upgrade, you must re-enable SELinux on each station in the system after the upgrade; perform “How do I enable SELinux on the NFM-P?” in the *NSP System Administrator Guide*.

5

If either of the following is true, perform “How do I enable SELinux enforcing mode for the NFM-P?” in the *NSP System Administrator Guide* to switch from SELinux permissive mode to enforcing mode:

- You have performed 15.9 “To prepare an SELinux-enabled Release 22.6 or earlier NFM-P system for an upgrade” (p. 649) to set SELinux in permissive mode before the upgrade, and want to restore the use of enforcing mode.

- The upgrade has enabled SELinux in the NFM-P for the first time, but in permissive mode, and you want the more stringent security of enforcing mode.

NFM-P Release 22.6 or earlier pre-upgrade procedures

15.8 To prepare for an NFM-P system upgrade from Release 22.6 or earlier

15.8.1 Description

CAUTION

Upgrade failure

An NFM-P system upgrade fails if each main server in the system is not fully initialized and functional before the upgrade.

Before you attempt an NFM-P system upgrade, you must ensure that the initialization of each main server in the NFM-P system is complete.

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

15.8.2 Steps

CAUTION

Deployment failure

The RHEL OS of any NSP component requires specific versions of some RHEL packages. If the required package versions are not installed, the component upgrade fails.

See “Manual NSP RHEL OS installation” (p. 70) 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 Planning Guide*.

Note: The hostname and IP address of each replacement station must match the hostname and IP address of the station being replaced.

For information about deploying the RHEL OS using an NSP OEM disk image, see 2.2.2 “NSP disk-image deployment” (p. 28).

Check component hardware

2

Perform a file system check on each component by entering the following for each file system device as the root user on the component station:

```
# e2fsck -n file_system ↵
```

where *file_system* is a specification such as /dev/sda*n* for a physical disk, or /dev/vda*n* for a virtual disk

If the check passes, the output is similar to the following

```
/dev/sdan: clean, a/b files, x/y blocks
```

If the check indicates a failure, you must correct the disk corruption before you continue.

3

Check each component station for system error messages; enter the following as the root user on the station:

```
# grep -i error /var/log/messages ↵
```

If no error messages are present, the command returns nothing. Otherwise, investigate and resolve the issues indicated by the error messages that are displayed.

4

Perform “How do I test NFM-P disk performance?” in the *NSP System Administrator Guide* on each component station to ensure that the disk speed and latency meet or exceed your system requirements.

Check component OS configuration

5

Verify that the /etc/hosts file contains the required host entry for each NFM-P component; enter the following as the root user on each station, and ensure that each required entry is present and correctly specified, as described in 13.5.3 “Network requirements” (p. 371):

```
# cat /etc/hosts ↵
```

6

Verify that the /etc/nsswitch.conf file is configured correctly; enter the following as the root user on each component station:

```
# cat /etc/nsswitch.conf ↵
```

Ensure that “files” is the first entry for passwd, shadow, group, and hosts, as shown in the following:

```
passwd:      files nis
shadow:      files nis
group:       files nis
hosts:       files dns myhostname
```

7

Verify that the OS version is compatible with the NFM-P release, as described in the *NSP Planning Guide*; enter the following as the root user on each component station:

```
# cat /etc/redhat-release ↵
Red Hat Enterprise Linux Server release R.r (codename)
```

8

Verify that the disk partitions are correctly allocated and sized; enter the following commands as the root user on each component station, and check the output against the specifications in Chapter 2, “NSP disk setup and partitioning”:

```
# lsblk ↵
# df -PH ↵
```

9

Verify that the required RHEL OS packages are installed; enter the following as the root user on each component station; see Chapter 3, “RHEL OS deployment for the NSP” for information about the required packages:

```
# dnf list installed ↵
```

Verify NE resynchronization status

10

Use the Discovery Manager in the NFM-P GUI to ensure that no NEs are undergoing or pending resynchronization.

1. Open an NFM-P GUI client.
2. Choose Administration→Discovery Manager from the NFM-P main menu. The Discovery Manager (Edit) form opens.
3. Click on the Resync Status tab.
4. Ensure that no NEs are in either of the following states:
   - In Progress
   - Requested
5. Close the Discovery Manager form.

Obtain new NFM-P license

11

The migration to RHEL 8 in a system upgrade from Release 22.6 or earlier changes each NFM-P station UUID. Consequently, an upgraded main server cannot recognize the NFM-P license from before the upgrade, and you must request a new licence based on the new main server UUIDs.

Perform the following steps on each main server station.

1. Enter the following as the root user:

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

   The station UUID is displayed.
2. Record the UUID.
3. Unzip the license file; enter the following:

   ```
   # tar -xvf license_file ↵
   ```

   where *license_file* is the path of the compressed license file

   The nfmpLicense.xml file is extracted to the current directory.
4. Open the nfmpLicense.xml file for viewing.
5. Review the license parameters to ensure the following:
   - The license enables the required functions.
   - The licensed capacities are correct and sufficient for you network.
6. Submit your license request to Nokia using the new UUIDs, and the required parameter values.

Back up NFM-P configuration

12

Copy the following configuration files to a secure location on a station that is not affected by the upgrade:

- from each main server station:
  - contents of /opt/nsp/nfmp/server/nms/config
  - /opt/nsp/nfmp/config/nms/config/main_config.xml
- from each auxiliary server station:
  - contents of /opt/nsp/nfmp/auxserver/nms/config
  - /opt/nsp/nfmp/config/nms/config/aux_config.xml
- from each main database station:
  - /opt/nsp/nfmp/samdb/install/config/dbconfig.properties
  - /opt/nsp/nfmp/config/nms/config/db_config.xml

Remove outdated logs

13

An NFM-P main server may retain logs saved during a previous upgrade in the following directory:

/opt/nsp/nfmp/server/nms/log/previous_log

The files in the directory may consume excessive disk space. If the directory exists on a main server, it is strongly recommended that you remove the files from the directory before the upgrade.

a. Move the files to a secure archive location on a station that does not host an NSP component.

b. Delete the files.

Check and configure firewalls

14

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 to Release 22.9 includes 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 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 Planning Guide*, which describes using NFM-P templates for rule creation.

b. Disable each firewall; see the external firewall documentation, or perform 3.19 “To disable the RHEL firewalld service” (p. 91).

Download installation files

15

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
- nsp-nfmp-nodeexporter-*R*.*r*.*p*-rel.*v*.rpm, if the NFM-P is in a shared-mode deployment and you want to forward NFM-P system metrics to the NSP
- 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

16

Before you upgrade a main database, you must ensure that the main database contains only valid records, or the upgrade fails.

i **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.

17

Transfer the following downloaded file to an empty directory on the main database station:

- OracleSw_PreInstall.sh

18

Navigate to the directory that contains the OracleSw_PreInstall.sh file.

19

Enter the following:

```
# chmod +x OracleSw_PreInstall.sh ↵
```

20

Perform the following steps to validate the Oracle database and resolve any conflicts that may prevent an upgrade.

i **Note:** If the validation check reports a small number of errors, for example, a few duplicate and invalid instances of an object, deleting the invalid instances manually may be sufficient. A large number of errors may indicate a significant problem that requires expert attention; in such a case, contact technical support for assistance.

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 21.

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

21

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 22.
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 reinstantiation begins, and the GUI status bar displays reinstantiation information.

Note: Database reinstantiation 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.

7. When the reinstantiation is complete, close the System Information form.

Back up database

22

Open an NFM-P GUI client.

23

Choose Administration→Database from the main menu. The Database Manager form opens.

24

Click on the Backup tab.

25

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 NSP 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.

ℹ **Note:** The backup directory that you specify must be a directory on a local mounted partition.

ℹ **Note:** The Oracle management user requires read and write permissions on the backup directory.

ℹ **Note:** If the NFM-P system is independent, rather than part of a shared-mode NSP deployment, a main database backup performed using the NFM-P client GUI also backs up the local Neo4j and PostgreSQL databases; a backup performed from a CLI does not. The Neo4j and PostgreSQL backup files may be required in the event that the upgrade fails and is to be rolled back.
The Neo4j and PostgreSQL backup files are stored on the standalone or primary main server in the /opt/nsp/os/backup directory.

Configure the following parameters:

- Manual Backup Directory
- Enable Backup File Compression

26

Click Apply.

27

Click Full Backup.

28

Click OK. The database backup begins, and the Backup State indicator reads In Progress.

ℹ **Note:** Depending on the database size, a backup may take considerable time.

29

Monitor the Backup State indicator, which is dynamically updated. The indicator displays Success when the backup is complete.

30

When the backup is complete, close the Database Manager (Edit) form.

31

Transfer the following backup file sets to a secure location on a separate station that is unaffected by the upgrade activity:

- Oracle database—copy from the specified backup location in Step 25 on the standalone or primary main database station
- Neo4j and PostgreSQL databases—copy from the /opt/nsp/os/backup directory on the standalone or primary main server station

Back up main server configuration

32

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:
   ```
   # chmod +x linuxMigration.sh ↵
   ```
6. Enter the following:
   ```
   # ./linuxMigration.sh -t main ↵
   ```
   The following is displayed:
   ```
   Backup NFM-P main config contents.
   ```
   When the backup is complete, the following is displayed:
   ```
   Please backup/transfer /opt/importConfigs/mainserverBackupConfigs.
   tar.gz to a secure location.
   You must restore this file to the exact same directory location on
   the RHEL 8 station before installing the rpm(s).
   ```

33

The script creates the following file on the station:

- /opt/importConfigs/mainserverBackupConfigs.tar.gz

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

34

Perform the following steps on each main server station.

1. Log in as the root user on the main server station.
2. Open a console window.
3. Enter the following:
   ```
   # cd /opt/nsp/nfmp ↵
   ```
4. Enter the following:
   ```
   # tar zcvf `date +%m-%d-%H-%M-%S`.tar.gz lte/ ↵
   ```

5. Enter the following:

```
# tar zcvf `date +%m-%d-%H-%M-%S`.tar.gz nebackup/ ↵
```

6. Enter the following:

```
# tar zcvf `date +%m-%d-%H-%M-%S`.tar.gz nelogs/ ↵
```

   Enter the following:

```
# tar zcvf `date +%m-%d-%H-%M-%S`.tar.gz nesoftware/ ↵
```

7. Enter the following:

```
# tar zcvf `date +%m-%d-%H-%M-%S`.tar.gz os/ ↵
```

8. Enter the following:

```
# tar zcvf `date +%m-%d-%H-%M-%S`.tar.gz
server/script/savedResults/ ↵
```

35

Each command creates a .tar.gz data backup file in the /opt/nsp/nfmp directory. Each file is named using the date and time of file creation.

Transfer the .tar.gz file set to a secure location on a separate station that is unaffected by the upgrade activity.

ℹ **Note:** In a redundant system, you must ensure that you record which main server the file set is from.

Back up custom configuration files

36

⚠ **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.

ℹ **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.

Verify compatibility with external systems

37

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

38

Close the LogViewer utility, if it is open.

Validate main server and GUI client firewall configuration

39

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 Planning Guide* for NFM-P port assignment information.

Verify NFM-P compatibility with managed NEs

40

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 Network Element Compatibility Guide*.

ℹ **Note:** See also 13.5 “NFM-P deployment requirements” (p. 370) for additional important device-specific compatibility requirements.

ℹ **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.

Perform one of the following for each managed NE at an unsupported release.

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, as described in the *NSP NFM-P User Guide*.

   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. If the NE is a pre-provisioned NE, delete the pre-provisioned NE using the NFM-P Pre-Provisioned NE Manager.

Clear CPAM checkpoints

41

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

42

Choose Administration→System Information from the main menu. The System Information form opens.

43

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

44

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

45

If the system includes one or more auxiliary servers, click on the Auxiliary Servers tab; otherwise, go to Step 49.

A list of auxiliary servers is displayed.

46

Perform the following steps for each auxiliary server listed on the form.

1. Select the auxiliary server and click Properties. The Auxiliary Server [Edit] 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 [Edit] form.

47

Click on the Auxiliary Services tab. Each Preferred auxiliary server entry has a check mark in the Selected column.

48

Record the hostname or IP address of each Preferred auxiliary server.

i **Note:** The auxiliary servers are collectively referred to as the [Aux1] auxiliary servers In 15.14 “To upgrade a redundant Release 22.6 or earlier NFM-P system” (p. 694). Any other listed auxiliary servers are the Reserved auxiliary servers, and are collectively referred to as [Aux2] in the procedure.

49

If the system includes one or more client delegate servers, click on the Client Delegate Servers tab. Otherwise, go to Step 51.

50

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.

51

Close the System Information form.

52

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

53

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

54

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.
2. Choose Administration→Security→NFM-P User Security from the main menu. The NFM-P User Security - Security Management (Edit) form opens.
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.
10. Close the NFM-P User Security - Security Management (Edit) form.

Uninstall Mac OS X clients

55

Uninstall each single-user client installed on Mac OS X.

ℹ **Note:** You must use the uninstallation procedure in the documentation for the installed client release, and not the uninstallation procedure in this guide.

Close GUI client

56

If the GUI client that you are using is not required for network monitoring during the upgrade, close the client.

END OF STEPS

15.9 To prepare an SELinux-enabled Release 22.6 or earlier NFM-P system for an upgrade

15.9.1 Purpose

Perform this procedure if:

- You are about to upgrade an NFM-P system.

AND

- SELinux has been enabled in the NFM-P system as described in “How do I enable SELinux on the NFM-P?” in the *NSP System Administrator Guide*.

In order to upgrade an NFM-P system in which SELinux is enabled before the upgrade, the following conditions must be true during the upgrade; performing this procedure ensures that the conditions are met.

- SELinux remains enabled in the system.
- SELinux is in permissive mode.

See “What is SELinux?” in the *NSP System Administrator Guide* for information about configuring SELinux.

ℹ **Note:** You require the following user privileges:

- on each main and auxiliary server station — 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

15.9.2 Steps

1

As the root user, enter the following on each main server, main database, and auxiliary server station to verify that SELinux is enabled:

```
# sestatus ↵
```

SELinux is enabled if the following is displayed:

```
SELinux status: enabled
```

2

Perform one of the following:

a. If SELinux is not enabled, perform “How do I enable SELinux on the NFM-P?” in the *NSP System Administrator Guide*.

b. Enter the following as the root user on each main server, main database, and auxiliary server station to switch to SELinux permissive mode:

i **Note:** You do not need to stop any NFM-P processes in order to switch from enforcing mode to permissive mode.

```
# /opt/nsp/nfmp/config/selinux/tools/bin/selinuxenable.sh -p ↵
```

3

Enter the following as the root user on each main server, main database, and auxiliary server station to verify that SELinux is enabled in permissive mode:

```
# getenforce ↵
```

SELinux is in permissive mode if the following is displayed:

```
Permissive
```

4

Close the open console windows.

END OF STEPS

Standalone NFM-P system upgrade from Release 22.6 or earlier

15.10 Workflow to upgrade a standalone Release 22.6 or earlier NFM-P system

15.10.1 Description

The following is the sequence of high-level actions required to upgrade a standalone Release 22.6 or earlier NFM-P system.

15.10.2 Stages

Note: The "Upgrade standalone system" (p. 651) links lead to sections in 15.11 "To upgrade a standalone Release 22.6 or earlier NFM-P system" (p. 654).

Prepare system for upgrade

1

Perform 15.8 "To prepare for an NFM-P system upgrade from Release 22.6 or earlier" (p. 634).

Upgrade standalone system

2

Check the available disk space; see "Check pre-upgrade disk space" (p. 654).

3

Open a GUI client for network monitoring; see "Open GUI client" (p. 655).

4

If the system includes one or more NSP analytics servers or Flow Collectors, stop each; see "Stop NSP analytics servers, Flow Collectors" (p. 655).

5

Prepare the main server for the upgrade; see "Stop and disable standalone main server" (p. 656).

1. Stop the main server.
2. Disable automatic main server startup.

6

Upgrade the main database; see "Upgrade standalone main database" (p. 657).

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.

7

If the system includes one or more auxiliary servers, stop the auxiliary servers; see “Stop auxiliary servers” (p. 666).

8

Upgrade the main server; see “Upgrade standalone main server” (p. 667).

9

Start the PKI server; see “Start PKI server” (p. 668).

10

Configure the main server; see “Configure standalone main server” (p. 668).

11

If the NFM-P is not in a shared-mode NSP deployment, restore the local NSP databases; see “Restore embedded nspOS, independent deployment” (p. 670).

12

If required, enable Windows Active Directory for client access; see “Enable Windows Active Directory access” (p. 673).

13

If required, configure ADFS to enable Common Access Card, or CAC, client access; see “Enable CAC access” (p. 675).

14

If the NFM-P is integrated with an WS-NOC system, configure the integration; see “Configure WS-NOC integration” (p. 678).

15

If the system includes one or more auxiliary servers, upgrade each auxiliary server; see “Upgrade auxiliary servers” (p. 679).

16

If the system includes one or more NSP Flow Collectors, upgrade each NSP Flow Collector Controller and Flow Collector; see “Upgrade NSP Flow Collector Controllers, Flow Collectors” (p. 679).

17

If the system includes an auxiliary database, upgrade the auxiliary database; see "Upgrade auxiliary database" (p. 679).

18

If the system includes one or more auxiliary servers, start each auxiliary server; see "Start auxiliary servers" (p. 680).

19

Restore the main server data files; see "Restore standalone main server data files" (p. 680).

20

Start the main server; see "Start main server" (p. 681).

21

Recheck the available disk space; see "Check post-upgrade disk space" (p. 683).

22

If the system includes one or more NSP analytics servers, upgrade each analytics server; see "Upgrade NSP analytics servers" (p. 683).

23

Install or upgrade single-user GUI clients, as required; see "Install or upgrade single-user GUI clients" (p. 683).

24

Install or upgrade client delegate servers, as required; see "Install or upgrade client delegate servers" (p. 684).

25

Stop the PKI server; see "Stop PKI server" (p. 684).

26

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. 684).

27

Configure and enable firewalls, if required; see "Configure and enable firewalls" (p. 684).

15.11 To upgrade a standalone Release 22.6 or earlier NFM-P system

15.11.1 Description

The following steps describe how to upgrade a collocated or distributed main database and main server in a standalone deployment at Release 22.6 or earlier. 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

15.11.2 Steps

Check pre-upgrade disk space

1

As part of the trial upgrade on a lab system in advance of a live upgrade, you must ensure that the available disk capacity on each NFM-P component remains within tolerance.

Note: If the disk usage on an NFM-P partition approaches or exceeds 80% after the trial upgrade, you may need to add disk capacity before you attempt the upgrade on a live system.

Perform the following steps on each of the following stations:

- main server
- auxiliary server
- main database
- auxiliary database

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following:

   ```
   # df -kh ↵
   ```

   The usage information for each partition is displayed.
4. Record the information for each NFM-P partition; see the tables in Chapter 2, “NSP disk setup and partitioning” for the partition names and required capacities.

Open GUI client

2

Open at least one GUI client to monitor the network before the upgrade.

Stop NSP analytics servers, Flow Collectors

3

If the system includes one or more NSP 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/analytics/bin/AnalyticsAdmin.sh stop ↵
```

The following is displayed:

```
Stopping Analytics Application
```

When the analytics server is completely stopped, the following message is displayed:

```
Analytics Application is not running
```

4

If the system includes one or more NSP Flow Collector Controllers and Flow Collectors, stop each NSP Flow Collector Controller.

ℹ **Note:** If the NSP Flow Collector Controller is collocated on a station with an NSP Flow Collector, stopping the NSP Flow Collector Controller also stops the Flow Collector.

1. Log in to the NSP Flow Collector Controller station as the nsp user.
2. Open a console window.
3. Enter the following:

   ```
   bash$ /opt/nsp/flow/fcc/bin/flowCollectorController.bash stop ↵
   ```

   The NSP Flow Collector Controller stops.

5

If the system includes one or more NSP Flow Collectors that are not collocated on a station with a Flow Collector Controller, stop each such NSP Flow Collector.

1. Log in to the NSP Flow Collector station as the nsp user.
2. Open a console window.
3. Enter the following:

   ```
   bash$ /opt/nsp/flow/fc/bin/flowCollector.bash stop ↵
   ```

   The NSP Flow Collector stops.

Stop and disable standalone main server

6

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.
6. Enter the following to switch to the root user:

   ```
   bash$ su ↵
   ```
7. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to display the nspOS service status:

   ```
   # nspdctl status ↵
   ```

   Information like the following is displayed.

   ```
   Mode:      active
   Role:      leader
   DC-Role:   dc_role
   DC-Name:   dc_name
   Registry:  IP_address:port
   State:     stopped
   Uptime:    0s
   SERVICE            STATUS
   service_a          inactive
   service_b          inactive
   service_c          inactive
   ```

   You must not proceed to the next step until all NSP services are stopped; if the State is not ‘stopped’, or the STATUS indicator of each listed service is not ‘inactive’, repeat this substep.

7

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:

   ```
   # systemctl disable nspos-nspd.service ↵
   ```

2. Enter the following:

   ```
   # systemctl disable nfmp-main-config.service ↵
   ```

3. Enter the following:

   ```
   # systemctl disable nfmp-main.service ↵
   ```

Upgrade standalone main database

8

Log in to the database station as the root user.

9

Open a console window.

10

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 ↵
   ```

11

Perform the following steps.

1. Open the /etc/fstab file using a plain-text editor such as vi.
2. Locate the tmpfs file system entry.
3. Remove the noexec option so that the entry reads as follows:

   ```
   tmpfs /dev/shm tmpfs nodev 0 0
   ```

4. Save and close the /etc/fstab file.
5. Enter the following to remount the /dev/shm partition:

   ```
   # mount -o remount /dev/shm ↵
   ```

12

If you are re-using the main database station, recommission the station according to the platform specifications in this guide and in the *NSP Planning Guide*.

For information about deploying the RHEL OS using an NSP OEM disk image, see 2.2.2 “NSP disk-image deployment” (p. 28).

13

Log in as the root user on the station that is commissioned as the main database station.

14

Perform one of the following.

a. If the main server and database are collocated on one station, perform the following steps.

1. Enter the following:

   ```
   # mkdir /opt/importConfigs ↵
   ```

2. Transfer the mainserverBackupConfigs.tar.gz file created in Step 32 of 15.8 “To prepare for an NFM-P system upgrade from Release 22.6 or earlier” (p. 634) to the /opt/importConfigs directory.

3. Transfer the following downloaded installation files to an empty directory on the collocated 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.

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
- nsp-nfmp-nodeexporter-*R.r.p*-rel.*v*.rpm, if downloaded

Note: In subsequent steps, the directory is called the NFM-P software directory.

15

Transfer the following downloaded file to an empty directory on the main database station:

- OracleSw_PreInstall.sh

16

Navigate to the directory that contains the OracleSw_PreInstall.sh file.

17

Enter the following:

```
# chmod +x OracleSw_PreInstall.sh ↵
```

18

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]:
```

19

Enter Yes. The following prompt is displayed:

```
Enter the Oracle dba group name [group]:
```

20

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:
```

21

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/oracle19].

Checking or Creating the Oracle user home directory
/opt/nsp/nfmp/oracle19...

Checking user username...

Adding username...

Changing ownership of the directory /opt/nsp/nfmp/oracle19 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:
```

22

Enter a password. The following prompt is displayed:

```
Re-enter new Password:
```

23

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]:
```

24

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.
```

25

When the script execution is complete, enter the following to reboot the station:

```
# systemctl reboot ↵
```

The station reboots.

26

When the reboot is complete, log in as the root user on the main database station.

27

Open a console window.

28

Navigate to the NFM-P software directory.

Note: Ensure that the directory contains only the installation files.

29

Enter the following:

```
# chmod +x * ↵
```

30

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

31

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

32

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/nsp/nfmp/dbbackup/backupset_1
```

Note: Ensure that the Oracle management user has full access to the directory and contents.

33

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 .....
<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
```

34

Stop 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 stop the main database:

   ```
   # systemctl stop nfmp-main-db.service ↵
   ```

35

You must prepare the restored database for the upgrade.

Navigate to the directory that contains the OracleSw_PreInstall.sh file.

36

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]:
```

37

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 NFM-P database version = version

Enter the password for the "SYS" Oracle user (terminal echo is off):
```

38

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/oracle19...

Checking user username...
```

```
usermod: no changes
Changing ownership of the directory /opt/nsp/nfmp/oracle19 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]:
```

39

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; otherwise, go to Step 40:

```
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 36.

40

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]:
```

41

Enter Yes or No, as required.

Messages like the following are displayed as the script execution completes:

```
INFO: Upgrade of a migrated database detected
INFO: No change to /etc/sysctl.d/97-nfmp-oracle.conf, no need to
apply.
INFO: Removing ulimit file /etc/security/limits.d/97-nfmp-oracle.conf
INFO: About to set ulimit parameters in /etc/security/limits.
d/97-nfmp-oracle.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.
d/97-nfmp-oracle.conf...
INFO: Completed running Oracle Pre-Install Tasks
```

42

Enter the following to upgrade the database:

Note: A database upgrade takes considerable time that varies, depending on the release from which you are upgrading.

```
# samupgradeDb ↵
```

The following prompt is displayed:

```
Enter the password for the "SAMUSER" database user (terminal echo is
off):
```

43

Enter the password.

Messages like the following are displayed as the database upgrade begins:

```
Validating...
Validation succeeded.
Upgrade log is /opt/nsp/nfmp/db/install/NFM-P_Main_Database.upgrade.
timestamp.stdout.txt
timestamp working..
timestamp Performing Step 1 of n - Initializing ...
.
```

```
.
.
timestamp Performing Step n of n - Finalizing ...
timestamp Database upgrade was successful
```

The database upgrade is complete when the following is displayed:

```
DONE
```

44

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; see 14.9 “NFM-P samconfig utility” (p. 432) for information about using samconfig.
4. Configure one or more parameters, if required, and then enter **back** ↵.
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.

45

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 the *NSP System Administrator Guide* for information.

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

46

If the system includes one or more auxiliary servers, stop 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 auxstop ↵
```

   The auxiliary server stops.

Upgrade standalone main server

47

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 Planning Guide*.

For information about deploying the RHEL OS using an NSP OEM disk image, see 2.2.2 “NSP disk-image deployment” (p. 28).

48

Log in as the root user on the station that is commissioned as the main server station.

49

Open a console window.

50

If the main server and database are on separate stations, perform the following steps:

1. Enter the following:

```
# mkdir /opt/importConfigs ↵
```

2. Transfer the mainserverBackupConfigs.tar.gz file created in Step 32 of 15.8 “To prepare for an NFM-P system upgrade from Release 22.6 or earlier” (p. 634) to the /opt/importConfigs directory.

51

Perform one of the following.

a. If the main server and database are collocated on one station, go to Step 57.

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
- nsp-nfmp-nodeexporter-*R.r.p*-rel.*v*.rpm, if downloaded

Note: In subsequent steps, the directory is called the NFM-P software directory.

52

Navigate to the NFM-P software directory.

Note: Ensure that the directory contains only the installation files.

53

Enter the following:

```
# chmod +x * ↵
```

54

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

55

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

Start PKI server

56

Start the PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 4.10 “To configure and enable a PKI server” (p. 113).

Note: The PKI server is required for internal system configuration purposes.

Configure standalone main server

57

Enter the following; see 14.9 “NFM-P samconfig utility” (p. 432) for information about using samconfig:

ℹ **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>
```

58

Enter the following:

```
<main> configure ↵
```

The prompt changes to `<main configure>`.

59

To apply a new or updated NFM-P license, enter the following:

ℹ **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 the *NSP System Administrator Guide*.

```
<main configure> license license_file back ↵
```

where *license_file* is the absolute path and file name of the NSP license bundle

60

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; see 14.9 “NFM-P samconfig utility” (p. 432) for information about using the samconfig utility.

3. Configure one or more parameters, if required.

   Note: The NFM-P uses the database backup settings to initialize the database during installation only. To change the backup settings after installation, you must use the Database Manager form in the NFM-P client GUI, as described in the *NSP System Administrator Guide*.

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

   ```
   <main configure> back ↵
   ```

   The prompt changes to `<main>`.

61

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

62

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

63

If the NFM-P is part of a shared-mode NSP system and you want to enable mTLS for internal Kafka authentication using two-way TLS, perform the following steps.

i **Note:** Enabling mTLS for internal Kafka authentication is supported only in an NSP deployment that uses separate interfaces for internal and client communication.

i **Note:** The parameter you must configure is displayed only if the ip-list parameter is set to a remote address.

i **Note:** The parameter is configurable only if the **secure** and **internal-certs** parameters in the **nspos** section are set to true.

1. Enter the following:

   ```
   # samconfig -m main ↵
   ```

   The following is displayed:

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

2. Enter the following:

   ```
   # configure nspos mtls-kafka-enabled back ↵
   ```

3. Enter the following:

   ```
   <main> apply ↵
   ```

   The configuration is applied.

4. Enter the following:

   ```
   <main> exit ↵
   ```

   The samconfig utility closes.

Restore embedded nspOS, independent deployment

64

In an independent NFM-P deployment, you must restore the embedded Neo4j and PostgreSQL databases. Otherwise, if the NFM-P is integrated with an NSP cluster, go to Step 70.

65

Enter the following:

```
# mkdir /opt/nsp/os/backup ↵
```

66

Enter the following:

```
# chown nsp:nsp /opt/nsp/os/backup ↵
```

67

Copy the Neo4j and PostgreSQL backup files saved in Step 31 of 15.8 “To prepare for an NFM-P system upgrade from Release 22.6 or earlier” (p. 634) to the /opt/nsp/os/backup directory.

68

Restore the Neo4j database.

1. Enter the following:

   ```
   # cd /opt/nsp/os/install/tools/database ↵
   ```

2. Enter the following:

   ```
   # ./db-restore.sh --target IP_address ↵
   ```

   where *IP_address* is the main server IP address

   The following message and prompt are displayed:

   ```
   Verifying prerequisites...
   Starting database restore ...
   Backupset file to restore (.tar.gz format):
   ```

3. Enter the following and press ↵:

   ```
   path/nspos-neo4j_backup_timestamp.tar.gz
   ```

   where

   path is the absolute path of the Neo4j backup file

   timestamp is the backup creation time

   Note: Neo4j backup files are stored in the following locations on a main server, depending on the backup type:

   - scheduled backup—/opt/nsp/os/backup/backupset_*n*
   - manual backup—/opt/nsp/os/backup/manual_*timestamp*

   The following messages and prompt are displayed:

   ```
   PLAY [all] **************************************************
   TASK [dbrestore : Create temporary directory] ***************
   changed: [server_IP]
   [dbrestore : pause]
   Do you want to restore the nspOS Neo4j db from file:
   path/nspos-neo4j_backup_timestamp.tar.gz? Press return to continue,
   or Ctrl+C to abort:
   ```

4. Press ↵.

   The restore operation begins, and messages like the following are displayed:

```
TASK [dbrestore : Copy backupset] ***************************
changed: [server_IP]
TASK [dbrestore : Running nspdctl stop] *********************
changed: [server_IP]
TASK [dbrestore : Ensure database service is stopped] *******
changed: [server_IP]
TASK [dbrestore : Perform database restore] *****************
changed: [server_IP]
TASK [dbrestore : Delete temporary directory] ***************
changed: [server_IP]
PLAY RECAP **************************************************
server_IP     : ok=n   changed=n    unreachable=n   failed=n
```

5. If the `failed` value is greater than zero, a restore failure has occurred; contact technical support for assistance.

69

Restore the PostgreSQL database.

1. Enter the following:

   ```
   # ./db-restore.sh --target IP_address ↵
   ```

   where *IP_address* is the main server IP address

   The following message and prompt are displayed:

   ```
   Verifying prerequisites...
   Starting database restore ...
   Backupset file to restore (.tar.gz format):
   ```

2. Enter the following and press ↵:

   ```
   path/nspos-postgresql_backup_timestamp.tar.gz
   ```

   where

   path is the absolute path of the PostgreSQL backup file

   timestamp is the backup creation time

   Note: PostgreSQL backup files are stored in the following locations on a main server, depending on the backup type:

   - scheduled backup—/opt/nsp/os/backup/backupset_*n*
   - manual backup—/opt/nsp/os/backup/manual_*timestamp*

   The following messages and prompt are displayed:

   ```
   PLAY [all] **************************************************
   [dbrestore : pause]
   Do you want to restore the nspOS PostgreSQL db from file:
   path/nspos-postgresql_backup_timestamp.tar.gz? Press return to
   continue, or Ctrl+C to abort:
   ```

3. Press ↲.

   The restore operation begins, and messages like the following are displayed:

   ```
   TASK [dbrestore : Running nspdctl stop] *********************
   changed: [server_IP]
   TASK [dbrestore : Perform database restore] *****************
   changed: [server_IP]
   TASK [dbrestore : Delete temporary directory] ***************
   changed: [server_IP]
   PLAY RECAP **************************************************
   server_IP     : ok=n   changed=n    unreachable=n   failed=n
   ```

4. If the `failed` value is greater than zero, a restore failure has occurred; contact technical support for assistance.

Enable Windows Active Directory access

70

If you intend to use Windows Active Directory, or AD, for single-sign-on client access, you must configure LDAP remote authentication for AD; otherwise, go to Step 89.

Open the following file as a reference for use in subsequent steps:

/opt/nsp/os/install/examples/config.yml

Note: Consider the following.

- The NFM-P does not assign a default user group to users of a remote authentication source that you define for Windows AD; the authentication source must provide the user group attributes.
- Windows AD supports the following LDAP server types for remote authentication:

  AD—The user group of an AD user is derived from the group_base_dn attribute in the server configuration; group search filters are not supported.

  AUTHENTICATED—The server configuration must include bind credentials; group search filters are supported. After NFM-P initialization, you add the AD server bind credentials to the NSP password vault using the NSP Session Manager REST API.

71

Locate the section that begins with the following lines:

```
#   ldap:
#     enabled: true
#     servers:
#       - type: AUTHENTICATED/AD/ANONYMOUS
#         url: ldaps://ldap.example.com:636
#         security: SSL/STARTTLS/NONE
```

72

Open the following file using a plain-text editor such as vi:

/opt/nsp/os/install/config.json

73

Locate the section that begins with the following line:

```
"sso": {
```

The section has one subsection for each type of SSO access.

Note: You can enable multiple remote authentication methods such as LDAP and RADIUS in the config.json file, or by using the NFM-P GUI. Using the GUI also allows you to specify the order in which the methods are tried during login attempts; however, no ordering is applied to multiple methods enabled in the config.json file.

74

In the **sso** section, create an **ldap** subsection as shown below using the parameter names from the **ldap** section of config.yml and the required values for your configuration.

The following example shows the LDAP configuration for two AD servers:

```
"ldap": {
"enabled": true,
"servers": [
{
"type": "auth_type",
"url": "ldaps://server1:port",
"server1_parameter_1": "value",
"server1_parameter_2": "value",
.
.
"server1_parameter_n": "value",
},
{
"type": "auth_type",
"url": "ldaps://server2:port",
"server2_parameter_1": "value",
"server2_parameter_2": "value",
.
.
"server2_parameter_n": "value",
},
}]
}
```

where *auth_type* is AD or AUTHENTICATED

75

Save and close the files.

76

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

77

Enter the following:

```
<main> apply ↵
```

The AD LDAP configuration is applied.

78

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Enable CAC access

79

If you do not intend to enable Common Access Card, or CAC, technology for NFM-P client access, go to Step 89.

80

Download the federationmetadata.xml from the following ADFS link:

https://*ADFS_server_name*/FederationMetadata/2007-06/federationmetadata.xml

where *ADFS_server_name* is the ADFS server FQDN

81

Add an ADFS server entry to the /etc/hosts file on the main server.

1. Open the /etc/hosts file using a plain-text editor such as vi.
2. Add the following line below the line that contains the main server IP address:

   ```
   IP_address FQDN
   ```

   where

   IP_address is the IP address of the ADFS server

   FQDN is the FQDN of the ADFS server
3. Save and close the file.

82

In order to enable CAC for client access, you must configure Active Directory Federation Services, or ADFS.

Open the following file using a plain-text editor such as vi:

/opt/nsp/os/install/config.json

83

In the **sso** section, create an **saml2** subsection as shown below using the parameter names from the **saml2** section of config.yml and the required values for your configuration.

The following example shows the ADFS configuration.

Note: You must preserve the lead spacing of each line.

```
  "sso" : {
    "saml2": {
       "enabled": true,
       "service_provider_entity_id": "NFM-P_identifier",
       "service_provider_metadata_filename": "casmetadata.xml",
       "maximum_authentication_lifetime": 3600,
       "accepted_skew": 300,
       "destination_binding": "urn:oasis:names:tc:SAML:2.0:bindings:
HTTP-Redirect",
       "identity_provider_metadata_path": "ADFS_metadata_file",
       "authn_context_class_ref": "urn:oasis:names:tc:SAML:2.0:ac:
classes:TLSClient",
       "authn_context_comparison_type": "minimum",
       "name_id_policy_format": "urn:oasis:names:tc:SAML:1.1:
nameid-format:unspecified",
       "force_auth": true,
       "passive": false,
       "wants_assertions_signed": false,
       "wants_responses_signed": false,
       "all_signature_validation_disabled": false,
       "sign_service_provider_metadata": false,
       "principal_id_attribute": "UPN",
       "use_name_qualifier": false,
       "provider_name": "ADFS_server_URI",
       "requested_attributes": [{
         "name": "http://schemas.xmlsoap.
org/ws/2005/05/identity/claims/emailaddress",
          "friendly_name": "E-Mail Address",
          "name_format": "urn:oasis:names:tc:SAML:2.0:attrname-format:
uri",
          "required": false
      } ],
       "mapped_attributes": [{
           "name": "http://schemas.xmlsoap.org/claims/Group",
           "mapped_to": "authorizationProfile"
      }, {
           "name": "http://schemas.xmlsoap.
org/ws/2005/05/identity/claims/upn",
           "mapped_to": "upn"
      } ]
    },
```

84

Configure the following parameters; leave all other parameters at the default:

- "service_provider_entity_id": "*NFM-P_identifier*"
- "identity_provider_metadata_path": "*ADFS_metadata_file*"
- "provider_name": "*ADFS_server_name*"

NFM-P_identifier is the unique ADFS Relying Trust Party identifier

*ADFS_metadata_fil*e is the absolute path of the ADFS metadata XML file, for example, /opt/federationmetadata.xml

ADFS_server_name is the ADFS server FQDN

85

Save and close the files.

86

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

87

Enter the following:

```
<main> apply ↵
```

The ADFS configuration is applied.

88

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Configure WS-NOC integration

89

If the NFM-P is integrated with a WS-NOC system, open the following file with a plain-text editor such as vi; otherwise, go to Step 99.

/opt/nsp/os/install/examples/config.json

See “WS-NOC and NSP integration” (p. 340) for comprehensive information about NFM-P integration with the WS-NOC.

90

Copy the following section:

```
  "nfmt": {
    "primary_ip": "",
    "standby_ip": "",
    "username": "",
    "password": "",
    "cert_provided": false
  },
```

91

Close the file.

92

Open the following file with a plain-text editor such as vi:

/opt/nsp/os/install/config.json

93

Paste in the copied section.

94

Configure the required parameters to enable the WS-NOC integration:

- primary_ip—the primary WS-NOC server IP address
- standby_ip—the standby WS-NOC server IP address
- username—the username required for WS-NOC access
- password—the password required for WS-NOC access

- cert_provided—whether a TLS certificate is used

95

Save and close the file.

96

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

97

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

98

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Upgrade auxiliary servers

99

If the system includes one or more auxiliary servers, perform 15.15 “To upgrade a Release 22.6 or earlier NFM-P auxiliary server” (p. 760) on each auxiliary server station.

Upgrade NSP Flow Collector Controllers, Flow Collectors

100

If the system includes one or more NSP Flow Collectors, upgrade each NSP Flow Collector Controller and Flow Collector as described in “NSP Flow Collector and Flow Collector Controller upgrade from Release 22.6 or earlier” (p. 607).

Upgrade auxiliary database

101

If the system includes an auxiliary database, perform 15.16 “To upgrade a Release 22.6 or earlier auxiliary database cluster” (p. 767).

Start auxiliary servers

102

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.

Restore standalone main server data files

103

Transfer the main server data backup .tar.gz file set created in Step 34 of 15.8 “To prepare for an NFM-P system upgrade from Release 22.6 or earlier” (p. 634) to the /opt/nsp/nfmp directory on the main server station.

104

Enter the following:

```
# cd /opt/nsp/nfmp ↵
```

105

Enter the following:

```
# chown nsp:nsp *.tar.gz ↵
```

106

Enter the following:

```
# ls *.tar.gz ↵
```

The data backup files are listed.

107

For each listed file, enter the following:

```
# tar -xf filename.tar.gz -C /opt/nsp/nfmp/ ↵
```

where *filename* is a backup timestamp in the format MM-DD-hh-mm

108

Enter the following:

```
# rm -f *.tar.gz ↵
```

109

Enter the following:

```
# chown -R nsp:nsp /opt/nsp/nfmp/lte ↵
```

110

Enter the following:

```
# chown -R nsp:nsp /opt/nsp/nfmp/nebackup ↵
```

111

Enter the following:

```
# chown -R nsp:nsp /opt/nsp/nfmp/nelogs ↵
```

112

Enter the following:

```
# chown -R nsp:nsp /opt/nsp/nfmp/nesoftware ↵
```

113

Enter the following:

```
# chown -R nsp:nsp /opt/nsp/nfmp/os ↵
```

114

Enter the following:

```
# chown -R nsp:nsp /opt/nsp/nfmp/server/script/savedResults ↵
```

Start main server

115

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 the *NSP 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.

116

If you have enabled CAC for NFM-P client access, download the casmetadata.xml file from the following URL, and then import the file into the ADFS server relying-trust-party:

https://*server*/cas/sp/metadata

where *server* is the main server IP address or hostname

After the download, the casmetadata.xml file is available in the following directory on the main server:

/opt/nsp/os/tomcat/conf/cas/saml

117

If you have enabled Windows Active Directory access using the AUTHENTICATED type of LDAP server, perform the following steps.

1. Use the NSP Session Manager REST API to add the LDAP server bind credentials; see the Network Developer Portal for information.
2. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to restart the local nspos-tomcat service:

   Note: The service restart may take a few minutes, during which NFM-P GUI and REST client access is degraded. General NFM-P operation is unaffected.

```
# systemctl restart nspos-tomcat ↵
```

118

Specify the memory requirement for GUI clients based on the type of network that the NFM-P is to manage.

1. Enter the following:

```
bash$ ./nmsdeploytool.bash clientmem -option ↵
```

where *option* is one of the following:

- m—medium, for management of limited-scale network
- l—large, for a network of 15 000 or more NEs

2. Record the setting, which is not preserved through an upgrade, for future use.
3. Enter the following to commit the configuration change:

```
bash$ ./nmsdeploytool.bash deploy ↵
```

119

Close the console window.

Check post-upgrade disk space

120

If you are performing a trial upgrade on a lab system in advance of a live upgrade, you must check the available capacity of the disk partitions on each component against the values recorded in Step 1.

Perform the following steps on each of the following stations:

- main server
- auxiliary server
- main database
- auxiliary database

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following:

   ```
   # df -kh ↵
   ```

   The usage information for each partition is displayed.
4. Record the information for each NFM-P partition; see the tables in Chapter 2, “NSP disk setup and partitioning” for the partition names and required capacities.
5. Compare the partition values with the values recorded in Step 1.
6. If the disk usage on an NFM-P partition approaches 80% or has increased substantially, you may need to add disk capacity before you attempt the upgrade on a live system. Contact technical support for assistance.

Upgrade NSP analytics servers

121

If the system includes one or more NSP analytics servers, upgrade each analytics server as described in “NSP analytics server upgrade from Release 22.6 or earlier” (p. 616).

Install or upgrade single-user GUI clients

122

As required, install or upgrade additional single-user GUI clients; see the following for information:

- “NFM-P single-user GUI client installation” (p. 585)
- “NFM-P single-user GUI client upgrade from Release 22.6 or earlier” (p. 782)

Install or upgrade client delegate servers

123

As required, install or upgrade client delegate servers; see the following for information:

- “NFM-P client delegate server installation” (p. 591)
- “NFM-P client delegate server upgrade from Release 22.6 or earlier” (p. 790)

Stop PKI server

124

If no other components are to be deployed, stop the PKI server by entering Ctrl+C in the console window.

Restore TLS version and cipher support configuration

125

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, see the *NSP System Administrator Guide* for information about how to restore the TLS version and cipher support settings.

Note: TLS 1.0 and 1.1 are disabled by default after an upgrade. If either version is enabled before an NFM-P system upgrade and required after the upgrade, you must re-enable the version support after the upgrade.

Configure and enable firewalls

126

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 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 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 upgrade from Release 22.6 or earlier

15.12 Component references

15.12.1 Description

CAUTION

Service Disruption

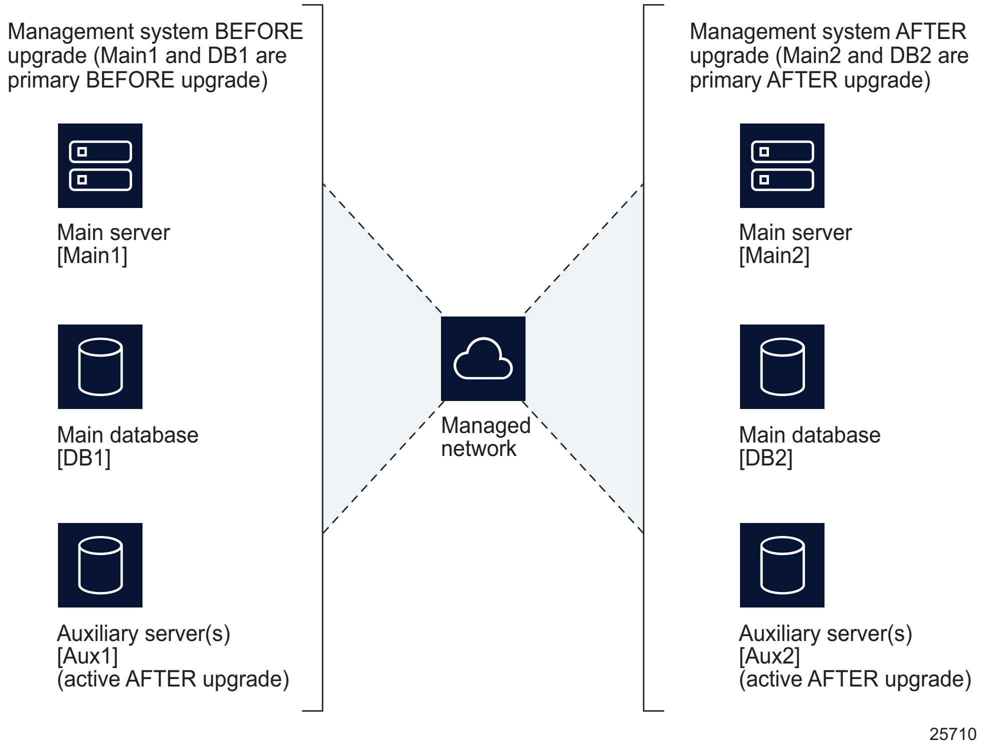
A redundant NFM-P system upgrade involves a network management outage.

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.

Figure 15-1 NFM-P component reference diagram


Management system BEFORE upgrade (Main1 and DB1 are primary BEFORE upgrade)
Main server [Main1]
Main database [DB1]
Auxiliary server(s) [Aux1] (active AFTER upgrade)
Managed network
Management system AFTER upgrade (Main2 and DB2 are primary AFTER upgrade)
Main server [Main2]
Main database [DB2]
Auxiliary server(s) [Aux2] (active AFTER upgrade)
25710

15.13 Workflow to upgrade a redundant Release 22.6 or earlier NFM-P system

15.13.1 Description

The following is the sequence of high-level actions required to upgrade a redundant NFM-P system at Release 22.6 or earlier.

15.13.2 Stages

Note: The "Upgrade redundant system" (p. 688) links lead to sections in 15.14 "To upgrade a redundant Release 22.6 or earlier NFM-P system" (p. 694).

Prepare system for upgrade

1

Perform 15.8 "To prepare for an NFM-P system upgrade from Release 22.6 or earlier" (p. 634).

Upgrade redundant system

2

Check the available disk space; see "Check pre-upgrade disk space" (p. 695).

3

Stop and disable the standby main server; see "Stop and disable standby main server [Main2]" (p. 695).

4

If the system includes auxiliary servers, stop the [Aux2] auxiliary servers; see "Stop auxiliary servers [Aux2]" (p. 697).

5

Disable the system redundancy functions; see "Disable database redundancy" (p. 697).

6

Upgrade the standby main database, which becomes the new primary main database; see "Upgrade standby main database [DB2]" (p. 698).

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.

7

Upgrade the standby main server; see "Upgrade standby main server [Main2]" (p. 708).

8

Start the PKI server; see "Start PKI server" (p. 709).

9

Configure the new primary main server; see "Configure new primary main server [Main2]" (p. 710).

10

If the NFM-P is not in a shared-mode NSP deployment, restore the local NSP databases; see "Restore embedded nspOS, independent deployment" (p. 712).

11

Restore the backed-up [Main2] data files; see "Restore new primary main server [Main2] data files" (p. 715).

12

If required, enable Windows Active Directory for client access; see "Enable Windows Active Directory access" (p. 716).

13

If required, configure ADFS to enable Common Access Card, or CAC, client access; see "Enable CAC access" (p. 718).

14

If the NFM-P is integrated with an WS-NOC system, configure the integration; see "Configure WS-NOC integration" (p. 721).

15

If the NFM-P system includes one or more NSP analytics servers or Flow Collectors, stop each; see "Stop NSP analytics servers, NSP Flow Collectors" (p. 722).

16

If the NFM-P system includes auxiliary servers, upgrade the [Aux2] auxiliary servers; see "Upgrade auxiliary servers [Aux2]" (p. 723).

17

If the system includes redundant auxiliary database clusters, verify the most recent data synchronization; see "Verify auxiliary database synchronization" (p. 723).

18

If the system includes redundant auxiliary database clusters, enable cluster maintenance mode; see "Enable maintenance mode on auxiliary database agent" (p. 724).

19

If the system includes redundant auxiliary database clusters, upgrade the standby cluster; see "Upgrade standby auxiliary database cluster" (p. 726).

20

Stop and disable the original primary main server; see "Stop and disable original primary main server [Main1]" (p. 726).

Note: This stage marks the beginning of the network management outage.

21

If the system includes one or more NSP Flow Collectors, upgrade each NSP Flow Collector Controller and Flow Collector; see "Upgrade NSP Flow Collector Controllers, Flow Collectors" (p. 728).

22

If the NFM-P system includes auxiliary servers, stop the [Aux1] auxiliary servers; see “Stop auxiliary servers [Aux1]” (p. 728).

23

Stop the original primary main database; see “Stop original primary main database [DB1]” (p. 728).

24

If the system includes a standalone auxiliary database cluster, upgrade the cluster; see “Upgrade auxiliary database, if not redundant” (p. 729).

25

If the system includes redundant auxiliary database clusters, enable maintenance mode for the former primary cluster; see “Enable maintenance mode for auxiliary database agent” (p. 729).

26

If the system includes redundant auxiliary database clusters, stop the former primary cluster; see “Stop former primary auxiliary database cluster” (p. 729).

27

Start the new primary main server; see “Start new primary main server [Main2]” (p. 730).

28

If the system includes auxiliary servers, start the [Aux2] auxiliary servers; see “Start auxiliary servers [Aux2]” (p. 732).

29

If the system includes redundant auxiliary database clusters, activate the upgraded former standby cluster, see “Activate upgraded former standby auxiliary database cluster” (p. 732).

30

If the system includes one or more NSP analytics servers, upgrade each analytics server; see “Upgrade analytics servers” (p. 733).

31

Upgrade or install at least one NFM-P single-user client or client delegate server; see “Enable GUI client” (p. 733).

Note: This stage marks the end of the network management outage.

32

Perform sanity testing on the NFM-P system using a GUI client; see “Test upgraded system using GUI client” (p. 734).

33

Uninstall the original primary main database; see "Uninstall original primary database [DB1]" (p. 734).

34

Install the new standby main database; see "Install new standby main database [DB1]" (p. 734).

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.

35

Reinstantiate the standby database; see "Reinstantiate standby database" (p. 740).

36

If the NSP system includes redundant auxiliary database clusters, upgrade the former primary cluster; see "Upgrade former primary auxiliary database cluster" (p. 741).

37

Upgrade the original primary main server as the new standby main server; see "Upgrade original primary main server [Main1]" (p. 741).

38

Restore the backed-up [Main1] data files; see "Restore new standby main server [Main1] data files" (p. 745)

39

Configure the new standby main server; see "Configure new standby main server [Main1]" (p. 742).

40

If required, enable Windows Active Directory for client access; see "Enable Windows Active Directory access" (p. 746).

41

If required, configure ADFS to enable Common Access Card, or CAC, client access; see "Enable CAC access" (p. 748).

42

If the NFM-P is integrated with an WS-NOC system, configure the integration; see "Configure WS-NOC integration" (p. 751).

43

Start the new standby main server; see "Start new standby main server [Main1]" (p. 752).

44

If the system includes auxiliary servers, upgrade the [Aux1] auxiliary servers; see "Upgrade auxiliary servers [Aux1]" (p. 754).

45

If the system includes auxiliary servers, start the [Aux1] auxiliary servers; see "Start auxiliary servers [Aux1]" (p. 754).

46

If the system includes redundant auxiliary database clusters, activate each cluster; see "Disable maintenance mode for auxiliary database agents" (p. 754).

47

If the system includes an auxiliary database, verify that the auxiliary database is functioning correctly; see "Verify auxiliary database status" (p. 755).

48

Recheck the available disk space; see "Check post-upgrade disk space" (p. 757).

49

Install or upgrade single-user GUI clients, as required; see "Install or upgrade single-user GUI clients" (p. 758).

50

Install or upgrade client delegate servers, as required; see "Install or upgrade client delegate servers" (p. 758).

51

Stop the PKI server; see "Stop PKI server" (p. 758).

52

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. 759).

53

Configure and enable firewalls, if required; see "Configure and enable firewalls" (p. 759).

15.13.3 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 15-2 Workflow for concurrent task execution during redundant upgrade

System redundancy mode	Operator A actions	Operator B actions
DUPLEX	Stage 1 — Actions described in 15.8 “To prepare for an NFM-P system upgrade from Release 22.6 or earlier” (p. 634)	
	Stage 2 — “Check pre-upgrade disk space” (p. 695) Stage 3 — “Stop and disable standby main server [Main2]” (p. 695)	Stage 4 — “Stop auxiliary servers [Aux2]” (p. 697) Stage 5 — “Disable database redundancy” (p. 697)
SIMPLEX	Stage 6 — “Upgrade standby main database [DB2]” (p. 698)	Stage 8 — “Start PKI server” (p. 709) Stage 7 — “Upgrade standby main server [Main2]” (p. 708)
	Stage 9 — “Configure new primary main server [Main2]” (p. 710)	Stage 11 — “Restore new primary main server [Main2] data files” (p. 715)
	Stage 10 — “Restore embedded nspOS, independent deployment” (p. 712) Stage 12 — “Enable Windows Active Directory access” (p. 716) Stage 13 — “Enable CAC access” (p. 718)	Stage 14 — “Configure WS-NOC integration” (p. 721)
	Stage 15 — “Stop NSP analytics servers, NSP Flow Collectors” (p. 722)	Stage 17 — “Verify auxiliary database synchronization” (p. 723) Stage 18 — “Enable maintenance mode on auxiliary database agent” (p. 724) Stage 19 — “Upgrade standby auxiliary database cluster” (p. 726)
	Stage 16 — “Upgrade auxiliary servers [Aux2]” (p. 723)	
OUTAGE	Stage 20 — “Stop and disable original primary main server [Main1]” (p. 726)	Stage 24 — “Upgrade auxiliary database, if not redundant” (p. 729)
	Stage 21 — “Upgrade NSP Flow Collector Controllers, Flow Collectors” (p. 728)	Stage 25— “Enable maintenance mode for auxiliary database agent” (p. 729)
	Stage 22 — “Stop auxiliary servers [Aux1]” (p. 728)	Stage 26— “Stop former primary auxiliary database cluster” (p. 729)
	Stage 23 — “Stop original primary main database [DB1]” (p. 728)	Stage 28 — “Start auxiliary servers [Aux2]” (p. 732)
	Stage 27 — “Start new primary main server [Main2]” (p. 730) **Note:** The outage persists until device discovery completes.	Stage 29 — “Activate upgraded former standby auxiliary database cluster” (p. 732)

Table 15-2 Workflow for concurrent task execution during redundant upgrade (continued)

System redundancy mode	Operator A actions	Operator B actions
SIMPLEX	Stage 30 — “Upgrade analytics servers” (p. 733)	Stage 31 — “Enable GUI client” (p. 733)
	Stage 32 — “Test upgraded system using GUI client” (p. 734)	
	Stage 33 — “Uninstall original primary database [DB1]” (p. 734) Stage 34 — “Install new standby main database [DB1]” (p. 734)	—
	Stage 35 — “Reinstantiate standby database” (p. 740) Stage 37 — “Upgrade original primary main server [Main1]” (p. 741) Stage 38 — “Restore new standby main server [Main1] data files” (p. 745)	Stage 36 — “Upgrade former primary auxiliary database cluster” (p. 741)
	Stage 39 — “Configure new standby main server [Main1]” (p. 742) Stage 40 — “Enable Windows Active Directory access” (p. 746) Stage 41 — “Enable CAC access” (p. 748)	Stage 42 — “Configure WS-NOC integration” (p. 751)
	Stage 43 — “Start new standby main server [Main1]” (p. 752)	Stage 44 — “Upgrade auxiliary servers [Aux1]” (p. 754) Stage 45 — “Start auxiliary servers [Aux1]” (p. 754) Stage 46 — “Disable maintenance mode for auxiliary database agents” (p. 754) Stage 47 — “Verify auxiliary database status” (p. 755)
DUPLEX	Stage 48 — “Check post-upgrade disk space” (p. 757) Stage 49 — “Install or upgrade single-user GUI clients” (p. 758)	Stage 50 — “Install or upgrade client delegate servers” (p. 758)
	Stage 51 — “Stop PKI server” (p. 758) Stage 52 — “Restore TLS version and cipher support configuration” (p. 759)	Stage 53 — “Configure and enable firewalls” (p. 759)

15.14 To upgrade a redundant Release 22.6 or earlier NFM-P system

15.14.1 Description

The following steps describe how to upgrade a collocated or distributed Release 22.6 or earlier 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:

- on each server station in the system — 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

15.14.2 Steps

Check pre-upgrade disk space

1

As part of the trial upgrade on a lab system in advance of a live upgrade, you must ensure that the available disk capacity on each NFM-P component remains within tolerance.

Note: If the disk usage on an NFM-P partition approaches or exceeds 80% after the trial upgrade, you may need to add disk capacity before you attempt the upgrade on a live system.

Perform the following steps on each of the following stations:

- main server
- auxiliary server
- main database
- auxiliary database

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following:

   ```
   # df -kh ↵
   ```

   The usage information for each partition is displayed.
4. Record the information for each NFM-P partition; see the tables in Chapter 2, “NSP disk setup and partitioning” for the partition names and required capacities.

Stop and disable standby main server [Main2]

2

Open a GUI client to monitor the network during the upgrade.

3

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.

6. Enter the following to switch to the root user:

   ```
   bash$ su ↵
   ```

7. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to display the nspOS service status:

   ```
   # nspdctl status ↵
   ```

   Information like the following is displayed.

   ```
   Mode:     DR
   Role:     redundancy_role
   DC-Role:  dc_role
   DC-Name:  dc_name
   Registry: IP_address:port
   State:    stopped
   Uptime:   0s
   SERVICE          STATUS
   service_a        inactive
   service_b        inactive
   service_c        inactive
   ```

   You must not proceed to the next step until all NSP services are stopped; if the State is not ‘stopped’, or the STATUS indicator of each listed service is not ‘inactive’, repeat this substep.

4

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:

   ```
   # systemctl disable nspos-nspd.service ↵
   ```

2. Enter the following:

   ```
   # systemctl disable nfmp-main-config.service ↵
   ```

3. Enter the following:

   ```
   # systemctl disable nfmp-main.service ↵
   ```

Stop auxiliary servers [Aux2]

5

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

6

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 ↵
   ```

4. Make a backup copy of the nms-server.xml file.
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:

   ```
   <db
   ```

7. Locate the following line in the section:

   ```
   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:

   ```
   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:

    ```
    redundancyEnabled="true"
    ```

    to read:

    ```
    redundancyEnabled="false"
    ```

12. Save and close the nms-server.xml file.
13. Enter the following:

    ```
    bash$ /opt/nsp/nfmp/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]

7

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.

8

Open a console window.

9

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 ↵
```

10

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.
6. Click Properties. The Aggregation Rule (multiple instances) [Edit] form opens.
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.

11

Perform the following steps.

1. Open the /etc/fstab file using a plain-text editor such as vi.
2. Locate the tmpfs file system entry.
3. Remove the noexec option so that the entry reads as follows:
   ```
   tmpfs /dev/shm tmpfs nodev 0 0
   ```
4. Save and close the /etc/fstab file.
5. Enter the following to remount the /dev/shm partition:
   ```
   # mount -o remount /dev/shm ↵
   ```

12

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 Planning Guide*.

For information about deploying the RHEL OS using an NSP OEM disk image, see 2.2.2 “NSP disk-image deployment” (p. 28).

Note: After the upgrade, the station is the new primary main database station.

13

Log in as the root user on the station that is commissioned as the main database [DB2] station.

14

Perform one of the following.

a. If the main server and database are collocated on one station, perform the following steps.

1. Enter the following:
   ```
   # mkdir /opt/importConfigs ↵
   ```
2. Transfer the mainserverBackupConfigs.tar.gz file created in Step 32 of 15.8 “To prepare for an NFM-P system upgrade from Release 22.6 or earlier” (p. 634) to the /opt/importConfigs directory.
3. Transfer the following downloaded installation files to an empty directory on the collocated 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.

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
- nsp-nfmp-nodeexporter-*R.r.p*-rel.*v*.rpm, if downloaded

Note: In subsequent steps, the directory is called the NFM-P software directory.

15

Transfer the following downloaded file to an empty directory on the main database station:

- OracleSw_PreInstall.sh

16

Navigate to the directory that contains the OracleSw_PreInstall.sh file.

17

Enter the following:

```
# chmod +x OracleSw_PreInstall.sh ↵
```

18

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]:
```

19

Enter Yes. The following prompt is displayed:

```
Enter the Oracle dba group name [group]:
```

20

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:
```

21

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/oracle19].

Checking or Creating the Oracle user home directory
/opt/nsp/nfmp/oracle19...

Checking user username...

Adding username...

Changing ownership of the directory /opt/nsp/nfmp/oracle19 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:
```

22

Enter a password. The following prompt is displayed:

```
Re-enter new Password:
```

23

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]:
```

24

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.
```

25

When the script execution is complete, enter the following to reboot the main database station:

```
# systemctl reboot ↵
```

The station reboots.

26

When the reboot is complete, log in to the main database [DB2] station as the root user.

27

Open a console window.

28

Navigate to the NFM-P software directory.

Note: Ensure that the directory contains only the installation files.

29

Enter the following:

```
# chmod +x * ↵
```

30

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

31

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

32

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/nsp/nfmp/dbbackup/backupset_1
```

Note: Ensure that the Oracle management user has full access to the directory and contents.

33

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 .....
<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
```

34

Stop 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 stop the main database:

   ```
   # systemctl stop nfmp-main-db.service ↵
   ```

35

You must prepare the restored database for the upgrade.

Navigate to the directory that contains the OracleSw_PreInstall.sh file.

36

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]:
```

37

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/samdb/install.

Existing NFM-P database version = version

Enter the password for the "SYS" Oracle user (terminal echo is off):
```

38

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/oracle19...

Checking user username...

usermod: no changes

Changing ownership of the directory /opt/nsp/nfmp/oracle19 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]:
```

39

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; otherwise, go to Step 40.

```
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 36.

40

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]:
```

41

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
```

42

Enter the following to upgrade the database:

Note: A database upgrade takes considerable time that varies, depending on the release from which you are upgrading.

```
# samupgradeDb ↵
```

The following prompt is displayed:

```
Enter the password for the "SAMUSER" database user (terminal echo is
off):
```

43

Enter the database user password.

The database upgrade begins, and messages like the following are displayed:

```
Validation succeeded.

Upgrade log is /opt/nsp/nfmp/db/install/NFM-P_Main_Database.upgrade.
timestamp.stdout.txt

Performing Step 1 of n - Initializing ..........

Performing NFM-P database upgrade will take time...

Executing PreOraUpgrade.sql ............

Executing ShutdownDBUpgrade.sql ....

Executing StartupDB.sql .....

Executing DbJavaReload.sql ...............
```

The database upgrade is complete when the following is displayed:

```
DONE
```

44

Verify the database configuration and create the database.

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; see 14.9 “NFM-P samconfig utility” (p. 432) for information about using samconfig.
4. Configure one or more parameters, if required, and then enter **back** ↵.
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]

45

If the main server [Main2] and database [DB2] are on separate stations, and you are re-using the [Main2] main server station, recommission the station according to the platform specifications in this guide and in the *NSP Planning Guide*.

For information about deploying the RHEL OS using an NSP OEM disk image, see 2.2.2 “NSP disk-image deployment” (p. 28).

46

Log in as the root user on the station that is commissioned as the [Main2] station.

Note: After the upgrade, the station is the new primary main server station.

47

Open a console window.

48

If the main server and database are on separate stations, perform the following steps.

1. Enter the following:

```
# mkdir /opt/importConfigs ↵
```

2. Transfer the mainserverBackupConfigs.tar.gz file created in Step 32 of 15.8 “To prepare for an NFM-P system upgrade from Release 22.6 or earlier” (p. 634) to the /opt/importConfigs directory.

49

Perform one of the following.

a. If the main server and database are collocated on one station, go to Step 55.

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
- nsp-nfmp-nodeexporter-*R.r.p*-rel.*v*.rpm, if downloaded

Note: In subsequent steps, the directory is called the NFM-P software directory.

50

Navigate to the NFM-P software directory.

51

Enter the following:

```
# chmod +x * ↵
```

52

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

53

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

Start PKI server

54

Start the PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 4.10 “To configure and enable a PKI server” (p. 113).

Note: The PKI server is required for internal system configuration purposes.

Configure new primary main server [Main2]

55

Enter the following; see 14.9 “NFM-P samconfig utility” (p. 432) 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>
```

56

Enter the following:

```
<main> configure ↵
```

The prompt changes to `<main configure>`.

57

To apply a new or updated NFM-P license, 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 the *NSP System Administrator Guide*.

```
<main configure> license license_file ↵
```

where *license_file* is the path and file name of the NSP license bundle

58

Enter the following:

```
<main configure> database instance primary_instance back ↵
```

where *primary_instance* is the [DB1] database instance name, which is the primary Instance Name recorded in Step 43 of 15.8 “To prepare for an NFM-P system upgrade from Release 22.6 or earlier” (p. 634)

59

Enter the following:

```
<main configure> redundancy database instance standby_instance back ↵
```

where *standby_instance* is the [DB2] database instance name, which is the standby Instance Name recorded in Step 44 of 15.8 “To prepare for an NFM-P system upgrade from Release 22.6 or earlier” (p. 634)

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

60

Enter the following:

```
<main configure redundancy> back ↵
```

The prompt changes to `<main configure>`.

61

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; see 14.9 “NFM-P samconfig utility” (p. 432) for information about using the samconfig utility.
3. Configure one or more parameters, if required.

   Note: The NFM-P uses the database backup settings to initialize the database during installation only. To change the backup settings after installation, you must use the Database Manager form in the NFM-P client GUI, as described in the *NSP System Administrator Guide*.
4. When you are certain that the configuration is correct, enter the following:

   ```
   <main configure> back ↵
   ```

   The prompt changes to `<main>`.

62

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

63

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

64

If the NFM-P is part of a shared-mode NSP system and you want to enable mTLS for internal Kafka authentication using two-way TLS, perform the following steps.

Note: Enabling mTLS for internal Kafka authentication is supported only in an NSP deployment that uses separate interfaces for internal and client communication.

Note: The parameter you must configure is displayed only if the ip-list parameter is set to a remote address.

Note: The parameter is configurable only if the **secure** and **internal-certs** parameters in the **nspos** section are set to true.

1. Enter the following:

   ```
   # samconfig -m main ↵
   ```

   The following is displayed:

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

2. Enter the following:

   ```
   # configure nspos mtls-kafka-enabled back ↵
   ```

3. Enter the following:

   ```
   <main> apply ↵
   ```

   The configuration is applied.

4. Enter the following:

   ```
   <main> exit ↵
   ```

   The samconfig utility closes.

Restore embedded nspOS, independent deployment

65

In an independent NFM-P deployment, you must restore the embedded Neo4j and PostgreSQL databases. Otherwise, if the NFM-P is integrated with an NSP cluster, go to Step 83.

66

Enter the following:

```
# mkdir /opt/nsp/os/backup ↵
```

67

Enter the following:

```
# chown nsp:nsp /opt/nsp/os/backup ↵
```

68

Copy the Neo4j and PostgreSQL backup files saved in Step 31 of 15.8 “To prepare for an NFM-P system upgrade from Release 22.6 or earlier” (p. 634) to the /opt/nsp/os/backup directory.

69

Restore the Neo4j database.

1. Enter the following:

   ```
   # cd /opt/nsp/os/install/tools/database ↵
   ```

2. Enter the following:

```
# ./db-restore.sh --target IP_address ↵
```

where *IP_address* is the main server [Main2] IP address

The following message and prompt are displayed:

```
Verifying prerequisites...

Starting database restore ...

Backupset file to restore (.tar.gz format):
```

3. Enter the following and press ↵:

```
path/nspos-neo4j_backup_timestamp.tar.gz
```

where

path is the absolute path of the Neo4j backup file

timestamp is the backup creation time

Note: Neo4j backup files are stored in the following locations on a main server, depending on the backup type:

- scheduled backup—/opt/nsp/os/backup/backupset_*n*
- manual backup—/opt/nsp/os/backup/manual_*timestamp*

The following messages and prompt are displayed:

```
PLAY [all] ************************************************

TASK [dbrestore : Create temporary directory] ***************

changed: [server_IP]

[dbrestore : pause]

Do you want to restore the nspOS Neo4j db from file:
path/nspos-neo4j_backup_timestamp.tar.gz? Press return to continue,
or Ctrl+C to abort:
```

4. Press ↵.

The restore operation begins, and messages like the following are displayed:

```
TASK [dbrestore : Copy backupset] ***************************

changed: [server_IP]

TASK [dbrestore : Running nspdctl stop] *********************

changed: [server_IP]

TASK [dbrestore : Ensure database service is stopped] *******

changed: [server_IP]

TASK [dbrestore : Perform database restore] *****************

changed: [server_IP]

TASK [dbrestore : Delete temporary directory] ***************

changed: [server_IP]

PLAY RECAP ************************************************

server_IP     : ok=n   changed=n    unreachable=n   failed=n
```

5. If the `failed` value is greater than zero, a restore failure has occurred; contact technical support for assistance.

70

Restore the PostgreSQL database.

1. Enter the following:

```
# ./db-restore.sh --target IP_address ↵
```

where *IP_address* is the main server [Main2] IP address

The following message and prompt are displayed:

```
Verifying prerequisites...
Starting database restore ...
Backupset file to restore (.tar.gz format):
```

2. Enter the following and press ↵:

```
path/nspos-postgresql_backup_timestamp.tar.gz
```

where

path is the absolute path of the PostgreSQL backup file

timestamp is the backup creation time

Note: PostgreSQL backup files are stored in the following locations on a main server, depending on the backup type:

- scheduled backup—/opt/nsp/os/backup/backupset_*n*
- manual backup—/opt/nsp/os/backup/manual_*timestamp*

The following messages and prompt are displayed:

```
PLAY [all] **************************************************
[dbrestore : pause]
Do you want to restore the nspOS PostgreSQL db from file:
path/nspos-postgresql_backup_timestamp.tar.gz? Press return to
continue, or Ctrl+C to abort:
```

3. Press ↵.

The restore operation begins, and messages like the following are displayed:

```
TASK [dbrestore : Running nspdctl stop] ********************
changed: [server_IP]
TASK [dbrestore : Perform database restore] *****************
changed: [server_IP]
TASK [dbrestore : Delete temporary directory] ***************
changed: [server_IP]
PLAY RECAP **************************************************
server_IP     : ok=n   changed=n    unreachable=n   failed=n
```

4. If the `failed` value is greater than zero, a restore failure has occurred; contact technical support for assistance.

Restore new primary main server [Main2] data files

71

Transfer the main server data backup .tar.gz file set created in Step 34 of 15.8 “To prepare for an NFM-P system upgrade from Release 22.6 or earlier” (p. 634) to the /opt/nsp/nfmp directory on the [Main2] main server station.

72

Enter the following:

```
# cd /opt/nsp/nfmp ↵
```

73

Enter the following:

```
# chown nsp:nsp *.tar.gz ↵
```

74

Enter the following:

```
# ls *.tar.gz ↵
```

The data backup files are listed.

75

For each listed file, enter the following:

```
# tar -xf filename.tar.gz -C /opt/nsp/nfmp/ ↵
```

where *filename* is a backup timestamp in the format MM-DD-hh-mm

76

Enter the following:

```
# rm -f *.tar.gz ↵
```

77

Enter the following:

```
# chown -R nsp:nsp /opt/nsp/nfmp/lte ↵
```

78

Enter the following:

```
# chown -R nsp:nsp /opt/nsp/nfmp/nebackup ↵
```

79

Enter the following:

```
# chown -R nsp:nsp /opt/nsp/nfmp/nelogs ↵
```

80

Enter the following:

```
# chown -R nsp:nsp /opt/nsp/nfmp/nesoftware ↵
```

81

Enter the following:

```
# chown -R nsp:nsp /opt/nsp/nfmp/os ↵
```

82

Enter the following:

```
# chown -R nsp:nsp /opt/nsp/nfmp/server/script/savedResults ↵
```

Enable Windows Active Directory access

83

If you intend to use Windows Active Directory, or AD, for single-sign-on client access, you must configure LDAP remote authentication for AD; otherwise,go to Step 102.

Open the following file as a reference for use in subsequent steps:

/opt/nsp/os/install/examples/config.yml

Note: Consider the following.

- The NFM-P does not assign a default user group to users of a remote authentication source that you define for Windows AD; the authentication source must provide the user group attributes.
- Windows AD supports the following LDAP server types for remote authentication:

  AD—The user group of an AD user is derived from the group_base_dn attribute in the server configuration; group search filters are not supported.

  AUTHENTICATED—The server configuration must include bind credentials; group search filters are supported. After NFM-P initialization, you add the AD server bind credentials to the NSP password vault using the NSP Session Manager REST API.

84

Locate the section that begins with the following lines:

```
#   ldap:
#     enabled: true
#     servers:
#       - type: AUTHENTICATED/AD/ANONYMOUS
#         url: ldaps://ldap.example.com:636
#         security: SSL/STARTTLS/NONE
```

85

Open the following file using a plain-text editor such as vi:

/opt/nsp/os/install/config.json

86

Locate the section that begins with the following line:

```
"sso": {
```

The section has one subsection for each type of SSO access.

Note: You can enable multiple remote authentication methods such as LDAP and RADIUS in the config.json file, or by using the NFM-P GUI. Using the GUI also allows you to specify the order in which the methods are tried during login attempts; however, no ordering is applied to multiple methods enabled in the config.json file.

87

In the **sso** section, create an **ldap** subsection as shown below using the parameter names from the **ldap** section of config.yml and the required values for your configuration.

The following example shows the LDAP configuration for two AD servers:

```
"ldap": {
"enabled": true,
"servers": [
{
"type": "auth_type",
"url": "ldaps://server1:port",
"server1_parameter_1": "value",
"server1_parameter_2": "value",
.
.
"server1_parameter_n": "value",
},
{
"type": "auth_type",
"url": "ldaps://server2:port",
"server2_parameter_1": "value",
"server2_parameter_2": "value",
.
.
"server2_parameter_n": "value",
},
}]
}
```

where *auth_type* is AD or AUTHENTICATED

88

Save and close the files.

89

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

90

Enter the following:

```
<main> apply ↵
```

The AD LDAP configuration is applied.

91

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Enable CAC access

92

If you do not intend to enable Common Access Card, or CAC, technology for NFM-P client access, go to Step 102.

93

Download the federationmetadata.xml from the following ADFS link:

https://*ADFS_server_name*/FederationMetadata/2007-06/federationmetadata.xml

where *ADFS_server_name* is the ADFS server FQDN

94

Add an ADFS server entry to the /etc/hosts file on the main server.

1. Open the /etc/hosts file using a plain-text editor such as vi.
2. Add the following line below the line that contains the main server IP address:

   ```
   IP_address FQDN
   ```

   where

   IP_address is the IP address of the ADFS server

   FQDN is the FQDN of the ADFS server
3. Save and close the file.

95

In order to enable CAC for client access, you must configure Active Directory Federation Services, or ADFS.

Open the following file using a plain-text editor such as vi:

/opt/nsp/os/install/config.json

96

In the **sso** section, create an **saml2** subsection as shown below using the parameter names from the **saml2** section of config.yml and the required values for your configuration.

The following example shows the ADFS configuration.

Note: You must preserve the lead spacing of each line.

```
  "sso" : {
    "saml2": {
       "enabled": true,
       "service_provider_entity_id": "NFM-P_identifier",
       "service_provider_metadata_filename": "casmetadata.xml",
       "maximum_authentication_lifetime": 3600,
       "accepted_skew": 300,
       "destination_binding": "urn:oasis:names:tc:SAML:2.0:bindings:
HTTP-Redirect",
       "identity_provider_metadata_path": "ADFS_metadata_file",
       "authn_context_class_ref": "urn:oasis:names:tc:SAML:2.0:ac:
classes:TLSClient",
       "authn_context_comparison_type": "minimum",
       "name_id_policy_format": "urn:oasis:names:tc:SAML:1.1:
nameid-format:unspecified",
       "force_auth": true,
       "passive": false,
       "wants_assertions_signed": false,
       "wants_responses_signed": false,
       "all_signature_validation_disabled": false,
       "sign_service_provider_metadata": false,
       "principal_id_attribute": "UPN",
       "use_name_qualifier": false,
       "provider_name": "ADFS_server_URI",
       "requested_attributes": [{
         "name": "http://schemas.xmlsoap.
org/ws/2005/05/identity/claims/emailaddress",
          "friendly_name": "E-Mail Address",
          "name_format": "urn:oasis:names:tc:SAML:2.0:attrname-format:
uri",
          "required": false
      } ],
       "mapped_attributes": [{
           "name": "http://schemas.xmlsoap.org/claims/Group",
           "mapped_to": "authorizationProfile"
      }, {
           "name": "http://schemas.xmlsoap.
org/ws/2005/05/identity/claims/upn",
           "mapped_to": "upn"
      } ]
    },
```

97

Configure the following parameters; leave all other parameters at the default:

- "service_provider_entity_id": "*NFM-P_identifier*"
- "identity_provider_metadata_path": "*ADFS_metadata_file*"
- "provider_name": "*ADFS_server_name*"

NFM-P_identifier is the unique ADFS Relying Trust Party identifier

*ADFS_metadata_fil*e is the absolute path of the ADFS metadata XML file, for example, /opt/federationmetadata.xml

ADFS_server_name is the ADFS server FQDN

98

Save and close the files.

99

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

100

Enter the following:

```
<main> apply ↵
```

The ADFS configuration is applied.

101

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Configure WS-NOC integration

102

If the NFM-P is integrated with a WS-NOC system, open the following file with a plain-text editor such as vi:

/opt/nsp/os/install/examples/config.json

Otherwise, go to Step 112.

103

Copy the following section:

```
  "nfmt": {
    "primary_ip": "",
    "standby_ip": "",
    "username": "",
    "password": "",
    "cert_provided": false
  },
```

104

Close the file.

105

Open the following file with a plain-text editor such as vi:

/opt/nsp/os/install/config.json

106

Paste in the copied section.

107

Configure the required parameters to enable the WS-NOC integration:

- primary_ip—the primary WS-NOC server IP address
- standby_ip—the standby WS-NOC server IP address
- username—the username required for WS-NOC access
- password—the password required for WS-NOC access
- cert_provided—whether a TLS certificate is used

108

Save and close the file.

109

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

110

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

111

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Stop NSP analytics servers, NSP Flow Collectors

112

If the system includes one or more NSP 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/analytics/bin/AnalyticsAdmin.sh stop ↵
   ```

The following is displayed:

```
Stopping Analytics Application
```

When the analytics server is completely stopped, the following message is displayed:

```
Analytics Application is not running
```

113

If the system includes one or more NSP Flow Collector Controllers and Flow Collectors, stop each NSP Flow Collector Controller.

> **Note:** If the NSP Flow Collector Controller is collocated on a station with an NSP Flow Collector, stopping the NSP Flow Collector Controller also stops the Flow Collector.

1. Log in to the NSP Flow Collector Controller station as the nsp user.

2. Open a console window.
3. Enter the following:

```
bash$ /opt/nsp/flow/fcc/bin/flowCollectorController.bash stop ↵
```

   The NSP Flow Collector Controller stops.

114

If the system includes one or more NSP Flow Collectors that are not collocated on a station with a Flow Collector Controller, stop each such NSP Flow Collector.

1. Log in to the NSP Flow Collector station as the nsp user.
2. Open a console window.
3. Enter the following:

```
bash$ /opt/nsp/flow/fc/bin/flowCollector.bash stop ↵
```

   The NSP Flow Collector stops.

Upgrade auxiliary servers [Aux2]

115

If the system includes auxiliary servers, perform 15.15 “To upgrade a Release 22.6 or earlier NFM-P auxiliary server” (p. 760) on each appropriate auxiliary server station [Aux2].

Verify auxiliary database synchronization

116

If the system does not include redundant auxiliary database clusters, go to Step 121.

117

If you are upgrading the first redundant auxiliary database cluster, you must verify the success of the most recent copy-cluster operation, which synchronizes the database data between the redundant clusters.

Note: You must not proceed to the next step until the copy-cluster operation is complete and successful.

Perform one of the following periodically to check the copy-cluster status.

a. If the NFM-P is in a shared-mode NSP deployment, issue the following REST API call:

   Note: In order to issue a REST API call, you require a REST token; see this tutorial on the Network Developer Portal for information.

```
GET https://address:8545/restconf/data/auxdb:/auxdb-agent
```

   where *address* is the advertised address of the primary NSP cluster

   The call returns a status of SUCCESS, as shown below, for a successfully completed copy-cluster operation:

```
<HashMap>
```

```
      <auxdb-agent>
         <name>nspos-auxdb-agent</name>
         <application-mode>ACTIVE</application-mode>
         <copy-cluster>
            <source-cluster>cluster_M</source-cluster>
            <target-cluster>cluster_N</target-cluster>
            <time-started>timestamp</time-started>
            <status>SUCCESS</status>
         </copy-cluster>
      </auxdb-agent>
</HashMap>
```

b. If the NFM-P is not in a shared-mode NSP deployment and you are upgrading from NSP 21.9 or earlier, enter the following as the root user on the primary main server station [Main1]:

```
# grep "The copy cluster state has changed.*to.*SUCCESS"
/opt/nsp/os/auxdb-agent/logs/nspos-auxdb-agent.log ↵
```

The command returns an output line like the following for a successfully completed copy-cluster operation:

```
<timestamp><I><server><ClusterManagerExecutorPool[0]><com.nokia.nsp.
nspos.auxdb.agent.cluster.ClusterManager>The copy cluster state has
changed from [RUNNING] to [SUCCESS] - [Completed..]
```

If no output is displayed, a copy-cluster operation may be in progress.

c. If the NFM-P is not in a shared-mode NSP deployment and you are upgrading from NSP 21.11 or later, enter the following as the root user on the primary main server station [Main1]:

```
# /opt/nsp/os/nspd/nspdctl auxdb agent-status ↵
```

The command returns output like the following for a successfully completed copy-cluster operation:

```
DC-ROLE HOST APPLICATION-MODE
active leader 203.0.113.101 ACTIVE
Copy Cluster Details
SOURCE TARGET TIME-STARTED STATUS
cluster_1 cluster_2 2022-03-14T15:09:26.535Z SUCCESS
```

Enable maintenance mode on auxiliary database agent

118

Perform one of the following to enable nspos-auxdb-agent maintenance mode.

a. If the NFM-P is in a shared-mode NSP deployment, perform the following steps.

1. Log in as the root user on the NSP cluster host in the primary data center.

2. Enter the following to set the nspos-auxdb-agent mode to maintenance:

   ```
   # kubectl patch configmap/nspos-auxdb-agent-overrides --type=merge
   -p '{"data":{"nspos-auxdb-agent-overrides.json":"{\"auxDbAgent\":
   {\"config\":{\"maintenance-mode\":true}}}"}}' ↵
   ```

3. Enter the following to restart the nspos-auxdb-agent pod:

   ```
   # kubectl delete pod `kubectl describe pods | grep -P ^^Name: |
   grep -oP nspos-auxdb-agent[-a-zA-Z0-9]+` ↵
   ```

4. Issue the following REST API call against the primary NSP cluster to verify that the agent is in maintenance mode:

   NOTE: In order to issue a REST API call, you require a REST token; see this tutorial on the Network Developer Portal for information.

   GET https://*address*:8545/restconf/data/auxdb:/auxdb-agent

   where *address* is the advertised address of the primary NSP cluster

   The call returns information like the following:

   ```
   {
       "auxdb-agent": {
           "name": "nspos-auxdb-agent",
           "application-mode": "MAINTENANCE",
           "copy-cluster": {
               "source-cluster": "cluster_2",
               "target-cluster": "cluster_1",
               "time-started": "timestamp",
               "status": "SUCCESS"
           }
       }
   }
   ```

   The agent is in maintenance mode if the application-mode is MAINTENANCE, as shown in the example.

5. Log in as the root user on the NSP cluster host in the standby data center.

6. Enter the following to set the nspos-auxdb-agent mode to maintenance:

   ```
   # kubectl patch configmap/nspos-auxdb-agent-overrides --type=merge
   -p '{"data":{"nspos-auxdb-agent-overrides.json":"{\"auxDbAgent\":
   {\"config\":{\"maintenance-mode\":true}}}"}}' ↵
   ```

b. If the NFM-P is not in a shared-mode NSP deployment and you are upgrading from Release 21.11 or later, perform the following steps.

1. Log in as the root user on the NSP cluster host in the primary data center.

2. Enter the following to set the nspos-auxdb-agent mode to maintenance:

   ```
   # sed -i -r 's/("maintenance-mode"\s*:\s*)false/\1true/g'
   /opt/nsp/os/auxdb-agent/conf/nspos-auxdb-agent-overrides.json ↵
   ```

3. Enter the following to verify that the nspos-auxdb-agent is in maintenance mode:

   ```
   # /opt/nsp/os/nspd/nspdctl auxdb agent-status ↵
   DC-ROLE          HOST              APPLICATION-MODE
   active leader    203.0.113.101     MAINTENANCE
   standby leader   203.0.113.102     inactive
   ```

   The agent is in maintenance mode if the APPLICATION-MODE of the active leader is MAINTENANCE, as shown in the example.
4. Log in as the root user on the NSP cluster host in the standby data center.
5. Enter the following to set the nspos-auxdb-agent mode to maintenance:

   ```
   # sed -i -r 's/("maintenance-mode"\s*:\s*)false/\1true/g'
   /opt/nsp/os/auxdb-agent/conf/nspos-auxdb-agent-overrides.json ↵
   ```

Upgrade standby auxiliary database cluster

119

If you are upgrading the first redundant auxiliary database cluster, perform the following steps to stop the database proxy on each station in each auxiliary database cluster.

1. Enter the following sequence of commands as the root user on each auxiliary database station in the standby data center:

   ```
   # systemctl stop nfmp-auxdbproxy.service ↵
   # systemctl disable nfmp-auxdbproxy.service ↵
   ```

   The proxy stops, and is disabled.
2. Enter the following sequence of commands as the root user on each auxiliary database station in the primary data center:

   ```
   # systemctl stop nfmp-auxdbproxy.service ↵
   # systemctl disable nfmp-auxdbproxy.service ↵
   ```

   The proxy stops, and is disabled.

120

Perform 15.16 “To upgrade a Release 22.6 or earlier auxiliary database cluster” (p. 767) to upgrade the standby auxiliary database cluster.

Stop and disable original primary main server [Main1]

121

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$ 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. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to display the nspOS service status:

   ```
   # nspdctl status ↵
   ```

   Information like the following is displayed.

   ```
   Mode:     DR
   Role:     redundancy_role
   DC-Role:  dc_role
   DC-Name:  dc_name
   Registry: IP_address:port
   State:    stopped
   Uptime:   0s
   SERVICE          STATUS
   service_a        inactive
   service_b        inactive
   service_c        inactive
   ```

   You must not proceed to the next step until all NSP services are stopped; if the State is not ‘stopped’, or the STATUS indicator of each listed service is not ‘inactive’, repeat this substep.

122

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:

   ```
   # systemctl disable nspos-nspd.service ↵
   ```

2. Enter the following:

   ```
   # systemctl disable nfmp-main-config.service ↵
   ```

3. Enter the following:

   ```
   # systemctl disable nfmp-main.service ↵
   ```

Upgrade NSP Flow Collector Controllers, Flow Collectors

123

If the system includes one or more NSP Flow Collectors, upgrade each NSP Flow Collector Controller and Flow Collector as described in "NSP Flow Collector and Flow Collector Controller upgrade from Release 22.6 or earlier" (p. 607).

Stop auxiliary servers [Aux1]

124

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 auxstop ↵
   ```

   The auxiliary server stops.

Stop original primary main database [DB1]

125

Log in to the original primary main database [DB1] station as the root user.

126

Open a console window.

127

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 ↵
   ```

128

Perform the following steps.

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

2. Locate the tmpfs file system entry.
3. Remove the noexec option so that the entry reads as follows:

   ```
   tmpfs /dev/shm tmpfs nodev 0 0
   ```
4. Save and close the /etc/fstab file.
5. Enter the following to remount the /dev/shm partition:

   ```
   # mount -o remount /dev/shm ↵
   ```

Upgrade auxiliary database, if not redundant

129

If the system does not include an auxiliary database, go to Step 133.

130

If the system includes a standalone auxiliary database, perform the following steps.

1. Perform 15.16 “To upgrade a Release 22.6 or earlier auxiliary database cluster” (p. 767).
2. Go to Step 133.

Enable maintenance mode for auxiliary database agent

131

If the system includes redundant auxiliary database clusters, and the NFM-P is not in a shared-mode NSP deployment, enter the following as the root user on the newly upgraded main server [Main2]:

```
# sed -i -r 's/("maintenance-mode"\s*:\s*)false/\1true/g'
/opt/nsp/os/auxdb-agent/conf/nspos-auxdb-agent-overrides.json ↵
```

The auxiliary database cluster enters maintenance mode within approximately one minute.

Stop former primary auxiliary database cluster

132

If the system includes redundant auxiliary database clusters, perform the following steps on one station in the upgraded former primary cluster.

1. Log in as the root user.
2. Open a console window.
3. Enter the following:

   ```
   # cd /opt/nsp/nfmp/auxdb/install/bin ↵
   ```
4. Enter the following to stop the auxiliary database:

   ```
   # ./auxdbAdmin.sh stop ↵
   ```
5. Enter the following to display the auxiliary database status:

   ```
   # ./auxdbAdmin.sh status ↵
   ```

Information like the following is displayed:

```
Database status
Node       | Host           | State | Version | DB
------------+---------------+-------+---------+-------
node_1 | internal_IP_1 | STATE | version | db_name
node_2 | internal_IP_2 | STATE | version | db_name
.
.
.
node_n | internal_IP_n | STATE | version | db_name
      Output captured in log_file
```

The cluster is stopped when each *STATE* entry reads DOWN.

6. Repeat substep 5 periodically until the cluster is stopped.

   Note: You must not proceed to the next step until the cluster is stopped.

Start new primary main server [Main2]

133

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 the *NSP 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.

134

If you have enabled CAC for NFM-P client access, download the casmetadata.xml file from the following URL, and then import the file into the ADFS server relying-trust-party:

https://*server*/cas/sp/metadata

where *server* is the main server IP address or hostname

After the download, the casmetadata.xml file is available in the following directory on the main server:

/opt/nsp/os/tomcat/conf/cas/saml

135

If you have enabled Windows Active Directory access using the AUTHENTICATED type of LDAP server, perform the following steps.

1. Use the NSP Session Manager REST API to add the LDAP server bind credentials; see the Network Developer Portal for information.
2. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to restart the local nspos-tomcat service:

   Note: The service restart may take a few minutes, during which NFM-P GUI and REST client access is degraded. General NFM-P operation is unaffected.

```
# systemctl restart nspos-tomcat ↵
```

136

Specify the memory requirement for GUI clients based on the type of network that the NFM-P is to manage.

1. Enter the following:

```
bash$ ./nmsdeploytool.bash clientmem -option ↵
```

   where *option* is one of the following:

   - m—medium, for management of limited-scale network

- l—large, for a network of 15 000 or more NEs

2. Record the setting, which is not preserved through an upgrade, for future use.
3. Enter the following to commit the configuration change:

```
bash$ ./nmsdeploytool.bash deploy ↵
```

Start auxiliary servers [Aux2]

137

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.

Activate upgraded former standby auxiliary database cluster

138

If the system does not include redundant auxiliary database clusters, go to Step 141.

139

Perform the following steps on each station in the upgraded former standby auxiliary database cluster.

1. Log in as the root user on the station.
2. Open a console window.
3. Enter the following sequence of commands to enable the database services:

```
# systemctl enable nspos-auxdb.service ↵
# systemctl enable nspos-auxdbproxy.service ↵
# systemctl enable vertica_agent.service ↵
# systemctl enable verticad.service ↵
```

The services are enabled.

4. Enter the following to start the database proxy:

```
# systemctl start nspos-auxdbproxy.service ↵
```

The proxy starts.

140

Perform one of the following to activate the former standby auxiliary database cluster, after which the cluster assumes the primary role.

a. If the NFM-P is in a shared-mode NSP deployment, issue the following REST API call:

> **Note:** In order to issue a REST API call, you require a REST token; see this tutorial on the Network Developer Portal for information.

```
POST https://{{address}}:8545/restconf/data/auxdb:/clusters/cluster=
cluster_N/activate
```

where

address is the advertised address of the primary NSP cluster

N is the auxiliary database cluster number

The following is the request body:

```
{
  "auxdb:input" : {
    "force": true
  }
}
```

The cluster is activated.

b. If the NFM-P is not in a shared-mode NSP deployment, enter the following as the root user on the new primary main server station:

```
# nspdctl auxdb activate cluster_N --force ↵
```

where *N* is the auxiliary database

A message like the following is displayed:

```
Auxiliary database activation request submitted for [cluster_N]
```

Upgrade analytics servers

141

If the system includes one or more NSP analytics servers, upgrade each analytics server as described in “NSP analytics server upgrade from Release 22.6 or earlier” (p. 616).

Enable GUI client

142

You require an NFM-P GUI client to complete the procedure; see the following for information:

> **Note:** A client delegate server installation typically takes more time than the other options. A single-user client or client delegate server upgrade is recommended if your maintenance period is limited.

- “NFM-P single-user GUI client installation” (p. 585)

- "NFM-P single-user GUI client upgrade from Release 22.6 or earlier" (p. 782)
- "NFM-P client delegate server installation" (p. 591)
- "NFM-P client delegate server upgrade from Release 22.6 or earlier" (p. 790)

Test upgraded system using GUI client

143

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].

Uninstall original primary database [DB1]

144

Enter the following to uninstall the original primary main database:

```
# yum remove nsp-nfmp-main-db nsp-nfmp-oracle ↵
```

The yum utility resolves any dependencies and displays the following prompt:

```
Installed size: nn G
Is this ok [y/N]:
```

145

Enter y. The following is displayed as the packages are removed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
Uninstalling the NFM-P package...
```

As each package removal completes, the following is displayed:

```
Complete!
```

Install new standby main database [DB1]

146

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 Planning Guide*.

For information about deploying the RHEL OS using an NSP OEM disk image, see 2.2.2 “NSP disk-image deployment” (p. 28).

Note: After the upgrade, the station is the new standby main database station.

147

Log in as the root user on the station that is commissioned as the main database [DB1] station.

148

Perform one of the following.

a. If the main server and database are collocated on one station, perform the following steps.

1. Enter the following:

```
# mkdir /opt/importConfigs ↵
```

2. Transfer the mainserverBackupConfigs.tar.gz file created in Step 32 of 15.8 “To prepare for an NFM-P system upgrade from Release 22.6 or earlier” (p. 634) to the /opt/importConfigs directory.

3. Transfer the following downloaded installation files to an empty directory on the collocated 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.

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
- nsp-nfmp-nodeexporter-*R.r.p*-rel.*v*.rpm, if downloaded

Note: In subsequent steps, the directory is called the NFM-P software directory.

149

Transfer the following downloaded file to an empty directory on the main database station:

- OracleSw_PreInstall.sh

150

Open a console window.

151

Navigate to the directory that contains the OracleSw_PreInstall.sh file.

152

Enter the following:

```
# chmod +x OracleSw_PreInstall.sh ↵
```

153

Enter the following:

```
# ./OracleSw_PreInstall.sh ↵
```

ℹ **Note:** A default value is displayed in brackets []. To accept the default, press ↵.

ℹ **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]:
```

154

Enter Yes. The following prompt is displayed:

```
Enter the Oracle dba group name [group]:
```

155

Enter a group name.

ℹ **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:
```

156

Enter a username.

ℹ **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/oracle19].

Checking or Creating the Oracle user home directory
/opt/nsp/nfmp/oracle19...

Checking user username...

Adding username...

Changing ownership of the directory /opt/nsp/nfmp/oracle19 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:
```

157

Enter a password. The following prompt is displayed:

```
Re-enter new Password:
```

158

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]:
```

159

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.
```

160

When the script execution is complete, enter the following to reboot the station:

```
# systemctl reboot ↵
```

The station reboots.

161

When the reboot is complete, log in as the root user on the station that is commissioned as the main database [DB1] station.

162

Open a console window.

163

Navigate to the NFM-P software directory.

Note: Ensure that the directory contains only the installation files.

164

Enter the following:

```
# chmod +x * ↵
```

165

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G

Installed size: nn G

Is this ok [y/d/N]:
```

166

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:

Running transaction check

Transaction check succeeded.

Running transaction test

Transaction test succeeded.

Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

167

Configure the database as a standby database; see 14.9 “NFM-P samconfig utility” (p. 432) for information about using samconfig.

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>`.

168

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; see 14.9 “NFM-P samconfig utility” (p. 432) for information about using the samconfig utility.
3. Configure one or more parameters, if required.
4. When you are certain that the configuration is correct, enter the following:

   ```
   <db configure> back ↵
   ```

   The prompt changes to `<db>`.

169

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.
```

170

When the database creation is complete, enter the following:

```
<db> exit ↵
```

The samconfig utility closes.

Reinstantiate standby database

171

Log in to an NFM-P GUI client as the admin user.

172

Choose Administration→System Information from the main menu. The System Information form opens.

173

Click Re-Instantiate Standby.

174

Click Yes to confirm the action. The reinstantiation begins, and the GUI status bar displays reinstantiation information.

> **Note:** Database reinstantiation 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.

175

When the reinstantiation is complete, close the System Information form.

Upgrade former primary auxiliary database cluster

176

If the system includes redundant auxiliary database clusters, perform 15.16 “To upgrade a Release 22.6 or earlier auxiliary database cluster” (p. 767) on the former primary auxiliary database cluster.

Upgrade original primary main server [Main1]

177

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 Planning Guide*.

For information about deploying the RHEL OS using an NSP OEM disk image, see 2.2.2 “NSP disk-image deployment” (p. 28).

Note: After the upgrade, the station is the new standby main server station.

178

Log in as the root user on the station that is commissioned as the main server [Main1] station.

179

Open a console window.

180

If the main server and database are on separate stations, perform the following steps.

1. Enter the following:

   ```
   # mkdir /opt/importConfigs ↵
   ```

2. Transfer the mainserverBackupConfigs.tar.gz file created in Step 32 of 15.8 “To prepare for an NFM-P system upgrade from Release 22.6 or earlier” (p. 634) to the /opt/importConfigs directory.

181

Perform one of the following.

a. If the main server and database are collocated on one station, go to Step 186.

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
- nsp-nfmp-nodeexporter-*R.r.p*-rel.*v*.rpm, if downloaded

Note: In subsequent steps, the directory is called the NFM-P software directory.

182

Navigate to the NFM-P software directory.

183

Enter the following:

```
# chmod +x * ↵
```

184

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

185

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

Configure new standby main server [Main1]

186

Enter the following; see 14.9 “NFM-P samconfig utility” (p. 432) for information about using samconfig:

ℹ **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>
```

187

Enter the following:

```
<main> configure ↵
```

The prompt changes to `<main configure>`.

188

To apply a new or updated NFM-P license, enter the following:

ℹ **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 the *NSP System Administrator Guide*.

```
<main configure> license license_file ↵
```

where *license_file* is the path and file name of the NSP license bundle

189

Enter the following:

```
<main configure> database instance standby_instance back ↵
```

where *standby_instance* is the [DB2] database instance name, which is the standby Instance Name recorded in Step 44 of 15.8 “To prepare for an NFM-P system upgrade from Release 22.6 or earlier” (p. 634)

190

Enter the following:

```
<main configure> redundancy database instance primary_instance back ↵
```

where *primary_instance* is the [DB1] database instance name, which is the primary Instance Name recorded in Step 43 of 15.8 “To prepare for an NFM-P system upgrade from Release 22.6 or earlier” (p. 634)

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

191

Enter the following:

```
<main configure redundancy> back ↵
```

The prompt changes to `<main configure>`.

192

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; see 14.9 “NFM-P samconfig utility” (p. 432) for information about using the samconfig utility.

3. Configure one or more parameters, if required.

   Note: The NFM-P uses the database backup settings to initialize the database during installation only. To change the backup settings after installation, you must use the Database Manager form in the NFM-P client GUI, as described in the *NSP System Administrator Guide*.

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

   ```
   <main configure> back ↵
   ```

   The prompt changes to `<main>`.

193

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

194

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

ℹ **Note:** This station is the new standby main server station.

195

If the NFM-P is part of a shared-mode NSP system and you want to enable mTLS for internal Kafka authentication using two-way TLS, perform the following steps.

ℹ **Note:** Enabling mTLS for internal Kafka authentication is supported only in an NSP deployment that uses separate interfaces for internal and client communication.

ℹ **Note:** The parameter you must configure is displayed only if the ip-list parameter is set to a remote address.

ℹ **Note:** The parameter is configurable only if the **secure** and **internal-certs** parameters in the **nspos** section are set to true.

1. Enter the following:

   ```
   # samconfig -m main ↵
   ```

The following is displayed:

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

2. Enter the following:

   ```
   # configure nspos mtls-kafka-enabled back ↵
   ```

3. Enter the following:

   ```
   <main> apply ↵
   ```

   The configuration is applied.

4. Enter the following:

   ```
   <main> exit ↵
   ```

   The samconfig utility closes.

Restore new standby main server [Main1] data files

196

Transfer the main server data backup .tar.gz file set created in Step 34 of 15.8 “To prepare for an NFM-P system upgrade from Release 22.6 or earlier” (p. 634) to the /opt/nsp/nfmp directory on the [Main1] main server station.

197

Enter the following:

```
# cd /opt/nsp/nfmp ↵
```

198

Enter the following:

```
# chown nsp:nsp *.tar.gz ↵
```

199

Enter the following:

```
# ls *.tar.gz ↵
```

The data backup files are listed.

200

For each listed file, enter the following:

```
# tar -xf filename.tar.gz -C /opt/nsp/nfmp/ ↵
```

where *filename* is a backup timestamp in the format MM-DD-hh-mm

201

Enter the following:

```
# rm -f *.tar.gz ↵
```

202

Enter the following:

```
# chown -R nsp:nsp /opt/nsp/nfmp/lte ↵
```

203

Enter the following:

```
# chown -R nsp:nsp /opt/nsp/nfmp/nebackup ↵
```

204

Enter the following:

```
# chown -R nsp:nsp /opt/nsp/nfmp/nelogs ↵
```

205

Enter the following:

```
# chown -R nsp:nsp /opt/nsp/nfmp/nesoftware ↵
```

206

Enter the following:

```
# chown -R nsp:nsp /opt/nsp/nfmp/os ↵
```

207

Enter the following:

```
# chown -R nsp:nsp /opt/nsp/nfmp/server/script/savedResults ↵
```

Enable Windows Active Directory access

208

If you intend to use Windows Active Directory, or AD, for single-sign-on client access, you must configure LDAP remote authentication for AD; otherwise, go to Step 227.

Open the following file as a reference for use in subsequent steps:

/opt/nsp/os/install/examples/config.yml

Note: Consider the following.

- The NFM-P does not assign a default user group to users of a remote authentication source that you define for Windows AD; the authentication source must provide the user group attributes.
- Windows AD supports the following LDAP server types for remote authentication:

  AD—The user group of an AD user is derived from the group_base_dn attribute in the server configuration; group search filters are not supported.

  AUTHENTICATED—The server configuration must include bind credentials; group search filters are supported. After NFM-P initialization, you add the AD server bind credentials to the NSP password vault using the NSP Session Manager REST API.

209

Locate the section that begins with the following lines:

```
#   ldap:
#     enabled: true
#     servers:
#       - type: AUTHENTICATED/AD/ANONYMOUS
#         url: ldaps://ldap.example.com:636
#         security: SSL/STARTTLS/NONE
```

210

Open the following file using a plain-text editor such as vi:

/opt/nsp/os/install/config.json

211

Locate the section that begins with the following line:

```
"sso": {
```

The section has one subsection for each type of SSO access.

Note: You can enable multiple remote authentication methods such as LDAP and RADIUS in the config.json file, or by using the NFM-P GUI. Using the GUI also allows you to specify the order in which the methods are tried during login attempts; however, no ordering is applied to multiple methods enabled in the config.json file.

212

In the **sso** section, create an **ldap** subsection as shown below using the parameter names from the **ldap** section of config.yml and the required values for your configuration.

The following example shows the LDAP configuration for two AD servers:

```
"ldap": {
"enabled": true,
"servers": [
{
"type": "auth_type",
"url": "ldaps://server1:port",
"server1_parameter_1": "value",
"server1_parameter_2": "value",
.
.
"server1_parameter_n": "value",
},
{
"type": "auth_type",
"url": "ldaps://server2:port",
"server2_parameter_1": "value",
"server2_parameter_2": "value",
.
.
"server2_parameter_n": "value",
},
}]
}
```

where *auth_type* is AD or AUTHENTICATED

213

Save and close the files.

214

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

215

Enter the following:

```
<main> apply ↵
```

The AD LDAP configuration is applied.

216

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Enable CAC access

217

If you do not intend to enable Common Access Card, or CAC, technology for NFM-P client access, go to Step 227.

218

Download the federationmetadata.xml from the following ADFS link:

https://*ADFS_server_name*/FederationMetadata/2007-06/federationmetadata.xml

where *ADFS_server_name* is the ADFS server FQDN

219

Add an ADFS server entry to the /etc/hosts file on the main server.

1. Open the /etc/hosts file using a plain-text editor such as vi.
2. Add the following line below the line that contains the main server IP address:

   ```
   IP_address FQDN
   ```

   where

   IP_address is the IP address of the ADFS server

   FQDN is the FQDN of the ADFS server
3. Save and close the file.

220

In order to enable CAC for client access, you must configure Active Directory Federation Services, or ADFS.

Open the following file using a plain-text editor such as vi:

/opt/nsp/os/install/config.json

221

In the **sso** section, create an **saml2** subsection as shown below using the parameter names from the **saml2** section of config.yml and the required values for your configuration.

The following example shows the ADFS configuration.

Note: You must preserve the lead spacing of each line.

```
  "sso" : {
    "saml2": {
       "enabled": true,
       "service_provider_entity_id": "NFM-P_identifier",
       "service_provider_metadata_filename": "casmetadata.xml",
       "maximum_authentication_lifetime": 3600,
       "accepted_skew": 300,
       "destination_binding": "urn:oasis:names:tc:SAML:2.0:bindings:
HTTP-Redirect",
       "identity_provider_metadata_path": "ADFS_metadata_file",
       "authn_context_class_ref": "urn:oasis:names:tc:SAML:2.0:ac:
classes:TLSClient",
       "authn_context_comparison_type": "minimum",
       "name_id_policy_format": "urn:oasis:names:tc:SAML:1.1:
nameid-format:unspecified",
       "force_auth": true,
       "passive": false,
```

```
       "wants_assertions_signed": false,
       "wants_responses_signed": false,
       "all_signature_validation_disabled": false,
       "sign_service_provider_metadata": false,
       "principal_id_attribute": "UPN",
       "use_name_qualifier": false,
       "provider_name": "ADFS_server_URI",
       "requested_attributes": [{
         "name": "http://schemas.xmlsoap.
org/ws/2005/05/identity/claims/emailaddress",
          "friendly_name": "E-Mail Address",
          "name_format": "urn:oasis:names:tc:SAML:2.0:attrname-format:
uri",
          "required": false
      } ],
       "mapped_attributes": [{
           "name": "http://schemas.xmlsoap.org/claims/Group",
           "mapped_to": "authorizationProfile"
      }, {
           "name": "http://schemas.xmlsoap.
org/ws/2005/05/identity/claims/upn",
           "mapped_to": "upn"
      } ]
    },
```

222

Configure the following parameters; leave all other parameters at the default:

- "service_provider_entity_id": "*NFM-P_identifier*"
- "identity_provider_metadata_path": "*ADFS_metadata_file*"
- "provider_name": "*ADFS_server_name*"

NFM-P_identifier is the unique ADFS Relying Trust Party identifier

*ADFS_metadata_fil*e is the absolute path of the ADFS metadata XML file, for example, /opt/federationmetadata.xml

ADFS_server_name is the ADFS server FQDN

223

Save and close the files.

224

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

225

Enter the following:

```
<main> apply ↵
```

The ADFS configuration is applied.

226

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Configure WS-NOC integration

227

If the NFM-P is integrated with an WS-NOC system, open the following file with a plain-text editor such as vi; otherwise, go to Step 237:

/opt/nsp/os/install/examples/config.json

228

Copy the following section:

```
  "nfmt": {
    "primary_ip": "",
    "standby_ip": "",
    "username": "",
    "password": "",
    "cert_provided": false
  },
```

229

Close the file.

230

Open the following file with a plain-text editor such as vi:

/opt/nsp/os/install/config.json

231

Paste in the copied section.

232

Configure the required parameters to enable the WS-NOC integration:

- primary_ip—the primary WS-NOC server IP address
- standby_ip—the standby WS-NOC server IP address
- username—the username required for WS-NOC access
- password—the password required for WS-NOC access
- cert_provided—whether a TLS certificate is used

233

Save and close the file.

234

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

235

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

236

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Start new standby main server [Main1]

237

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 the *NSP 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.

238

If you have enabled CAC for NFM-P client access, download the casmetadata.xml file from the following URL, and then import the file into the ADFS server relying-trust-party:

https://*server*/cas/sp/metadata

where *server* is the main server IP address or hostname

After the download, the casmetadata.xml file is available in the following directory on the main server:

/opt/nsp/os/tomcat/conf/cas/saml

239

If you have enabled Windows Active Directory access using the AUTHENTICATED type of LDAP server, perform the following steps.

1. Use the NSP Session Manager REST API to add the LDAP server bind credentials; see the Network Developer Portal for information.

2. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to restart the local nspos-tomcat service:

   Note: The service restart may take a few minutes, during which NFM-P GUI and REST client access is degraded. General NFM-P operation is unaffected.

   ```
   # systemctl restart nspos-tomcat ↵
   ```

240

Specify the memory requirement for GUI clients based on the type of network that the NFM-P is to manage.

1. Enter the following:

   ```
   bash$ ./nmsdeploytool.bash clientmem -option ↵
   ```

   where *option* is one of the following:

   - m—medium, for management of limited-scale network

- l—large, for a network of 15 000 or more NEs

2. Record the setting, which is not preserved through an upgrade, for future use.
3. Enter the following to commit the configuration change:

```
bash$ ./nmsdeploytool.bash deploy ↵
```

241

Close the console window.

Upgrade auxiliary servers [Aux1]

242

If the system includes auxiliary servers, perform 15.15 “To upgrade a Release 22.6 or earlier NFM-P auxiliary server” (p. 760) on each [Aux1] auxiliary server station.

Start auxiliary servers [Aux1]

243

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.

Disable maintenance mode for auxiliary database agents

244

If the system does not include an auxiliary database, go to Step 248.

245

If the system includes redundant auxiliary database clusters, perform one of the following to put each agent in active mode.

a. If the NFM-P is in a shared-mode NSP deployment, perform the following steps.

1. Log in as the root user on the NSP cluster host in the primary data center.
2. Enter the following to set the nspos-auxdb-agent mode to active:

```
# kubectl patch configmap/nspos-auxdb-agent-overrides --type=merge
-p '{"data":{"nspos-auxdb-agent-overrides.json":"{\"auxDbAgent\":
{\"config\":{\"maintenance-mode\":false}}}"}}' ↵
```

3. Enter the following to restart the nspos-auxdb-agent:

```
# kubectl delete pod `kubectl describe pods | grep -P ^^Name: |
grep -oP nspos-auxdb-agent[-a-zA-Z0-9]+` ↵
```

4. Log in as the root user on the NSP cluster host in the standby data center.

5. Enter the following to set the nspos-auxdb-agent mode to active:

```
# kubectl patch configmap/nspos-auxdb-agent-overrides --type=merge
-p '{"data":{"nspos-auxdb-agent-overrides.json":"{\"auxDbAgent\":
{\"config\":{\"maintenance-mode\":false}}}"}}' ↵
```

b. If the NFM-P is not in a shared-mode NSP deployment, enter the following as the root user on the new primary main server [Main2]:

```
# sed -i -r 's/("maintenance-mode"\s*:\s*)true/\1false/g'
/opt/nsp/os/auxdb-agent/conf/nspos-auxdb-agent-overrides.json ↵
```

The cluster enters active mode within approximately one minute.

Verify auxiliary database status

246

You must verify that the standalone or new primary auxiliary database cluster is in active mode.

a. If the NFM-P is in a shared-mode NSP deployment, issue the following REST API call:

Note: In order to issue a REST API call, you require a REST token; see this tutorial on the Network Developer Portal for information.

```
GET /data/auxdb:/auxdb-agent HTTP/1.1
```

Request body:

```
Host: address:8545
Content-Type: application/json
Authorization: bearer_and_token_from_session_manager
```

where *address* is the advertised address of the primary NSP cluster

The cluster is in active mode if the REST response includes ACTIVE.

b. If the NFM-P is not in a shared-mode NSP deployment, enter the following as the root user on the new primary main server [Main2]:

```
# /opt/nsp/os/nspd/nspdctl auxdb agent-status ↵
```

A status message is displayed.

The cluster is in active mode if the message includes ACTIVE.

247

Perform one of the following to verify the auxiliary database operation.

a. If the NFM-P is in a shared-mode NSP deployment, issue the following REST API call:

Note: In order to issue a REST API call, you require a REST token; see this tutorial on the Network Developer Portal for information.

GET https://{{*address*}}:8545/restconf/data/auxdb:/clusters

where *address* is the advertised address of the primary NSP cluster

The call returns auxiliary database cluster status information like the following, which is the output for redundant clusters; if each mode and status value are not as shown below, contact technical support.

```
<HashMap>
    <clusters>
        <cluster>
            <name>cluster_M</name>
            <mode>ACTIVE</mode>
            <status>UP</status>
            <nodes>
                <external-ip>203.0.113.101</external-ip>
                <internal-ip>10.1.2.101</internal-ip>
                <status>UP</status>
            </nodes>
            <nodes>
                <external-ip>203.0.113.102</external-ip>
                <internal-ip>10.1.2.102</internal-ip>
                <status>UP</status>
            </nodes>
            <nodes>
                <external-ip>203.0.113.103</external-ip>
                <internal-ip>10.1.2.103</internal-ip>
                <status>UP</status>
            </nodes>
        </cluster>
        <cluster>
            <name>cluster_N</name>
            <mode>STANDBY</mode>
            <status>ON_STANDBY</status>
            <nodes>
                <external-ip>203.0.113.104</external-ip>
                <internal-ip>10.1.2.104</internal-ip>
                <status>READY</status>
            </nodes>
            <nodes>
```

```
                <external-ip>203.0.113.105</external-ip>
                <internal-ip>10.1.2.105</internal-ip>
                <status>READY</status>
            </nodes>
            <nodes>
                <external-ip>203.0.113.106</external-ip>
                <internal-ip>10.1.2.106</internal-ip>
                <status>READY</status>
            </nodes>
        </cluster>
    </clusters>
</HashMap>
```

b. If the NFM-P is not in a shared-mode NSP deployment, enter the following as the root user on the primary main server [Main2]:

```
# nspdctl auxdb status ↵
```

Cluster status information such as the following is displayed.

Note: The Output for a standalone auxiliary database shows only one cluster.

```
CLUSTER    DC-ROLE   STATE
cluster_M  ACTIVE    UP
NODE           INTERNAL IP   STATE
203.0.113.101  10.1.2.101    UP
203.0.113.102  10.1.2.102    UP
203.0.113.103  10.1.2.103    UP
CLUSTER    DC-ROLE   STATE
cluster_N  STANDBY   ON_STANDBY
NODE           INTERNAL IP    STATE
203.0.113.104  10.1.2.104     READY
203.0.113.105  10.1.2.105     READY
203.0.113.106  10.1.2.106     READY
```

If each STATE value is not as shown above, contact technical support.

Check post-upgrade disk space

248

If you are performing a trial upgrade on a lab system in advance of a live upgrade, you must check the available capacity of the disk partitions on each component against the values recorded in Step 1.

Perform the following steps on each of the following stations:

- main server
- auxiliary server
- main database
- auxiliary database

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following:

   ```
   # df -kh ↵
   ```

   The usage information for each partition is displayed.
4. Record the information for each NFM-P partition; see the tables in Chapter 2, “NSP disk setup and partitioning” for the partition names and required capacities.
5. Compare the partition values with the values recorded in Step 1.
6. If the disk usage on an NFM-P partition approaches 80% or has increased substantially, you may need to add disk capacity before you attempt the upgrade on a live system. Contact technical support for assistance.

Install or upgrade single-user GUI clients

249

As required, install or upgrade additional single-user GUI clients; see the following for information:

- “NFM-P single-user GUI client installation” (p. 585)
- “NFM-P single-user GUI client upgrade from Release 22.6 or earlier” (p. 782)

Install or upgrade client delegate servers

250

As required, install or upgrade client delegate servers; see the following for information:

- “NFM-P client delegate server installation” (p. 591)
- “NFM-P client delegate server upgrade from Release 22.6 or earlier” (p. 790)

Stop PKI server

251

If no other components are to be deployed, stop the PKI server by entering Ctrl+C in the console window.

Restore TLS version and cipher support configuration

252

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, see the *NSP System Administrator Guide* for information about how to restore the TLS version and cipher support settings.

Note: TLS 1.0 and 1.1 are disabled by default after an upgrade. If either version is enabled before an NFM-P system upgrade and required after the upgrade, you must re-enable the version support after the upgrade.

Configure and enable firewalls

253

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 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 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 from Release 22.6 or earlier

15.15 To upgrade a Release 22.6 or earlier NFM-P auxiliary server

15.15.1 Description

The following steps describe how to upgrade the Release 22.6 or earlier 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 performs only SNMP statistics 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

15.15.2 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 Planning Guide*.

Note: The hostname and IP address of a replacement station must match the hostname and IP address of the station being replaced.

For information about deploying the RHEL OS using an NSP OEM disk image, see 2.2.2 “NSP disk-image deployment” (p. 28).

Back up configuration

2

Log in as the root user on the existing auxiliary server station.

3

Download the following NFM-P installation file to an empty local directory on the existing auxiliary server station:

- linuxMigration.sh

4

Open a console window.

5

Enter the following sequence of commands to disable the auxiliary server services:

```
# systemctl disable nfmp-aux.service ↵
# systemctl disable nfmp-aux-config.service ↵
```

6

Navigate to the directory that contains the downloaded linuxMigration.sh file.

7

Enter the following:

```
# chmod +x linuxMigration.sh ↵
```

8

Enter the following:

```
# ./linuxMigration.sh -t aux ↵
```

The following is displayed:

```
Backup auxiliary server config contents.
```

When the backup is complete, the following is displayed:

```
Please backup/transfer /opt/importConfigs/auxserverBackupConfigs.
tar.gz to a secure location.

You must restore this file to the exact same directory location on the
RHEL 8 station before installing the rpm(s).
```

The script creates the following file on the station:

- /opt/importConfigs/auxserverBackupConfigs.tar.gz

9

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

10

If the auxiliary server is running, stop the auxiliary server.

1. Enter the following to switch to the nsp user:

   ```
   # su - nsp ↵
   ```

2. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/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.

5. Enter the following to switch back to the root user:

   ```
   # exit ↵
   ```

11

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]:
```

12

Enter y. The following is displayed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
Uninstalling the NFM-P package...
```

As each package removal completes, the following is displayed:

```
Complete!
```

13

Return to Step 11 as required to remove the next package in the sequence.

Recommission existing station, if required

14

If you are re-using the auxiliary server station, recommission the station according to the platform specifications in this guide and in the *NSP Planning Guide*.

For information about deploying the RHEL OS using an NSP OEM disk image, see 2.2.2 “NSP disk-image deployment” (p. 28).

Install auxiliary server software

15

Log in as the root user on the station that is commissioned as the auxiliary server station.

16

Enter the following:

```
# mkdir /opt/importConfigs ↵
```

17

Transfer the auxserverBackupConfigs.tar.gz file created in Step 8 to the /opt/importConfigs directory.

18

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
- nsp-nfmp-nodeexporter-*R.r.p*-rel.*v*.rpm, if the NFM-P is in a shared-mode deployment and you want to forward NFM-P system metrics to the NSP

where

R.r.p is the NSP release identifier, in the form *MAJOR.minor.patch*

v is a version identifier

19

Navigate to the directory that contains the NFM-P installation files.

Note: Ensure that the directory contains only the installation files.

20

Enter the following:

```
# chmod +x * ↵
```

21

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

22

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

23

Enter the following; see 14.9 “NFM-P samconfig utility” (p. 432) for information about using samconfig:

```
# samconfig -m aux ↵
```

The following is displayed:

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

24

Enter the following:

```
<aux> configure tls ↵
```

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

25

Perform one of the following; see Table 15-3, “Auxiliary server parameters — `tls`” (p. 765) for parameter information.

a. If you are using the PKI server to generate the internal and external certificates; enter the following commands:

```
no keystore-file
no keystore-pass
```

b. If you are using custom external certificates and PKI-server generated internal certificates;

enter the following commands:

```
keystore-file keystore_file
keystore-pass keystore_password
```

Table 15-3 Auxiliary server parameters — tls

Parameter	Description
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
pki-server	The PKI server IP address or hostname Default: —
pki-server-port	The TCP port on which the PKI server listens for and services requests Default: 2391
regenerate-certs	Whether to regenerate the internal TLS certificates Certificate regeneration is required when the current certificates are about to expire, or a new internal root certificate is available. A new internal root certificate is available when the root certificate is reset, or when the PKI server is run on a station other than the station used for the previous certificate deployment. Default: false

26

Enter the following:

```
<aux configure tls> exit ↵.
```

The prompt changes to `<aux>`.

27

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; see 14.9 “NFM-P samconfig utility” (p. 432) for information about using the samconfig utility.

3. If required, modify one or more parameter values, and then enter **back** ↵.

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.

28

Close the console window.

END OF STEPS

Auxiliary database upgrade from Release 22.6 or earlier

15.16 To upgrade a Release 22.6 or earlier auxiliary database cluster

15.16.1 Description

The following procedure is performed as part of a standalone or redundant system upgrade from Release 22.6 or earlier.

In a redundant NFM-P system upgrade, the standby components are upgraded while the primary components remain operational. The upgraded standby components then assume the primary role while the former primary components are upgraded.

If a redundant system includes a redundant auxiliary database, the network outage during a redundant system upgrade is limited to the initialization time of the upgraded former standby components.

If a redundant system includes a standalone auxiliary database, the network outage during a redundant system upgrade includes the auxiliary database upgrade duration.

Upgrade process

A typical NSP component upgrade from Release 22.6 or earlier involves moving from RHEL 7 to RHEL 8. The process restores the component database backup on the new RHEL 8 station before upgrading the NSP software.

The process for upgrading a Release 22.6 or earlier auxiliary database is somewhat different. The auxiliary database software is upgraded in place on the RHEL 7 cluster, and then the database is restored on the RHEL8 stations.

Note: CPU frequency scaling 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” CPU frequency scaling governor on a station.

Setting CPU frequency scaling to “performance” effectively disables the function, so may result in greater energy consumption by a station.

Note: Enabling TLS on an auxiliary database is not supported during an upgrade.

Note: You require the following user privileges on each auxiliary database station:

- root
- samauxdb

Note: Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

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

15.16.2 Steps

Obtain software

1

Download the following installation files to an empty local directory on a station that is reachable by each auxiliary database station in the cluster:

- nspos-auxdb-*R*.*r*.*p*-rel.*v*.rpm
- VerticaSw_PreInstall.sh
- nspos-jre-*R*.*r*.*p*-rel.*v*.rpm
- vertica-*R*.*r*.*p*-rel.tar

where

R.*r*.*p* is the NSP release identifier, in the form *MAJOR*.*minor*.*patch*

v is a version number

Commission new stations, if required

2

If you are deploying the auxiliary database on one or more new stations, perform the following steps.

For information about deploying the RHEL OS using an NSP OEM disk image, see 2.2.2 “NSP disk-image deployment” (p. 28).

Note: The IP addresses on the interfaces of a new auxiliary database station must match the addresses on the station that it replaces.

1. Commission each station according to the platform specifications in this guide and in the *NSP Planning Guide*.
2. Perform 3.3 “To apply the RHEL 8 swappiness workaround” (p. 66) on the station.

Back up database

3

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.

If you are upgrading a standalone auxiliary database, or the standby cluster in a redundant auxiliary database, 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 1 Gb/s link to the location is required; if achievable, a higher-capacity link is recommended.

For auxiliary database backup information, see the *NSP System Administrator Guide* for the installed release.

Stop cluster

4

Log in as the root user on an auxiliary database station in the cluster that is being upgraded.

5

Open a console window.

6

Enter the following:

```
# cd /opt/nsp/nfmp/auxdb/install/bin ↵
```

7

Enter the following to stop the auxiliary database:

```
# ./auxdbAdmin.sh stop ↵
```

8

Enter the following to display the auxiliary database status:

```
# ./auxdbAdmin.sh status ↵
```

Information like the following is displayed:

```
Database status
Node       | Host          | State | Version | DB
------------+---------------+-------+---------+-------
node_1 | internal_IP_1 | STATE | version | db_name
node_2 | internal_IP_2 | STATE | version | db_name
.
.
.
node_n | internal_IP_n | STATE | version | db_name
      Output captured in log_file
```

The cluster is stopped when each *STATE* entry reads DOWN.

9

Repeat Step 8 periodically until the cluster is stopped.

ℹ **Note:** You must not proceed to the next step until the cluster is stopped.

Prepare all stations for upgrade

10

Perform Step 12 to Step 28 on each auxiliary database station in the cluster that is being upgraded.

11

Go to Step 29.

Prepare individual station for upgrade

12

Log into the auxiliary database station as the root user.

13

Open a console window.

14

Enter the following sequence of commands to stop the auxiliary database services:

```
# systemctl stop nfmp-auxdb.service ↵
# systemctl stop vertica_agent.service ↵
# systemctl stop verticad.service ↵
```

15

Enter the following sequence of commands to disable the database services:

```
# systemctl disable nfmp-auxdb.service ↵
# systemctl disable nfmp-auxdbproxy.service ↵
# systemctl disable vertica_agent.service ↵
# systemctl disable verticad.service ↵
```

16

Transfer the downloaded installation files to an empty directory on the station.

ℹ **Note:** You must ensure that the directory is empty.

ℹ **Note:** In subsequent steps, the directory is called the software directory.

17

Navigate to the software directory.

Note: The directory must contain only the installation files.

18

Enter the following:

```
# chmod +x * ↵
```

19

Enter the following:

```
# ./VerticaSw_PreInstall.sh ↵
```

Information like the following is displayed:

```
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...
```

20

Enter the following to reboot the station:

```
# systemctl reboot ↵
```

The station reboots.

21

When the reboot is complete, log in to the station as the root user.

22

Open a console window.

23

Enter the following:

```
# cd /opt/nsp/nfmp/auxdb/install/bin ↵
```

24

Enter the following to display the auxiliary database status:

```
# ./auxdbAdmin.sh status ↵
```

Information like the following is displayed:

```
Database status

Node       | Host          | State | Version | DB

------------+---------------+-------+---------+-------

node_1 | internal_IP_1 | STATE | version | db_name

node_2 | internal_IP_2 | STATE | version | db_name

.

.

.

node_n | internal_IP_n | STATE | version | db_name
```

```
      Output captured in log_file
```

25

if any *STATE* entry is not DOWN, perform the following steps.

1. Enter the following to stop the auxiliary database:

   ```
   # ./auxdbAdmin.sh stop ↵
   ```

2. Repeat Step 24 periodically until each *STATE* entry reads DOWN.

   Note: You must not proceed to the next step until each *STATE* entry reads DOWN.

26

Navigate to the software directory.

27

Enter the following:

```
# yum install nspos-*.rpm ↵
```

The yum utility resolves any package dependencies, and displays the following prompt for each package:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

28

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

Upgrade database

29

Log in as the root user on an auxiliary database station in the cluster that is being upgraded.

30

Open a console window.

31

Enter the following:

```
# cd /opt/nsp/nfmp/auxdb/install/bin ↵
```

32

Enter the following:

```
# ./auxdbAdmin.sh upgrade tar_file ↵
```

where *tar_file* is the absolute path and filename of the vertica-*R.r.p*-rel.tar file in the software directory

The following prompt is displayed:

```
Updating Vertica - Please perform a backup before proceeding with this option

Do you want to proceed (YES/NO)?
```

33

Enter YES ↵.

The following prompt is displayed:

```
Please enter auxiliary database dba password [if you are doing initial setup for auxiliary database, press enter]:
```

34

Enter the dba password.

The following prompt is displayed:

```
Please verify auxiliary database dba password:
```

35

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
```

36

Enter the following to display the auxiliary database status:

```
# ./auxdbAdmin.sh status ↵
```

Information like the following is displayed:

```
Database status

Node        | Host           | State | Version | DB

------------+----------------+-------+---------+-------
```

```
node_1 | internal_IP_1 | STATE | version | db_name
node_2 | internal_IP_2 | STATE | version | db_name
.
.
.
node_n | internal_IP_n | STATE | version | db_name
       Output captured in log_file
```

The cluster is running when each *STATE* entry reads UP.

37

Repeat Step 36 periodically until the cluster is running.

Note: You must not proceed to the next step until the cluster is running.

Back up database for migration to new OS version

38

If no backup has previously been performed on the cluster, for example, if the cluster has always had the standby role, perform the following steps.

1. Open a console window on a station in the current cluster.
2. Copy the following file from a station in the peer cluster to the same directory on the current station:

   backup path/samAuxDbBackup_restore.conf

   where *backup_path* is the backup location specified in Step 3
3. Enter the following:

   ```
   # chown samauxdb:samauxdb backup_path/samAuxDbBackup_restore.conf ↵
   ```
4. Enter the following:

   ```
   # ./auxdbAdmin.sh status ↵
   ```

   Information like the following is displayed:

   ```
   Database status
   Node         | Host            | State | Version | DB
   ------------+---------------+-------+---------+-------
   node_1 | internal_IP_1 | STATE | version | db_name
   node_2 | internal_IP_2 | STATE | version | db_name
   .
   .
   .
   node_n | internal_IP_n | STATE | version | db_name
          Output captured in log_file
   ```

5. Open the following file using a plain-text editor such as vi:

   backup_path/samAuxDbBackup_restore.conf

6. Locate the section that begins with the following:

   ```
   [mapping]
   ```

7. Replace the primary cluster node values in the section with the standby node values displayed in substep 4, as shown in the following example for a three-node cluster:

   ```
   node_1 = [internal_IP_1]:backup_path
   node_2 = [internal_IP_2]:backup_path
   node_3 = [internal_IP_3]:backup_path
   ```

8. Save and close the file.

39

You must back up the auxiliary database data and configuration information to prepare for the migration to the new OS version.

Note: The operation may take considerable time.

Perform the following steps.

1. Enter the following:

   ```
   # ./auxdbAdmin.sh backup /path/samAuxDbBackup_restore.conf ↵
   ```

   where *path* is the backup file path specified in Step 3

   The following prompt is displayed:

   ```
   Please enter auxiliary database dba password [if you are doing
   initial setup for auxiliary database, press enter]:
   ```

2. Enter the dba password.

   The backup operation begins, and messages like the following are displayed.

   ```
   Copying backup config file to /tmp/auxdbadmin-backup-ID
   Backup snapshot name - AuxDbBackUpID_auxdbAdmin
   Starting auxiliary database backup...
   ```

   The backup is complete when the following is displayed:

   ```
   Output captured in
   /opt/nsp/nfmp/auxdb/install/log/auxdbAdmin.sh.timestamp.log
   ```

3. Copy the following file from one auxiliary database station to a secure location that is unaffected by the upgrade activity:

   /opt/nsp/nfmp/auxdb/install/config/install.config

Recommission stations, if required

40

If you are reusing any auxiliary database stations, recommission each station according to the platform specifications in this guide and in the *NSP Planning Guide*.

For information about deploying the RHEL OS using an NSP OEM disk image, see 2.2.2 “NSP disk-image deployment” (p. 28).

Note: You must reformat the following disk partitions:

- root
- /opt/nsp/nfmp/auxdb/data

Install new software, restore database

41

Perform 14.21 “To prepare a station for auxiliary database installation” (p. 558) on each auxiliary database station.

42

Log in as the root user on any auxiliary database station in the cluster.

43

Copy the install.config file saved in Step 39, substep 3 to the following directory:

/opt/nsp/nfmp/auxdb/install/config

44

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.

45

Enter the required password at each prompt. The script installs the software on the station.

46

When the script execution is complete, if you are deploying a geo-redundant auxiliary database, perform the following steps on each auxiliary database station in the current cluster.

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following:

   ```
   bash$ su - samauxdb ↵
   ```

4. Enter the following for each station in the geo-redundant cluster:

   ```
   bash$ ssh-copy-id station_IP ↵
   ```

   where *station_IP* is the IP address of a station in the geo-redundant cluster

47

Stop the auxiliary database.

1. Enter the following on any station in the cluster:

   ```
   # cd /opt/nsp/nfmp/auxdb/install/bin ↵
   ```
2. Enter the following to stop the auxiliary database:

   ```
   # ./auxdbAdmin.sh stop ↵
   ```
3. Enter the following to display the auxiliary database status:

   ```
   # ./auxdbAdmin.sh status ↵
   ```

   Information like the following is displayed:

   ```
   Database status
   Node       | Host          | State | Version | DB
   ------------+---------------+-------+---------+-------
   node_1 | internal_IP_1 | STATE | version | db_name
   node_2 | internal_IP_2 | STATE | version | db_name
   .
   .
   .
   node_n | internal_IP_n | STATE | version | db_name
         Output captured in log_file
   ```

   The cluster is stopped when each *STATE* entry reads DOWN.
4. Repeat substep 3 periodically until the cluster is stopped.

   Note: You must not proceed to the next step until the cluster is stopped.

48

Restore the database backup created in Step 39; see the auxiliary database restore procedure in the *NSP System Administrator Guide* for information.

Update database schema

49

Update the NFM-P database schema.

Note: The schema update may take considerable time.

1. Log in as the nsp user on the NFM-P main server.
2. Open a console window.
3. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↵
   ```
4. Enter the following:

   ```
   bash$ ./nmsserver.bash upgradeAuxDbSchema ↵
   ```

   The following prompt is displayed:

   ```
   Auxiliary database clusters:
   ```

```
1: IP_a,IP_b,IP_c
2: IP_x,IP_y,IP_z
Select auxiliary database to upgrade:
```

5. Enter the number that corresponds to the cluster you are upgrading.

   The following messages and prompt are displayed:

   ```
   WARNING: About to upgrade samdb schema on the auxiliary database
   cluster [IP_a,IP_b,IP_c].
   It is recommended that a database backup is performed before
   proceeding.
   Type "YES" to continue
   ```

6. Enter YES.

   The following prompt is displayed:

   ```
   Please enter the auxiliary database port [5433]:
   ```

7. Enter the auxiliary database port number; press Enter to accept the default of 5433.

   The following prompt is displayed:

   ```
   Please enter the auxiliary database user password:
   ```

8. Enter the required password.

   The following messages are displayed as the upgrade begins:

   ```
   INFO: Database upgrade can take a very long time on large
   databases.
   INFO: logs are stored under /opt/nsp/nfmp/server/nms/log/auxdb.
   Check the logs for progress.
   INFO: Node Name[v_samdb_node0001]->IP[IP_address]->Status[UP]
   INFO: About to perform upgrade
   ```

Enable required database services and proxies

50

If the NFM-P is in a shared-mode NSP system, perform the following steps.

1. Log on as the root user on the NSP cluster host.
2. Open a console window.
3. Enter the following:

   ```
   # cd /opt ↵
   ```

4. Enter the following:

   ```
   # sftp root@deployer_IP ↵
   ```

   where *deployer_IP* is the NSP deployer host IP address

   The prompt changes to `sftp>`.

5. Enter the following:

   ```
   sftp> cd
   ```

```
/opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/database ↵
```

6. Enter the following:

```
sftp> get sync-auxdb-password.bash ↵
```

7. Enter the following:

```
sftp> quit ↵
```

8. Enter the following:

```
# chmod 777 sync-auxdb-password.bash ↵
```

9. Enter the following:

```
# ./sync-auxdb-password.bash ↵
```

10. If the command in substep 9 succeeds, output like the following is displayed:

```
timestamp: Synchronizing password for Auxiliary DB Output...
timestamp: deployment.apps/tlm-vertica-output scaled
timestamp: secret/tlm-vertica-output patched
timestamp: deployment.apps/tlm-vertica-output scaled
timestamp: Synchronization completed.
```

11. If the command output is not as expected, the NFM-P initialization may not be complete; wait 30 minutes, and then return to substep 9. Several attempts may be required.

51

Perform the following steps on each station in the auxiliary database cluster.

1. Log in as the root user.
2. Open a console window.
3. Enter the following sequence of commands to enable the database services:

```
systemctl enable nspos-auxdb.service
systemctl enable nspos-auxdbproxy.service
systemctl enable vertica_agent.service
systemctl enable verticad.service
```

52

If you are upgrading the standby auxiliary database cluster in a redundant deployment, go to Step 54.

53

Enter the following on each station in the auxiliary database cluster to start the database proxy:

```
# systemctl start nspos-auxdbproxy.service ↵
```

54

Close the open console windows.

END OF STEPS

NFM-P single-user GUI client upgrade from Release 22.6 or earlier

15.17 Upgrading a Release 22.6 or earlier single-user GUI client

15.17.1 Introduction

This section describes how to upgrade a Release 22.6 or earlier NFM-P single-user GUI client in a standalone or redundant NFM-P deployment.

You must comply with the general requirements in “NFM-P deployment configuration” (p. 370), and any specific requirements in this section, before you attempt to upgrade an NFM-P single-user GUI client.

Post-upgrade client connection to multiple NFM-P systems

You can configure a single-user client to connect to multiple NFM-P systems. For information , see 13.19 “To configure a GUI client login form to list multiple NFM-P systems” (p. 394).

15.17.2 Platform requirements

Single-user GUI client deployment is supported on the following platforms:

- Mac OS X
- Microsoft Windows
- RHEL

General

The following are the security requirements for single-user client upgrade:

- An upgrade requires only local user privileges.
- Only the user that deploys the client software, or a user with sufficient privileges, such as root or a local administrator, can start a single-user client.

Note: Single-user client upgrade requires a supported web browser on the client station. See the *NSP Planning Guide* for browser support information.

Mac OS

See the *NSP Planning Guide* for the Mac OS single-user client deployment requirements.

Microsoft Windows

See the *NSP Planning Guide* for the Microsoft Windows single-user client deployment requirements.

RHEL

A RHEL single-user GUI client station must have:

- a supported OS release and patch level, as described in the *NSP Planning Guide*
- the required RHEL OS configuration and packages, as described in Chapter 3, “RHEL OS deployment for the NSP”

Optionally, for greater system security, you can remove the world permissions from RHEL compiler executable files; see A.1 “Resetting GCC-compiler file permissions” (p. 1093) for information.

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

15.18 To upgrade a Release 22.6 or earlier NFM-P single-user GUI client

15.18.1 Purpose

The following steps describe how to upgrade the NFM-P software on a Release 22.6 or earlier single-user GUI client station.

Note: The main server to which the client connects must be upgraded and running when you perform the 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

Note: A leading `bash$` in a CLI command line represents the RHEL prompt, and is not to be included in the command.

15.18.2 Steps

1

Log in to the client station.

2

Close the client GUI, if it is open.

3

Use a browser to open the NSP sign-in page.

4

Enter the required login credentials and click SIGN IN. The NSP UI is displayed.

5

If one of the following is true, perform the following steps.

- The client is configured to connect to only one NFM-P system.
- The client is configured to connect to multiple NFM-P systems, and you do not want to keep the current client version.

Note: If the client is configured to connect to multiple NFM-P systems, and after the upgrade you select a non-upgraded system in the Server drop-down list of the client, you are prompted to downgrade the client. A client downgrade erases the multiple-system client configuration. If you want to preserve the Server drop-down options, do not downgrade the client.

1. Double-click on the NSP NFM-P Client desktop icon.
2. Go to Step 8.

6

Perform the following steps if the following conditions are true:

- The client is configured to connect to multiple NFM-P systems.
- You want to keep the current client version for connection to a system that is not yet upgraded.
- The system is the first of the multiple NFM-P systems to be upgraded.

If the conditions are true, you must remove the upgraded system from the configuration on the client station, and must not use the desktop icon to open the client.

a. On a Windows station:

1. Open the Registry Editor.
2. Navigate to the following key:

   Computer\HKEY_CURRENT_USER\SOFTWARE\JavaSoft\Prefs
3. Select and delete the IP address or hostname of each upgraded NFM-P main server.
4. Close the Registry Editor.
5. Edit the following file to remove the <j2ee and <systemMode lines for the upgraded NFM-P system.

   install_dir\nms\config\nms-client.xml

   where *install_dir* is the client installation directory
6. Edit the following file to replace all occurrences of the upgraded system, if present, with the IP address or hostname of a system that is not yet upgraded:

   Note: It is recommended to use the address or hostname of the system that is to be upgraded last.

   Note: For a redundant system, you must replace both main server addresses or hostnames.

   install_dir\nms\bin\locallaunch.jnlp
7. Right-click the desktop icon, select Properties, and change the name on the General tab to the IP address or hostname of a different NFM-P system.

   Note: It is recommended to use the address or hostname of the system that is to be upgraded last.
8. From the Java Control Panel, clear the Java cache of any entries for the recently upgraded system.
9. Right-click the client desktop icon, select Properties, and change the name on the General tab to the IP address or hostname of a different NFM-P system.
10. Install a new client instance.

Note: You must specify a new client installation location, and not the current location.

b. On a RHEL station:

1. Open the following file using a plain-text editor such as vi:

   ~/.java/.userPrefs/prefs.xml

2. Select and delete the IP address or hostname of each upgraded NFM-P main server.
3. Save and close the file.
4. Edit the following file to remove the <j2ee and <systemMode lines for the upgraded NFM-P system.

   install_dir/nms/config/nms-client.xml

   where *install_dir* is the client installation directory

5. Edit the following file to replace all occurrences of the upgraded system, if present, with the IP address or hostname of a system that is not yet upgraded:

   Note: It is recommended to use the address or hostname of the system that is to be upgraded last.

   Note: For a redundant system, you must replace both main server addresses or hostnames.

   install_dir/nms/bin/locallaunch.jnlp

6. Edit the desktop icon file to replace each occurrence of the upgraded system with the IP address or hostname of a system that is not yet upgraded.

   Note: It is recommended to use the address or hostname of the system that is to be upgraded last.

7. From the Java Control Panel, clear the Java cache of any entries for the recently upgraded system.
8. Install a new client instance.

Note: You must specify a new client installation location, and not the current location.

7

If the client is configured to connect to multiple NFM-P systems, and the upgraded system is not the first to be upgraded, perform the following steps.

a. For a Windows client:

1. Edit the following file to add <j2ee and <systemMode lines for each main server in the upgraded NFM-P system:

   new_install_dir\nms\config\nms-client.xml

   where *new_install_dir* is the installation directory of the new client installed in Step 6

2. Use the new client desktop icon to open the GUI for the upgraded system.

b. For a RHEL client:

1. Edit the following file to add <j2ee and <systemMode lines for each main server in the upgraded NFM-P system:

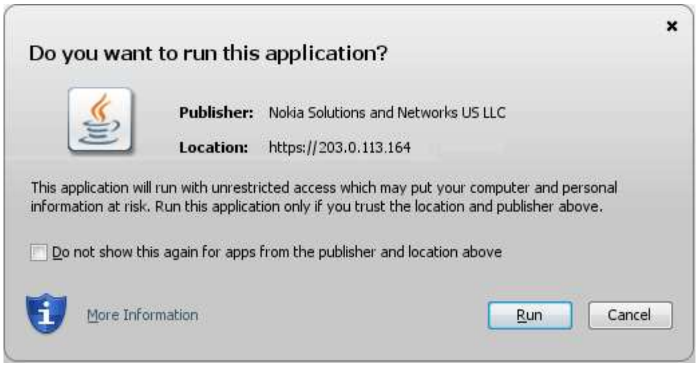
   new_install_dir/nms/config/nms-client.xml where *new_install_dir* is the installation directory of the new client installed in Step 6

2. Use the new client desktop icon to open the GUI for the upgraded system.

8

A form like the following is displayed.

Figure 15-2 Do you want to run this application?



Do you want to run this application?

Publisher: Nokia Solutions and Networks US LLC

Location: https://203.0.113.164

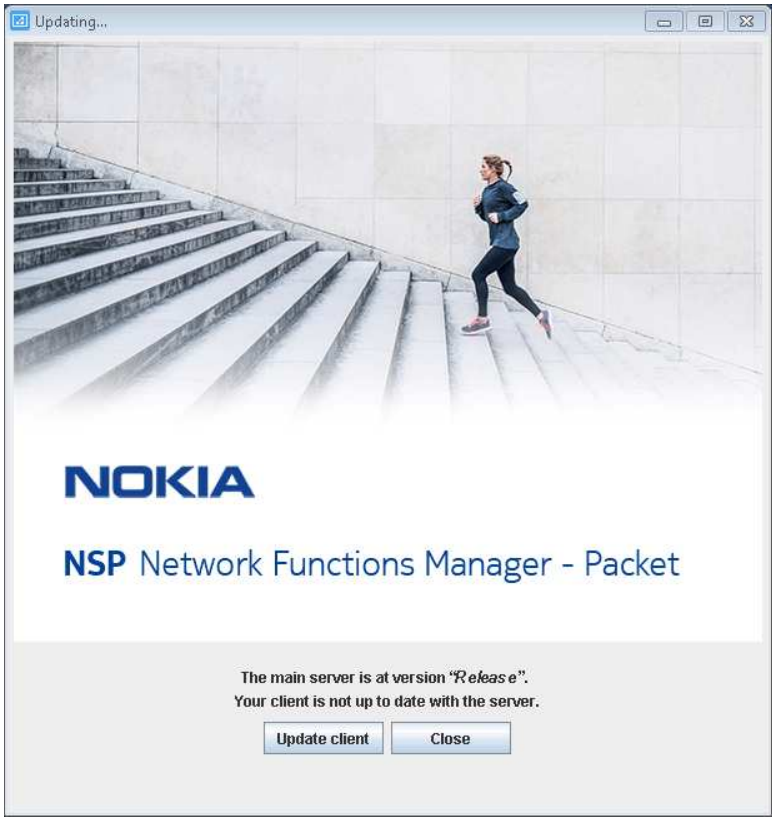
This application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the location and publisher above.

□ Do not show this again for apps from the publisher and location above

Click Run.

The panel shown in Figure 15-3, “Updating...” (p. 787) is displayed.

Figure 15-3 Updating...



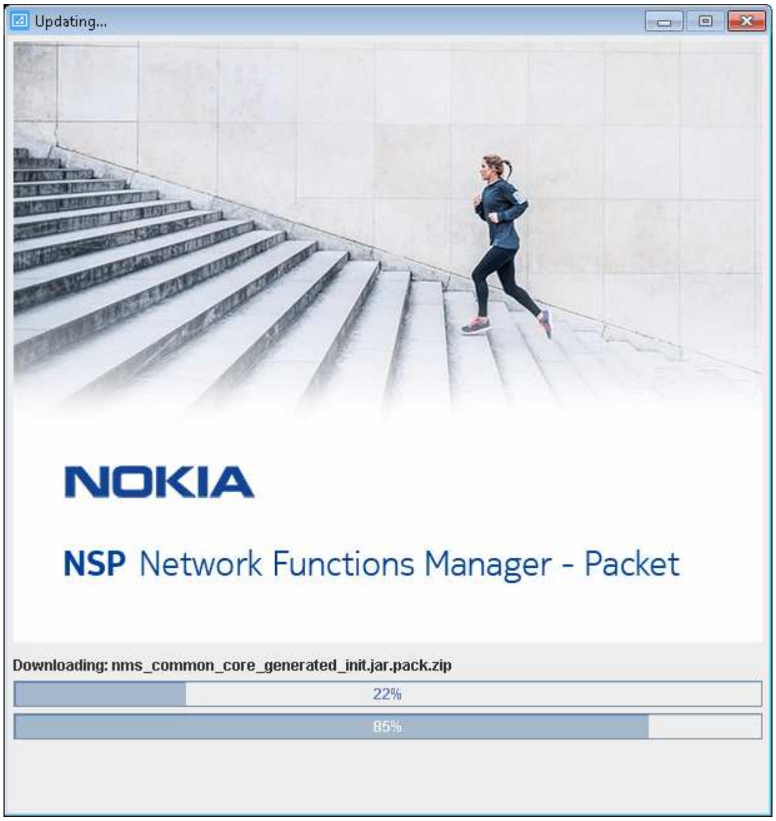
The main server is at version "Release".
Your client is not up to date with the server.

9

Click Update client.

The client upgrade begins, and the panel shown in Figure 15-4, "Updating..." (p. 788) is displayed. The panel uses separate bars to indicate the overall and current task progress.

Figure 15-4 Updating...



Downloading: nms_common_core_generated_init.jar.pack.zip

10

If the client is installed on Mac OS X, perform the following steps.

1. Open a console window.
2. Navigate to the following directory:

   /Applications/NFMPclient.*IP_address*.app/Contents/Resources/nms/bin
3. Enter the following:

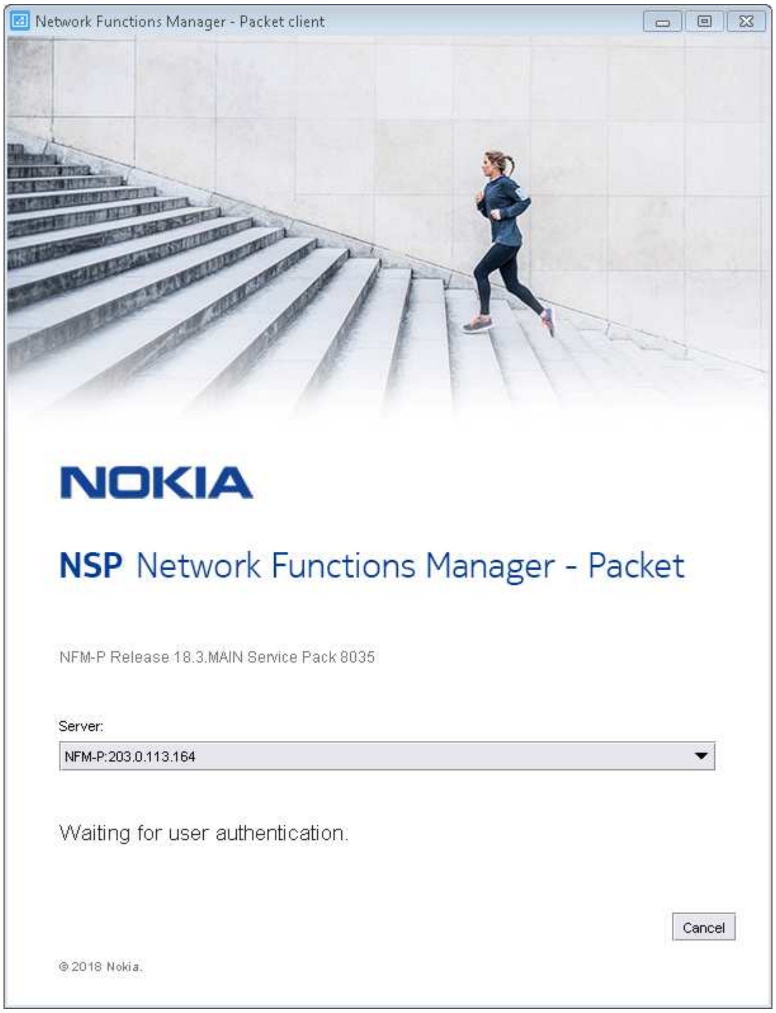
   chmod +x nmsclient.bash ↵

11

If you are not currently logged in, the splash screen shown in Figure 15-5, “Waiting for user authentication” (p. 789) opens, and the NSP sign-in page is displayed.

Enter the required login credentials on the NSP sign-in page and click SIGN IN. The NSP UI is displayed, and the client GUI opens.

Figure 15-5 Waiting for user authentication



Network Functions Manager - Packet client

NOKIA

NSP Network Functions Manager - Packet

NFM-P Release 18.3.MAIN Service Pack 8035

Server:

NFM-P:203.0.113.164

Waiting for user authentication.

© 2018 Nokia.

12

Verify that the GUI is operational and correctly displayed.

END OF STEPS

NFM-P client delegate server upgrade from Release 22.6 or earlier

15.19 Upgrading a Release 22.6 or earlier client delegate server

15.19.1 Introduction

This section describes how to upgrade a Release 22.6 or earlier NFM-P client delegate server in a standalone or redundant NFM-P deployment.

You must comply with the general requirements in “NFM-P deployment configuration” (p. 370), and any specific requirements in this section, before you attempt to upgrade an NFM-P client delegate server.

15.19.2 Platform requirements

Client delegate server deployment is supported on the following platforms:

- RHEL
- Microsoft Windows

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 Planning Guide* for a list of the ports that must be open on each component.

Note: Client delegate server deployment requires a supported web browser on the client delegate server station. See the *NSP Planning Guide* for browser support information.

Microsoft Windows

See the *NSP Planning Guide* for the supported Microsoft Windows versions for client delegate server deployment.

Note: Client delegate server deployment on Windows requires local Administrator privileges.

RHEL

A RHEL client delegate server station must have:

- a supported OS release and patch level, as described in the *NSP Planning Guide*
- the required RHEL OS configuration and packages, as described in Chapter 3, “RHEL OS deployment for the NSP”
- the required Oracle JRE version; see the *NSP Planning Guide* for information

Optionally, for greater system security, you can remove the world permissions from RHEL compiler executable files; see A.1 “Resetting GCC-compiler file permissions” (p. 1093) for information.

Note: Client delegate server deployment on RHEL requires root user privileges.

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

15.20 To upgrade a Release 22.6 or earlier NFM-P client delegate server

15.20.1 Purpose

The following steps describe how to upgrade the Release 22.6 or earlier NFM-P software on a client delegate server station in a standalone or redundant NFM-P deployment.

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:

- Microsoft Windows—local Administrator
- RHEL—root

15.20.2 Steps

1

Close each remote client GUI session that the client delegate server hosts.

2

Log in to the client delegate server station.

3

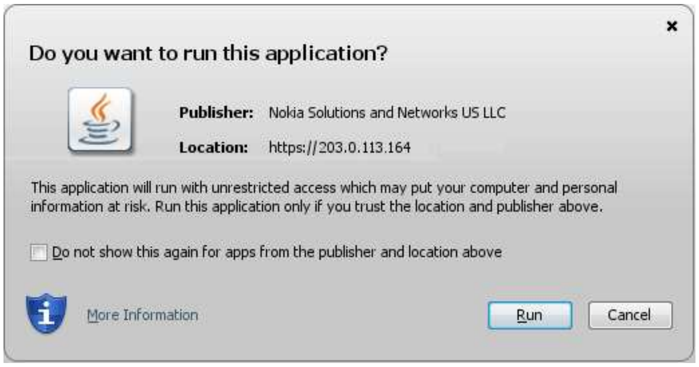
Close the local client GUI, if it is open.

4

Double-click on the NSP NFM-P Client desktop icon.

A form like the following is displayed.

Figure 15-6 Do you want to run this application?



Do you want to run this application?

Publisher: Nokia Solutions and Networks US LLC

Location: https://203.0.113.164

This 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.

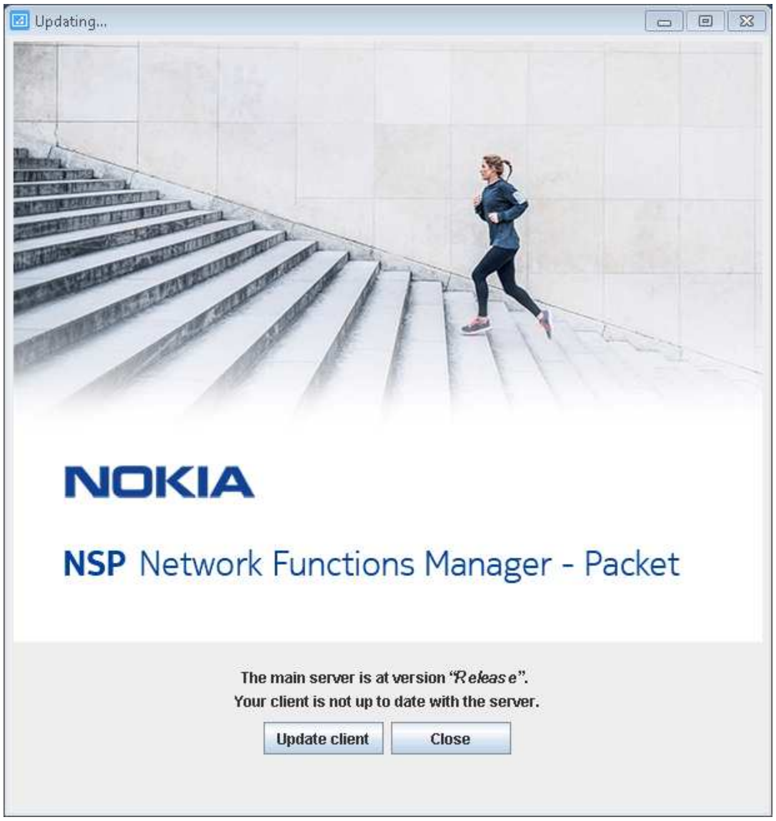
☐ Do not show this again for apps from the publisher and location above

5

Click Run.

The panel shown in Figure 15-7, “Updating...” (p. 791) is displayed.

Figure 15-7 Updating...



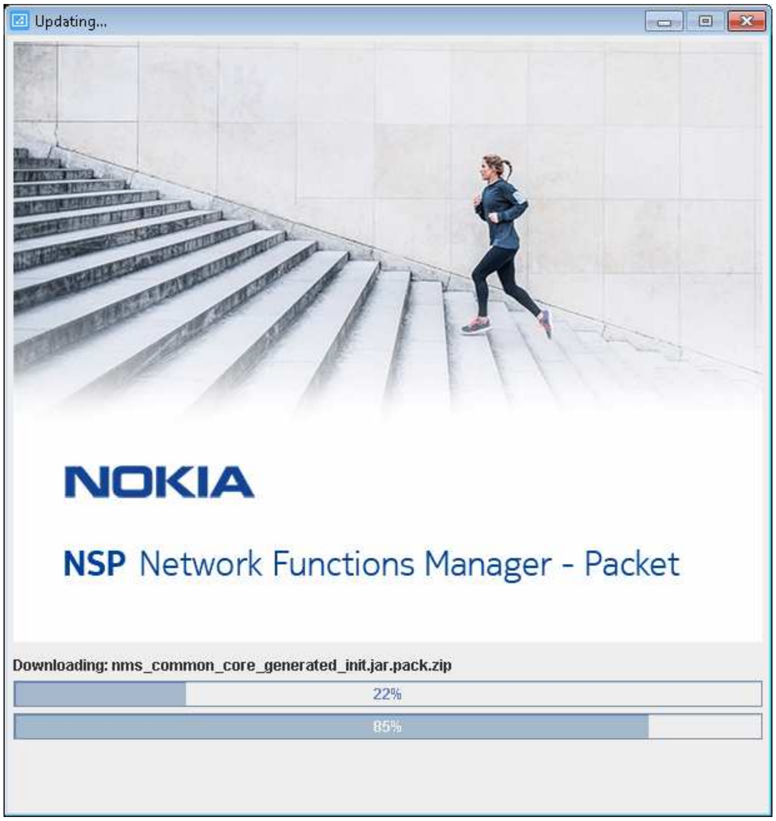
The main server is at version “Release”.
Your client is not up to date with the server.

6

Click Update client.

The client delegate server upgrade begins, and the panel shown in Figure 15-8, “Updating...” (p. 793) is displayed. The panel uses separate bars to indicate the overall and current task progress.

Figure 15-8 Updating...



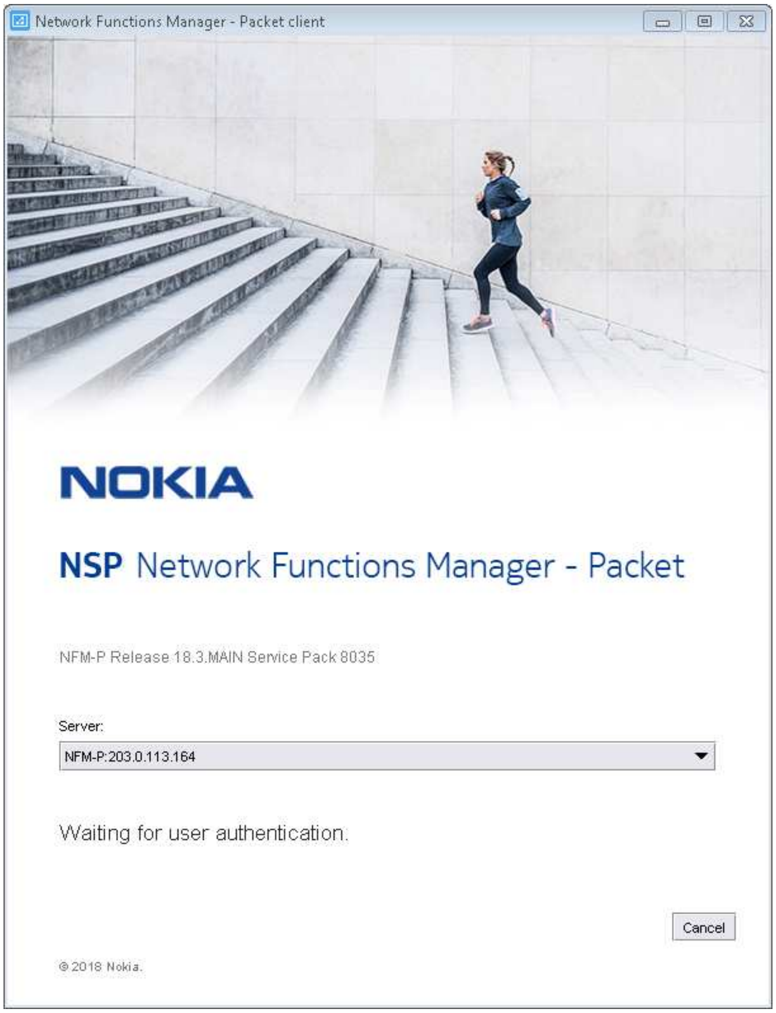
Downloading: nms_common_core_generated_init.jar.pack.zip

7

If you are not currently logged in, the splash screen shown in Figure 15-9, “Waiting for user authentication” (p. 794) opens, and the NSP sign-in page is displayed.

Enter the required login credentials on the NSP sign-in page and click SIGN IN. The NSP UI is displayed, and the client GUI opens.

Figure 15-9 Waiting for user authentication


Network Functions Manager - Packet client
NOKIA
NSP Network Functions Manager - Packet
NFM-P Release 18.3.MAIN Service Pack 8035
Cancel
© 2018 Nokia.

Server:
NFM-P:203.0.113.164

Waiting for user authentication.

8

Verify that the GUI is operational and correctly displayed.

END OF STEPS

16 NSP component upgrade from Release 22.9 or later

16.1 Overview

16.1.1 Purpose

This chapter describes the upgrade of NSP Release 22.9 or later components that are deployed outside the NSP cluster.

16.1.2 Contents

Upgrading NSP components from Release 22.9 or later

16.2 NSP component upgrade overview

16.2.1 Component upgrade support

CAUTION

Deployment failure

You cannot successfully upgrade an NSP component that has never initialized.

Before you attempt an NSP component upgrade, ensure that the component has successfully initialized.

Before you attempt to perform a procedure in this chapter, you must ensure that your deployment meets the hardware and software requirements described in the *NSP Planning Guide*.

Note: When you upgrade a shared-mode NSP system that includes the NFM-P, the existing Service Supervision groups are migrated from the NFM-P to the NSP. The migration may take a few hours, depending on the number of services. During this time, you must not auto-create Service Supervision groups. You can use the Find Ungrouped members count in the Group Manager application to help determine when the upload is complete, after which you can auto-create groups.

Note: It is strongly recommended that you verify the GPG signature of each RPM file that you download from Nokia to ensure that each file has a valid Nokia signature.

Note: It is strongly recommended that you verify the message digest of each NSP image file or software bundle that you download from the Nokia Support portal. The download page includes the MD5, SHA256, and SHA512 checksums for comparison with the output of the RHEL md5sum, sha256sum, or sha512sum command. See the associated RHEL man page for command usage information.

Note: If you have modified any NFM-P template files, contact technical support before you attempt an NSP or NFM-P system upgrade; an upgrade overwrites customized template values.

Note: NFM-P language localization files are not automatically backed up during an NSP upgrade. To preserve your language localization, you must back up your localization file before an NSP upgrade, and then redeploy the file after the upgrade.

Shared-mode upgrades

CAUTION

Upgrade Failure

If the system locales of the NFM-P and the NSP components of a shared-mode deployment do not match, a system upgrade may fail.

Ensure that the NSP system locale matches the NFM-P locale before you attempt a shared-mode system upgrade. If the locales do not match, contact technical support for assistance.

The components that comprise a shared-mode NSP deployment must be upgraded in a specific order, starting with the NSP cluster. During the upgrade, the NSP UI is unavailable, as is an NFM-P or WS-NOC that is part of the NSP system. After the NSP component upgrade, the NFM-P and WS-NOC can be upgraded in any order.

See the NSP compatibility matrix in the *NSP Release Notice* to ensure that the proposed upgrade results in a supported configuration.

NSP Flow Collector and Flow Collector Controller upgrade from Release 22.9 or later

16.3 To upgrade Release 22.9 or later NSP Flow Collectors and Flow Collector Controllers

16.3.1 Purpose

Use this procedure to upgrade the standalone or redundant Release 22.9 or later NSP Flow Collector Controllers and NSP Flow Collectors in an NSP data center.

Note: You cannot upgrade an NSP Flow Collector or Flow Collector Controller to a collocated deployment that has both on one station.

Note: The install.sh utility requires SSH access to a target station. To enable SSH access, you must do one of the following.

- Configure the required SSH keys on the stations.
- If each remote station has the same root user password, add the --ask-pass argument to the install.sh command; for example:

```
./install.sh --ask-pass --target remote_station
```

16.3.2 Steps

Stop NSP Flow Collector Controllers

1

Perform the following steps on each NSP Flow Collector Controller station to stop the NSP Flow Collector Controller.

Note: If an NSP Flow Collector is also installed on the station, the Flow Collector stops automatically.

1. Log in to the station as the nsp user.
2. Enter the following:

```
bash$ /opt/nsp/flow/fcc/bin/flowCollectorController.bash stop ↵
```

The NSP Flow Collector Controller stops.

Stop NSP Flow Collectors

2

Stop each NSP Flow Collector that is not collocated with an NSP Flow Collector Controller.

Note: Any NSP Flow Collector that is collocated with a Flow Collector Controller is automatically stopped earlier in the procedure.

1. Log in to the NSP Flow Collector station as the nsp user.

2. Enter the following:

```
bash$ /opt/nsp/flow/fc/bin/flowCollector.bash stop ↵
```

The NSP Flow Collector stops.

Set SELinux mode

3

If SELinux enforcing mode is enabled on the NSP Flow Collector or Flow Collector Controller, you must switch to permissive mode on each; otherwise, you can skip this step.

Perform “How do I switch between SELinux modes on NSP system components?” in the *NSP System Administrator Guide* on the Flow Collector or Flow Collector Controller.

Note: If SELinux enforcing mode is enabled during the upgrade, the upgrade fails.

Apply OS update

4

If the NSP Flow Collector or Flow Collector Controller is deployed in a VM created using an NSP RHEL OS disk image, perform 3.4 “To apply a RHEL update to an NSP image-based OS” (p. 67).

Start PKI server

5

Start the PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 4.10 “To configure and enable a PKI server” (p. 113).

Note: The PKI server is required for internal system configuration purposes.

Upgrade software

6

Download the NSP component installer package (NSP_NSD_NRC_*R_r*.tar.gz) from OLCS and extract it on any station running a supported version of RHEL. This does not have to be the station on which the NSP Flow Collector Controller or an NSP Flow Collector is installed; the installer can perform remote upgrades.

An NSD_NRC_*R_r* directory is created in the current directory, where *R_r* is the release identifier in the form *MAJOR_minor*.

Note: In subsequent steps, the directory is called the NSP installer directory or *NSP_installer_directory*.

7

Log in as the root user on the station that has the downloaded NSP software bundle.

8

Enter the following:

```
# cd NSP_installer_directory/NSD_NRC_R_r/bin ↵
```

9

Create a hosts file in the current directory that contains the required entries in the following sections:

- [nspos]—one entry for each ZooKeeper host; the ZooKeeper hosts are one of the following:
  - if the NSP system includes only the NFM-P, the NFM-P main servers
  - otherwise, the VIP address of each NSP cluster
- [fcc]—one line entry for each Flow Collector Controller
- [fc]—one line entry for each Flow Collector

Note: If an NSP Flow Collector Controller and Flow Collector are to be collocated on one station, specify the same address for in the [fc] and [fcc] sections; for example:

```
[fcc] 203.0.113.3 advertised_address=198.51.100.3 ansible_host=
198.51.100.3
[fc] 203.0.113.3 ansible_host=198.51.100.3 fc_mode=AA
```

See 13.3 “NSP hosts file” (p. 364) for configuration information.

Note: A sample hosts file is in the following directory; you must use a modified copy of the file for installation:

- *NSP_installer_directory*/NSD_NRC_*R_r*/examples

  where *R_r* is the NSP software release

10

Create a config.yml file in the NSP installer directory that includes the following sections; see 13.4 “NSP RPM-based configuration file” (p. 366) for information.

- multi-component deployment:
  - **sso**
  - **tls**
  - section for each component to install
- independent deployment, for example, if you are adding a Flow Collector or Flow Collector Controller to an NFM-P-only system:
  - **sso**
  - **tls**

Note: The following parameter values in the **tls** section must match the values in the NSP configuration file; otherwise, the values must match the values in the NFM-P main server configuration:

- secure
- PKI server parameters

You can use the samconfig “show” command on a main server to display the **tls** parameters. See 14.9 “NFM-P samconfig utility” (p. 432) for information about using the samconfig utility.

Note: A sample config.yml file is in the following directory; you must use a modified copy of the file for installation:

- *NSP_installer_directory*/NSD_NRC_*R_r*/examples

  where *R_r* is the NSP software release

11

Enter the following:

Note: Include the --ask-pass option only if each target station has the same root user password.

```
# ./install.sh --ask-pass --target target_list ↵
```

where *target_list* is a comma-separated list of the NSP Flow Collector Controller and NSP Flow Collector IP addresses

The NSP Flow Collector Controller or NSP Flow Collector software is upgraded on each station.

Configure NFM-P in DR deployment

12

If the NSP cluster and NSP Flow Collector Controllers are not in a DR deployment, go to Step 19.

13

Log in as the root user on the NFM-P main server in the same data center as the NSP Flow Collector Controller.

14

Open a console window.

15

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.

5. Enter the following to switch back to the root user:

```
bash$ su - ↵
```

6. If the NFM-P is not in a shared-mode NSP deployment, enter the following to display the NSP service status:

```
# nspdctl status ↵
```

Information like the following is displayed.

```
Mode:     DR
Role:     redundancy_role
DC-Role:  dc_role
DC-Name:  dc_name
Registry: IP_address:port
State:    stopped
Uptime:   0s
SERVICE           STATUS
service_a         inactive
service_b         inactive
service_c         inactive
```

You must not proceed to the next step until all NSP services are stopped; if the State is not ‘stopped’, or the STATUS indicator of each listed service is not ‘inactive’, repeat this substep.

16

You must create an association between the local NSP Flow Controller and the local NFM-P main server to ensure that the Flow Collector and Controller remain in communication with the local NFM-P during NSP DR activity.

Add the local data center name to the main-server configuration.

Note: The data center name must be a name other than “default”.

1. Enter the following:

```
# samconfig -m main ↵
```

The samconfig utility opens, and the following is displayed:

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

2. Enter the following:

```
<main> configure nspos dc-name data_center ↵
```

where *data_center* is the data center name, which must match the dcName value for the local NSP cluster in the NSP configuration file

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

3. Enter the following:

   ```
   <main configure nspos> exit ↵
   ```

   The prompt changes to `<main>`.

4. Enter the following:

   ```
   <main> apply ↵
   ```

   The configuration is applied.

5. Enter the following:

   ```
   <main> exit ↵
   ```

   The samconfig utility closes.

17

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.

Restore SELinux enforcing mode

18

If you switched from SELinux enforcing mode to permissive mode before the upgrade, and want to restore the use of enforcing mode, perform “How do I switch between SELinux modes on NSP system components?” in the *NSP System Administrator Guide* on the NSP Flow Collector or Flow Collector Controller.

Start NSP Flow Collector Controllers

19

Perform the following steps on each NSP Flow Collector Controller station.

Note: If an NSP Flow Collector is also installed on the station, the Flow Collector starts automatically.

1. Log in to the station as the nsp user.
2. Enter the following:

   ```
   bash$ /opt/nsp/flow/fcc/bin/flowCollectorController.bash start ↵
   ```

   The NSP Flow Collector Controller starts.
3. Close the console window.

Start NSP Flow Collectors

20

Start each NSP Flow Collector that is not collocated with an NSP Flow Collector Controller.

Note: Any NSP Flow Collector that is collocated with a Flow Collector Controller is automatically started earlier in the procedure.

1. Log in to the NSP Flow Collector station as the nsp user.
2. Enter the following:

   ```
   bash$ /opt/nsp/flow/fc/bin/flowCollector.bash start ↵
   ```

   The NSP Flow Collector starts.
3. Close the console window.

21

Perform the following steps for each NSP Flow Collector.

1. Use a browser to open the web UI at the following URL:

   https://*server*:8443/fc/admin

   where *server* is the NSP Flow Collector IP address or hostname

   The Collection Policy configuration page opens.
2. Verify the settings on each configuration page to ensure that the settings from before the upgrade are preserved.

22

If no other components are to be deployed, stop the PKI server by entering Ctrl+C in the console window.

23

Close the open console windows.

END OF STEPS

NSP analytics server upgrade from Release 22.9 or later

16.4 To upgrade Release 22.9 or later NSP analytics servers

16.4.1 Purpose

The following steps describe how to upgrade the Release 22.9 or later analytics servers in an NSP system.

Note: You cannot selectively upgrade analytics servers; all analytics servers must be upgraded in one operation as described in the procedure.

Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

Note: Each running NSP analytics server and each running NFM-P auxiliary database in the NSP system must be at the same release.

Note: If you are replacing any analytics server stations, it is recommended that you commission the stations in advance of the upgrade to reduce the upgrade duration.

For information about deploying the RHEL OS using an NSP OEM disk image, see 2.2.2 “NSP disk-image deployment” (p. 28).

Note: After an 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 *NSP Release Notice* for limitations regarding specific reports.

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

16.4.2 Steps

Download installation files

1

Log in as the root user on a station that is reachable from each analytics server station.

2

Open a console window.

3

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
- analyticsBackupForMigration.sh

where

R.r.p is the NSP release ID, in the form *MAJOR.minor.patch*

v is a version number

Back up analytics report repository, security files

4

Log in as the root user on any analytics server station in the data center..

5

Transfer the downloaded analyticsBackupForMigration.sh file to the /opt/nsp directory.

6

Enter the following:

```
# chown nsp:nsp /opt/nsp/analyticsBackupForMigration.sh ↵
```

7

Enter the following:

```
# chmod +x /opt/nsp/analyticsBackupForMigration.sh ↵
```

8

Enter the following to switch to the nsp user:

```
# su - nsp ↵
```

9

Enter the following:

```
bash$ ./analyticsBackupForMigration.sh ↵
```

The server security keys and configuration file are backed up to the following file in the current directory, /opt/nsp:

analyticsBackup.tar.gz

10

Enter the following:

```
bash$ tar -tzf analyticsBackup.tar.gz ↵
```

The backed-up files are listed.

11

Verify that the output matches the following; if any file is not listed, contact technical support:

- opt/nsp/.jrsks
- opt/nsp/.jrsksp
- opt/nsp/analytics/config/install.config
- opt/nsp/analytics/backup/analytics_backup_*version*_*timestamp*.zip
  where
  version is the current analytics software version
  timestamp is the current timestamp

12

Copy the /opt/nsp/analyticsBackup.tar.gz file to a secure location on a separate station that is not affected by the upgrade activity.

Stop analytics servers

13

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/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
   ```

Uninstall all analytics servers

14

Perform Step 1 to Step 8 of 19.2 “To uninstall an NSP analytics server” (p. 1076) on each analytics server station.

Set SELinux mode

15

If SELinux enforcing mode is enabled on the NSP Analytics servers, you must switch to permissive mode on each; otherwise, you can skip this step.

Perform “How do I switch between SELinux modes on NSP system components?” in the *NSP System Administrator Guide* on each NSP analytics server station.

ℹ **Note:** If SELinux enforcing mode is enabled during the upgrade, the upgrade fails.

Start PKI server

16

Start the PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 4.10 “To configure and enable a PKI server” (p. 113).

ℹ **Note:** The PKI server is required for internal system configuration purposes, so must be running before you continue.

ℹ **Note:** All NSP components must use TLS artifacts that are signed by the same root CA. If the NSP or NFM-P to which the analytics server connects is using TLS artifacts from a previous deployment, you must ensure that the private key file and public certificate file from the previous deployment are copied to the PKI server, as described in 4.10 “To configure and enable a PKI server” (p. 113).

17

Perform Step 19 to Step 35 on each analytics server station.

18

Go to Step 36.

Upgrade individual analytics server

19

If the analytics server is deployed in a VM created using an NSP RHEL OS disk image, perform 3.4 “To apply a RHEL update to an NSP image-based OS” (p. 67).

20

Log in as the root user on the analytics server station.

21

Open a console window.

22

Transfer the installation files downloaded in Step 3 to an empty temporary directory on the station.

ℹ **Note:** You must ensure that the directory contains only the installation files.

23

Navigate to the directory that contains the installation files.

24

Enter the following:

```
# chmod +x * ↵
```

25

Enter the following:

```
# dnf install *.rpm ↵
```

For each package, the dnf 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
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

27

Perform one of the following.

a. If the analytics server is the first analytics server to be upgraded, perform the following steps.

1. Copy the /opt/nsp/analyticsBackup.tar.gz saved in Step 13 to the /opt/nsp directory.
2. Enter the following to switch to the nsp user:

   ```
   # su - nsp ↵
   ```

3. Enter the following:

```
bash$ cd /opt/nsp/analytics/bin ↵
```

4. Enter the following:

```
bash$ ./preInstallWithBackup.sh /opt/nsp/analyticsBackup.tar.gz ↵
```

The configuration is restored.

b. If the analytics server is not the first analytics server to be upgraded, perform the following steps.

1. Transfer the following files from the first upgraded analytics server to the /opt/nsp directory on the analytics server that you are currently upgrading:
   - /opt/nsp/.jrsks
   - /opt/nsp/.jrsksp
2. Enter the following:

```
# chown nsp:nsp /opt/nsp/.jrsks ↵
```

3. Enter the following:

```
# chown nsp:nsp /opt/nsp/.jrsksp ↵
```

4. Enter the following to switch to the nsp user:

```
# su - nsp ↵
```

28

Enter the following:

```
bash$ /opt/nsp/analytics/bin/AnalyticsAdmin.sh updateConfig ↵
```

The script displays the following message and prompt:

```
THIS ACTION UPDATES /opt/nsp/analytics/config/install.config
Please type 'YES' to continue
```

29

Enter YES.

The script displays a series of prompts.

30

At each prompt, enter a parameter value; to accept a default in brackets, press ↵.

Note: Accept all the previous values unless they have changed.

The following table lists and describes each parameter.

Table 16-1 NSP analytics server parameters

Parameter	Description
Analytics Server Hostname or IP Address	The analytics server hostname or IP address that is reachable by the NSP cluster and the client browsers Default: —

Table 16-1 NSP analytics server parameters (continued)

Parameter	Description
Enter IP address or hostname for internal network	The analytics server internal IP address, if configured Default: —
Is NSPOS secure	Whether the internal NSP system communication is secured using TLS In a shared-mode NSP system, the value must match the “nspos secure” parameter value; otherwise, the value must match the “secure” value in the nspos section of the NFM-P main server configuration.
Use internal certificates	Whether internal service communication between NSP components is secured using internally generated TLS certificates You can set the parameter to true only if the “Is NSPOS secure” parameter is set to true.
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 • the internalAdvertisedAddress value in the primary or standalone NSP configuration file, if configured; otherwise, the advertisedAddress value
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 • the internalAdvertisedAddress value in the standby NSP configuration file, if configured; otherwise, the advertisedAddress value
Primary Oracle Data Source DB Host	The primary or standalone main database IP address or hostname
Primary Oracle Data Source DB Name	The primary or standalone main database instance name
Primary Oracle Data Source DB Port	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 or hostname
Secondary Oracle Data Source DB Name	In a redundant system, the standby main database instance name
Secondary Oracle Data Source DB Port	In a redundant system, the TCP port on the standby main database station that receives database requests
PKI Server IP Address or Hostname	The PKI server IP address or hostname Regardless of whether you are using the manual or automated TLS configuration method, you must specify the PKI server address.

Table 16-1 NSP analytics server parameters (continued)

Parameter	Description
PKI Server Port	The PKI server port
Zookeeper Connection String	The IP address or hostname, and port of each ZooKeeper host, in the following format: `server1_address:port;server2_address:port` where *server1_address* and *server2_address* are the IP addresses or hostnames of the ZooKeeper hosts *port* is a port number based on the **Is NSPOS secure** setting: • 2181, if false • 2281, if true **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** • **the advertisedAddress of each cluster from the NSP configuration file**
Use NFM-P-only mode? (true/false)	Specifies how the Analytics server communicates with the NSP system The parameter must be set to true if the deployment includes only the NFM-P and has no NSP cluster.

31

If you are upgrading the first analytics server, and either of the following is true, you must purge the Analytics data from the NSP PostgreSQL database, and restore critical files from the backup; otherwise, you can skip this step.

- The software version from which you are upgrading is still installed on one or more analytics servers.

  OR

- One or more analytics servers were still installed when the NSP PostgreSQL database backup was created for the NSP system upgrade.

1. Enter the following:

   ```
   bash$ ./AnalyticsAdmin.sh genCertificate ↵
   ```

   Note: The command may generate the following error message that you can safely ignore:

   ```
   /opt/nsp/analytics/bin/vault.sh: line 46: ./eap-vault-update.sh: No
   such file or directory
   ```

2. Enter the following:

   ```
   bash$ ./AnalyticsAdmin.sh force_uninstall ↵
   ```

   The NSP PostgreSQL database is purged of analytics-server information.

3. Enter the following:

```
bash$ tar -xzf /opt/nsp/analyticsBackup.tar.gz --directory /opt/nsp
'./.jrsks*' ↵
```

32

Perform one of the following to install the analytics server software on the station.

a. If the analytics server is the first analytics server to be upgraded, enter the following:

```
bash$ /opt/nsp/analytics/bin/AnalyticsAdmin.sh installWithBackup ↵
```

b. If the analytics server is not the first analytics server to be upgraded, enter the following:

```
bash$ /opt/nsp/analytics/bin/AnalyticsAdmin.sh install ↵
```

Note: The analytics server starts automatically after the installation.

The following prompt is displayed if the Use NFM-P-only mode parameter in Step 30 is set to false.

```
Enter NSP user name:
```

33

If the prompt is displayed, perform the following steps.

1. Enter admin ↵.

   The following prompt is displayed:

   ```
   Enter NSP user password (hidden):
   ```

2. Enter the password of the NSP admin user.

34

The following messages and prompt are displayed:

```
Access token retrieved successfully
date time Analytics App is UP and Running
Version check passed. NSP version = RR.r; Analytics server version =
RR.r
date time Installing Analytics Server...
Do you have existing TLS certificates?(yes/no)
```

35

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 Certificate 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 upgrade proceeds, and messages like the following are displayed:

```
Creating Analytics Repository Schema
```

```
Analytics Repository Schema creation is complete
Modified JIRoles Table
Please wait while Analytics Server is being installed...This may take
a few minutes
Restoring backup
Retrieving AUXDB Connection Configurations
AUXDB Connection Configuration successfully retrieved
date time Deploying customization zip file
date time  Analytics server upgrade is complete. Starting analytics
server
date time Starting Analytics Application
Waiting for Analytics Server to come up
date time Analytics Server is UP and Running
Oracle Redundancy Configuration Detected
Analytics Server successfully started
Importing reports for upgrade
Deploying Reports After Upgrade
Start Deploying /opt/nsp/analytics/analytics-report/domains.zip
Tracking nn reports...
Inserted nn reports into Tracker Table
All reports successfully tracked
Start Deploying /opt/nsp/analytics/analytics-report/reports.zip
Tracking nnn reports...
All reports successfully tracked
Waiting for upgrading reports...
Moving resources under Results folder to Shared folder
Updating scheduled jobs
Transferred roles to user
Deleting Analytics resources metadata...
Analytics resources metadata deleted
Updating Analytics resources metadata...
Analytics resources metadata updated
date time Analytics server upgraded successfully
```

Restore SELinux enforcing mode

36

If you switched from SELinux enforcing mode to permissive mode before the upgrade, and want to restore the use of enforcing mode, perform “How do I switch between SELinux modes on NSP system components?” in the *NSP System Administrator Guide* on each analytics server.

Stop PKI server

37

If no other components are to be deployed, stop the PKI server by entering Ctrl+C in the console window.

38

Close the open console windows.

END OF STEPS

NFM-P system upgrade from Release 22.9 or later

16.5 Upgrade requirements

16.5.1 Primary considerations

CAUTION

Service Disruption

An NFM-P system upgrade 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 Planning Guide, and the NSP 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.

CAUTION

Upgrade Failure

A system upgrade fails unless you strictly comply with the upgrade requirements and operate within the upgrade restrictions.

Ensure that you have a thorough understanding of the NFM-P system upgrade requirements and restrictions in “NFM-P deployment configuration” (p. 370) and in the NSP Planning Guide, and that you perform a test upgrade in advance of a live upgrade, as described in 16.5.2 “Staging your upgrade” (p. 820).

This section describes the general conditions that apply to NFM-P system upgrades. Before you attempt to upgrade an NFM-P component, you must comply with the conditions in “NFM-P deployment configuration” (p. 370) and this section.

“NFM-P single-user GUI client upgrade from Release 22.9 or later” (p. 955) and “NFM-P client delegate server upgrade from Release 22.9 or later” (p. 963) describe how to upgrade an NFM-P single-user GUI client or client delegate server.

Note: It is strongly recommended that you verify the message digest of each NSP image file or software bundle that you download from the Nokia Support portal. The download page includes the MD5, SHA256, and SHA512 checksums for comparison with the output of the RHEL md5sum, sha256sum, or sha512sum command. See the associated RHEL man page for command usage information.

Note: Before a system upgrade, you must ensure that you have sufficient time to complete a main database upgrade. The time required for the upgrade depends on the platform resources, database complexity, and tablespace configuration. Contact technical support to obtain a database upgrade duration estimate.

Note: The following NFM-P main server **aux** parameters remain in the samconfig utility, but are obsolete and not to be configured:

- calltrace
- pcmd
- webdav
- disable-cn-check
- custom-http-headers
- calltrace-pairs
- pcmd-pairs

Note: The following NFM-P auxiliary server **service** parameters remain in the samconfig utility, but are obsolete and not to be configured:

- pcmd
- calltrace

Note: The following NFM-P auxiliary server **tls** parameter remains in the samconfig utility, but is obsolete and not to be configured:

- disable-cn-check

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

Geo-redundant system upgrades

The upgrade of geo-redundant NFM-P sites in a DR NSP deployment is orchestrated using the NSP system upgrade procedures in Chapter 9, “NSP system upgrade from Release 22.9 or later”. Consequently, an NFM-P system upgrade is an operation that is independent of the NSP deployment type.

Note: The upgrade procedures include a limited number of conditional workflow or procedure steps for special geo-redundant considerations such as auxiliary database upgrades.

Note: If the main servers in a redundant NFM-P system use different time zones, as in a geo-redundant deployment, and NSP Analytics 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 an event, after both main servers are upgraded you must use the client GUI to change the Analytics aggregation time-zone setting.

See the *NSP Analytics Report Catalog* for aggregation configuration information.

16.5.2 Staging your upgrade

It is essential that you plan, document, and test an upgrade in advance on a lab system in a closed environment that is representative of the actual network. Contact technical support to assess the system upgrade requirements.

Note: In a large or complex network, it is strongly recommended that you engage the technical support upgrade service.

Performing a test upgrade involves the same preparation and series of actions as a live upgrade; see 16.7 "General NFM-P Release 22.9 or later upgrade workflow" (p. 822) for information.

16.5.3 TLS configuration

In 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.

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.

Note: TLS 1.0 and 1.1 are disabled by default. If either version is enabled before an NFM-P system upgrade and required after the upgrade, you must re-enable the version support after the upgrade.

See the *NSP System Administrator Guide* for information about using the tool.

16.5.4 XML API client compatibility

An OSS client must use the samOss.jar from the current NFM-P release. If a different samOss.jar is used, the NFM-P system may become unstable. The NFM-P release information is in the JAR manifest file.

Note: If you intend to use an existing OSS client from a previous NFM-P release, you must review the list of NFM-P schema changes in the *NSP NFM-P XML API Developer Guide* to identify modifications to packages, classes, types, methods, and properties that the OSS client uses.

See the *NSP NFM-P XML API Developer Guide* for information about how to obtain the required samOss.jar file, and how to configure and test a JMS connection.

16.6 NFM-P system upgrade restrictions

16.6.1 Description

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 a main server upgrade, specific NFM-P configuration and log files are copied to a time-stamped directory in the installation directory, and specific directories below the installation directory are deleted.

If you create or modify a file under the main server installation directory, you risk losing the file during an upgrade unless you first back up the file to a location that is unaffected by the upgrade.

CAUTION

Upgrade failure

An NFM-P main server upgrade fails if each main server in the system is not fully initialized and functional before the upgrade.

Before you attempt to upgrade a main server, you must ensure that the initialization of each main server in the NFM-P system is complete.

The following restrictions apply to an NFM-P system upgrade.

- A redundant system upgrade requires a network-management outage and must be performed only during a scheduled maintenance period of sufficient duration.

Note: An NFM-P server upgrade applies a default set of file permissions to each directory below the main or auxiliary 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.

16.7 General NFM-P Release 22.9 or later upgrade workflow

16.7.1 Description

The following is the sequence of high-level actions required to upgrade an NFM-P system.

Note: The workflow applies to an upgrade in a staging environment or in a live network.

16.7.2 Stages

Pre-upgrade

1

Perform 16.8 “To prepare for an NFM-P system upgrade from Release 22.9 or later” (p. 824) to collect the required information and to ensure that the correct upgrade conditions are in place.

2

If SELinux is enabled in the NFM-P, and you want SELinux enabled after the upgrade, perform 16.9 “To prepare an SELinux-enabled NFM-P Release 22.9 or later system for an upgrade” (p. 837) to ensure that SELinux is enabled and in permissive mode before the upgrade.

Upgrade

3

Perform one of the following.

a. Upgrade a standalone NFM-P system; see “Standalone NFM-P system upgrade from Release 22.9 or later” (p. 839).

b. Upgrade a redundant NFM-P system; see “Redundant NFM-P system upgrade from Release 22.9 or later” (p. 869).

Post-upgrade

4

If either of the following is true, perform “How do I enable SELinux enforcing mode for the NFM-P?” in the *NSP System Administrator Guide* to switch from SELinux permissive mode to enforcing mode.

- You have performed 16.9 “To prepare an SELinux-enabled NFM-P Release 22.9 or later system for an upgrade” (p. 837) to set SELinux in permissive mode before the upgrade, and want to restore the use of enforcing mode.
- The upgrade has enabled SELinux in the NFM-P for the first time, but in permissive mode, and you want the more stringent security of enforcing mode.

NFM-P pre-upgrade procedures for Release 22.9 or later

16.8 To prepare for an NFM-P system upgrade from Release 22.9 or later

16.8.1 Description

CAUTION

Upgrade failure

An NFM-P system upgrade fails if each main server in the system is not fully initialized and functional before the upgrade.

Before you attempt an NFM-P system upgrade, you must ensure that the initialization of each main server in the NFM-P system is complete.

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

16.8.2 Steps

CAUTION

Deployment failure

The RHEL OS of any NSP component requires specific versions of some RHEL packages. If the required package versions are not installed, the component upgrade fails.

See “Manual NSP RHEL OS installation” (p. 70) for the required package versions.

Check component hardware

1

Perform a file system check on each component by entering the following for each file system device as the root user on the component station:

```
# e2fsck -n file_system ↵
```

where *file_system* is a specification such as /dev/sda*n* for a physical disk, or /dev/vda*n* for a virtual disk

If the check passes, the output is similar to the following

```
/dev/sdan: clean, a/b files, x/y blocks
```

If the check indicates a failure, you must correct the disk corruption before you continue.

2

Check each component station for system error messages; enter the following as the root user on the station:

```
# grep -i error /var/log/messages ↵
```

If no error messages are present, the command returns nothing. Otherwise, investigate and resolve the issues indicated by the error messages that are displayed.

3

Perform “How do I test NFM-P disk performance?” in the *NSP System Administrator Guide* on each component station to ensure that the disk speed and latency meet or exceed your system requirements.

Check component OS configuration

4

Verify that the /etc/hosts file contains the required host entry for each NFM-P component; enter the following as the root user on each station, and ensure that each required entry is present and correctly specified, as described in 13.5.3 “Network requirements” (p. 371):

```
# cat /etc/hosts ↵
```

5

Verify that the /etc/nsswitch.conf file is configured correctly; enter the following as the root user on each component station:

```
# cat /etc/nsswitch.conf ↵
```

Ensure that “files” is the first entry for passwd, shadow, group, and hosts, as shown in the following:

```
passwd:     files nis
shadow:     files nis
group:      files nis
hosts:      files dns myhostname
```

6

Verify that the OS version is compatible with the NFM-P release, as described in the *NSP Planning Guide*; enter the following as the root user on each component station:

```
# cat /etc/redhat-release ↵
```

```
Red Hat Enterprise Linux Server release R.r (codename)
```

7

Verify that the disk partitions are correctly allocated and sized; enter the following commands as the root user on each component station, and check the output against the specifications in Chapter 2, “NSP disk setup and partitioning”:

```
# lsblk ↵
# df -PH ↵
```

8

Verify that the required RHEL OS packages are installed; enter the following as the root user on each component station; see Chapter 3, “RHEL OS deployment for the NSP” for information about the required packages:

```
# dnf list installed ↵
```

Verify NE resynchronization status

9

Use the Discovery Manager in the NFM-P GUI to ensure that no NEs are undergoing or pending resynchronization.

1. Open an NFM-P GUI client.
2. Choose Administration→Discovery Manager from the NFM-P main menu. The Discovery Manager (Edit) form opens.
3. Click on the Resync Status tab.
4. Ensure that no NEs are in either of the following states:
   - In Progress
   - Requested
5. Close the Discovery Manager form.

Verify NFM-P license

10

Verify that you have a valid license; perform the following steps on each main server station.

Note: Ensure that you do not modify the contents of a license file; otherwise, the license is unusable.

1. Enter the following as the root user:

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

   The station UUID is displayed.
2. Record the UUID.
3. Unzip the license file; enter the following:

   ```
   # tar -xvf license_file ↵
   ```

where *license_file* is the path of the compressed license file

The nfmpLicense.xml file is extracted to the current directory.

4. Open the nfmpLicense.xml file for viewing.
5. Review the license parameters to ensure the following:
    - The UUIDs match the station UUIDs; if the same license is used for the two main servers in a redundant deployment, the license includes both UUIDs.
    - The license is for the correct release. A license is specific to a major release only; a new license is not required for an upgrade to a different minor release in the same major release.
    - The license enables the required functions.
    - The licensed capacities are correct and sufficient for you network.

Back up NFM-P configuration

11

Copy the following configuration files to a secure location on a station that is not affected by the upgrade:

- from each main server station:
    - contents of /opt/nsp/nfmp/server/nms/config
    - /opt/nsp/nfmp/config/nms/config/main_config.xml
- from each auxiliary server station:
    - contents of /opt/nsp/nfmp/auxserver/nms/config
    - /opt/nsp/nfmp/config/nms/config/aux_config.xml
- from each main database station:
    - /opt/nsp/nfmp/samdb/install/config/dbconfig.properties
    - /opt/nsp/nfmp/config/nms/config/db_config.xml

Remove outdated logs

12

An NFM-P main server may retain logs saved during a previous upgrade in the following directory:

/opt/nsp/nfmp/server/nms/log/previous_log

The files in the directory may consume excessive disk space. If the directory exists on a main server, it is strongly recommended that you remove the files from the directory before the upgrade.

a. Move the files to a secure archive location on a station that does not host an NSP component.

b. Delete the files.

Check and configure firewalls

13

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 allows the required traffic to pass. See the *NSP 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 Planning Guide*, which describes using NFM-P templates for rule creation.

b. Disable each firewall; see the external firewall documentation, or perform 3.19 “To disable the RHEL firewalld service” (p. 91).

Download installation files

14

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.

- 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
- nsp-nfmp-nodeexporter-*R.r.p*-rel.*v*.rpm, if the NFM-P is in a shared-mode deployment and you want to forward NFM-P system metrics to the NSP
- 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

15

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.

16

Transfer the following downloaded file to an empty directory on the main database station:

- OracleSw_PreInstall.sh

17

Navigate to the directory that contains the OracleSw_PreInstall.sh file.

18

Enter the following:

```
# chmod +x OracleSw_PreInstall.sh ↵
```

19

Perform the following steps to validate the Oracle database and resolve any conflicts that may prevent an upgrade.

Note: If the validation check reports a small number of errors, for example, a few duplicate and invalid instances of an object, deleting the invalid instances manually may be sufficient. A large number of errors may indicate a significant problem that requires expert attention; in such a case, contact technical support for assistance.

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 20.
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

20

If the system is redundant, ensure that no archive log gap exists between the primary and standby main databases.

ℹ **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 21.
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 reinstantiation begins, and the GUI status bar displays reinstantiation information.

   Note: Database reinstantiation 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.
7. When the reinstantiation is complete, close the System Information form.

Back up database

21

Open an NFM-P GUI client.

22

Choose Administration→Database from the main menu. The Database Manager form opens.

23

Click on the Backup tab.

24

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 NSP 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: If the NFM-P system is independent, rather than part of a shared-mode NSP deployment, a main database backup performed using the NFM-P client GUI also backs up the local Neo4j and PostgreSQL databases; a backup performed from a CLI does not. The Neo4j and PostgreSQL backup files may be required in the event that the upgrade fails and is to be rolled back.
The Neo4j and PostgreSQL backup files are stored on the standalone or primary main server in the /opt/nsp/os/backup directory.

Configure the following parameters:

- Manual Backup Directory
- Enable Backup File Compression

25

Click Apply.

26

Click Full Backup.

27

Click OK. The database backup begins, and the Backup State indicator reads In Progress.

ℹ **Note:** Depending on the database size, a backup may take considerable time.

28

Monitor the Backup State indicator, which is dynamically updated. The indicator displays Success when the backup is complete.

29

When the backup is complete, close the Database Manager (Edit) form.

30

Transfer the following backup file sets to a secure location on a separate station that is unaffected by the upgrade activity:

- Oracle database—copy from the specified backup location in Step 24 on the standalone or primary main database station
- Neo4j and PostgreSQL databases—copy from the /opt/nsp/os/backup directory on the standalone or primary main server station

Back up custom configuration files

31

⚠ **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.

ℹ **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.

Verify compatibility with external systems

32

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

33

Close the LogViewer utility, if it is open.

Validate main server and GUI client firewall configuration

34

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 Planning Guide* for NFM-P port assignment information.

Verify NFM-P compatibility with managed NEs

35

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 Network Element Compatibility Guide*.

Note: See also 13.5 “NFM-P deployment requirements” (p. 370) for additional important device-specific compatibility requirements.

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.

Perform one of the following for each managed NE at an unsupported release.

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, as described in the *NSP NFM-P User Guide*.

   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. If the NE is a pre-provisioned NE, delete the pre-provisioned NE using the NFM-P Pre-Provisioned NE Manager.

Clear CPAM checkpoints

36

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

37

Choose Administration→System Information from the main menu. The System Information form opens.

38

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

39

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

40

If the system includes one or more auxiliary servers, click on the Auxiliary Servers tab; otherwise, go to Step 44.

A list of auxiliary servers is displayed.

41

Perform the following steps for each auxiliary server listed on the form.

1. Select the auxiliary server and click Properties. The Auxiliary Server [Edit] 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 [Edit] form.

42

Click on the Auxiliary Services tab. Each Preferred auxiliary server entry has a check mark in the Selected column.

43

Record the hostname or IP address of each Preferred auxiliary server.

Note: The auxiliary servers are collectively referred to as the [Aux1] auxiliary servers In 16.14 “To upgrade a redundant Release 22.9 or later NFM-P system” (p. 877). Any other listed auxiliary servers are the Reserved auxiliary servers, and are collectively referred to as [Aux2] in the procedure.

44

If the system includes one or more client delegate servers, click on the Client Delegate Servers tab. Otherwise, go to Step 46.

45

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.

46

Close the System Information form.

47

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

48

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

49

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.
2. Choose Administration→Security→NFM-P User Security from the main menu. The NFM-P User Security - Security Management (Edit) form opens.
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.
10. Close the NFM-P User Security - Security Management (Edit) form.

Uninstall Mac OS X clients

50

Uninstall each single-user client installed on Mac OS X.

> **Note:** You must use the uninstallation procedure in the documentation for the installed client release, and not the uninstallation procedure in this guide.

Close GUI client

51

If the GUI client that you are using is not required for network monitoring during the upgrade, close the client.

END OF STEPS

16.9 To prepare an SELinux-enabled NFM-P Release 22.9 or later system for an upgrade

16.9.1 Purpose

Perform this procedure if:

- You are about to upgrade an NFM-P system.

AND

- SELinux has been enabled in the NFM-P system as described in “How do I enable SELinux on the NFM-P?” in the *NSP System Administrator Guide*.

In order to upgrade an NFM-P system in which SELinux is enabled before the upgrade, the following conditions must be true during the upgrade; performing this procedure ensures that the conditions are met.

- SELinux remains enabled in the system.
- SELinux is in permissive mode.

See “What is SELinux?” in the *NSP System Administrator Guide* for information about configuring SELinux.

> **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

16.9.2 Steps

1

As the root user, enter the following on each main server, main database, and auxiliary server station to verify that SELinux is enabled:

```
# sestatus ↵
```

SELinux is enabled if the following is displayed:

```
SELinux status: enabled
```

2

Perform one of the following:

a. If SELinux is not enabled, perform “How do I enable SELinux on the NFM-P?” in the *NSP System Administrator Guide*.

b. Enter the following as the root user on each main server, main database, and auxiliary server station to switch to SELinux permissive mode:

Note: You do not need to stop any NFM-P processes in order to switch from enforcing mode to permissive mode.

```
# /opt/nsp/nfmp/config/selinux/tools/bin/selinuxenable.sh -p ↵
```

3

Enter the following as the root user on each main server, main database, and auxiliary server station to verify that SELinux is enabled in permissive mode:

```
# getenforce ↵
```

SELinux is in permissive mode if the following is displayed:

```
Permissive
```

4

Close the open console windows.

END OF STEPS

Standalone NFM-P system upgrade from Release 22.9 or later

16.10 Workflow to upgrade a standalone Release 22.9 or later NFM-P system

16.10.1 Description

The following is the sequence of high-level actions required to upgrade a standalone NFM-P system at Release 22.9 or later.

16.10.2 Stages

ℹ **Note:** The "Upgrade standalone system" (p. 839) links lead to sections in 16.11 "To upgrade a standalone Release 22.9 or later NFM-P system" (p. 841).

Prepare system for upgrade

1

Perform 16.8 "To prepare for an NFM-P system upgrade from Release 22.9 or later" (p. 824).

Upgrade standalone system

2

Check the available disk space; see "Check pre-upgrade disk space" (p. 842).

3

Open a GUI client for network monitoring; see "Open GUI client" (p. 842).

4

If the system includes one or more NSP analytics servers or Flow Collectors, stop each; see "Stop NSP analytics servers, Flow Collectors" (p. 843).

5

Prepare the main server for the upgrade; see "Stop and disable standalone main server" (p. 843).

1. Stop the main server.
2. Disable automatic main server startup.

6

Upgrade the main database; see "Upgrade standalone main database" (p. 845).

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.

7

If the system includes one or more auxiliary servers, stop the auxiliary servers; see "Stop auxiliary servers" (p. 851).

8

Upgrade the main server; see "Upgrade standalone main server" (p. 851).

9

Start the PKI server; see "Start PKI server" (p. 853).

10

Configure the main server; see "Configure standalone main server" (p. 853).

11

If the NFM-P is not in a shared-mode NSP deployment, restore the local NSP databases; see "Restore embedded nspOS, independent deployment" (p. 855).

12

If required, enable Windows Active Directory for client access; see "Enable Windows Active Directory access" (p. 857).

13

If required, configure ADFS to enable Common Access Card, or CAC, client access; see "Enable CAC access" (p. 859).

14

If the NFM-P is integrated with a WS-NOC system, configure the integration; see "Configure WS-NOC integration" (p. 862).

15

If the system includes one or more auxiliary servers, upgrade each auxiliary server; see "Upgrade auxiliary servers" (p. 863).

16

If the system includes one or more NSP Flow Collectors, upgrade each NSP Flow Collector Controller and Flow Collector; see "Upgrade NSP Flow Collector Controllers, Flow Collectors" (p. 864).

17

If the system includes an auxiliary database, upgrade the auxiliary database; see “Upgrade auxiliary database” (p. 864).

18

If the system includes one or more auxiliary servers, start each auxiliary server; see “Start auxiliary servers” (p. 864).

19

Start the main server; see “Start main server” (p. 864).

20

Recheck the available disk space; see “Check post-upgrade disk space” (p. 866).

21

If the system includes one or more NSP analytics servers, upgrade each analytics server; see “Upgrade NSP analytics servers” (p. 866).

22

Install or upgrade single-user GUI clients, as required; see “Install or upgrade single-user GUI clients” (p. 866).

23

Install or upgrade client delegate servers, as required; see “Install or upgrade client delegate servers” (p. 867).

24

Stop the PKI server; see “Stop PKI server” (p. 867).

25

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. 867).

26

Configure and enable firewalls, if required; see “Configure and enable firewalls” (p. 867).

16.11 To upgrade a standalone Release 22.9 or later NFM-P system

16.11.1 Description

The following steps describe how to upgrade a collocated or distributed Release 22.9 or later NFM-P 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

16.11.2 Steps

Check pre-upgrade disk space

1

As part of the trial upgrade on a lab system in advance of a live upgrade, you must ensure that the available disk capacity on each NFM-P component remains within tolerance.

Note: If the disk usage on an NFM-P partition approaches or exceeds 80% after the trial upgrade, you may need to add disk capacity before you attempt the upgrade on a live system.

Perform the following steps on each of the following stations:

- main server
- auxiliary server
- main database
- auxiliary database

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following:

   ```
   # df -kh ↵
   ```

   The usage information for each partition is displayed.
4. Record the information for each NFM-P partition; see the tables in Chapter 2, “NSP disk setup and partitioning” for the partition names and required capacities.

Open GUI client

2

Open at least one GUI client to monitor the network before the upgrade.

Stop NSP analytics servers, Flow Collectors

3

If the system includes one or more NSP 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/analytics/bin/AnalyticsAdmin.sh stop ↵
```

The following is displayed:

```
Stopping Analytics Application
```

When the analytics server is completely stopped, the following message is displayed:

```
Analytics Application is not running
```

4

If the system includes one or more NSP Flow Collector Controllers and Flow Collectors, stop each NSP Flow Collector Controller.

Note: If the NSP Flow Collector Controller is collocated on a station with an NSP Flow Collector, stopping the NSP Flow Collector Controller also stops the Flow Collector.

1. Log in to the NSP Flow Collector Controller station as the nsp user.
2. Open a console window.
3. Enter the following:

```
bash$ /opt/nsp/flow/fcc/bin/flowCollectorController.bash stop ↵
```

The NSP Flow Collector Controller stops.

5

If the system includes one or more NSP Flow Collectors that are not collocated on a station with a Flow Collector Controller, stop each such NSP Flow Collector.

1. Log in to the NSP Flow Collector station as the nsp user.
2. Open a console window.
3. Enter the following:

```
bash$ /opt/nsp/flow/fc/bin/flowCollector.bash stop ↵
```

The NSP Flow Collector stops.

Stop and disable standalone main server

6

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.

6. Enter the following to switch to the root user:

   ```
   bash$ su ↵
   ```

7. If the NFM-P is not in a shared-mode NSP deployment, enter the following to display the NSP service status:

   ```
   # nspdctl status ↵
   ```

   Information like the following is displayed.

   ```
   Mode:      standalone
   Role:      —
   DC-Role:   —
   DC-Name:   dc_name
   Registry:  IP_address:port
   State:     stopped
   Uptime:    0s
   SERVICE            STATUS
   service_a          inactive
   service_b          inactive
   service_c          inactive
   ```

   You must not proceed to the next step until all NSP services are stopped; if the State is not ‘stopped’, or the STATUS indicator of each listed service is not ‘inactive’, repeat this substep.

7

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:

   ```
   # systemctl disable nspos-nspd.service ↵
   ```

2. Enter the following:

   ```
   # systemctl disable nfmp-main-config.service ↵
   ```

3. Enter the following:

```
# systemctl disable nfmp-main.service ↵
```

Upgrade standalone main database

8

Log in to the database station as the root user.

9

Open a console window.

10

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 ↵
   ```

11

Perform the following steps.

1. Perform 3.4 “To apply a RHEL update to an NSP image-based OS” (p. 67)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 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 ↵
   ```

12

If you are re-using the main database station, recommission the station according to the platform specifications in this guide and in the *NSP Planning Guide*.

For information about deploying the RHEL OS using an NSP OEM disk image, see 2.2.2 “NSP disk-image deployment” (p. 28).

13

Log in as the root user on the main database station.

14

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 collocated 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. You must remove the semvalidator package if it is installed; otherwise, the upgrade is blocked.

      Enter the following:

      ```
      # rpm -q nsp-nfmp-semvalidator ↵
      ```

      If the package is installed, the following is displayed:

      ```
      nsp-nfmp-semvalidator-version
      ```

      If the package is not installed, the following is displayed:

      ```
      package nsp-nfmp-semvalidator is not installed
      ```
   3. If the package is installed, enter the following:

      ```
      # dnf remove nsp-nfmp-semvalidator ↵
      ```

      The package is removed.

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
   - nsp-nfmp-nodeexporter-*R.r.p*-rel.*v*.rpm, if downloaded

   Note: In subsequent steps, the directory is called the NFM-P software directory.

15

Transfer the following downloaded file to an empty directory on the main database station:

- OracleSw_PreInstall.sh

16

Navigate to the directory that contains the OracleSw_PreInstall.sh file.

17

Enter the following:

```
# chmod +x OracleSw_PreInstall.sh ↵
```

18

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.

Do you want to continue? [Yes/No]:
```

19

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 NFM-P main database version = version

Enter the password for the "SYS" Oracle user (terminal echo is off):
```

20

Enter the SYS user password.

The following messages and prompt are displayed:

```
Validateing the database for upgrade. Please wait ...

INFO: Database upgrade validation passed.

Create/Update base nsp/oracle user directories

Creating group group if it does not exist ...

Checking or Creating the Oracle user home directory
/opt/nsp/nfmp/oracle19...

Checking user username... usermod: no changes

Changing ownership of the directory /opt/nsp/nfmp/oracle19 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]:
```

21

Enter No.

The following messages 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]:
```

22

Enter Yes or No, as required.

Messages like the following are displayed as the script execution completes:

```
INFO: Created /etc/sysctl.d/97-nfmp-oracle.conf, not a reconfig
scenario, not applying changes at this time.
INFO: Removing ulimit file /etc/security/limits.d/97-nfmp-oracle.conf
INFO: About to set ulimit parameters in /etc/security/limits.
d/97-nfmp-oracle.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.
d/97-nfmp-oracle.conf...
INFO: Completed running Oracle Pre-Install Tasks, you *MUST* reboot
your box.
```

23

When the script execution is complete, enter the following to reboot the station:

```
# systemctl reboot ↵
```

The station reboots.

24

When the reboot is complete, log in as the root user on the main database station.

25

Open a console window.

26

Navigate to the NFM-P software directory.

Note: Ensure that the directory contains only the installation files.

27

Enter the following:

```
# chmod +x * ↵
```

28

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/N]:
```

29

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

30

Enter the following to upgrade the database:

Note: A database upgrade takes considerable time that varies, depending on the release from which you are upgrading.

```
# samupgradeDb ↵
```

The following prompt is displayed:

```
Enter the password for the "SAMUSER" database user (terminal echo is
off):
```

31

Enter the password.

The database upgrade begins, and messages like the following are displayed:

```
Validation succeeded.
```

```
Upgrade log is /opt/nsp/nfmp/db/install/NFM-P_Main_Database.upgrade.
timestamp.stdout.txt
Performing Step 1 of n - Initializing ..........
Performing NFM-P database upgrade will take time...
Executing PreOraUpgrade.sql ............
Executing ShutdownDBUpgrade.sql ....
Executing StartupDB.sql .....
Executing DbJavaReload.sql ...............
```

The database upgrade is complete when the following is displayed:

```
DONE
```

32

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; see 14.9 “NFM-P samconfig utility” (p. 432) for information about using samconfig.
4. Configure one or more parameters, if required, and then enter **back** ↵.
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.

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 the *NSP System Administrator Guide* for information.

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

34

If the system includes one or more auxiliary servers, stop 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 auxstop ↵
```

The auxiliary server stops.

Upgrade standalone main server

35

If the main server and database are on separate stations and deployed in VMs created using an NSP RHEL OS disk image, perform 3.4 “To apply a RHEL update to an NSP image-based OS” (p. 67) on the main server station.

36

Log in as the root user on the main server station.

37

Open a console window.

38

Perform one of the following.

a. If the main server and database are collocated on one station, go to Step 45.

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
- nsp-nfmp-nodeexporter-*R.r.p*-rel.*v*.rpm, if downloaded

Note: In subsequent steps, the directory is called the NFM-P software directory.

39

You must remove the semvalidator package if it is installed; otherwise, the upgrade is blocked.

Perform the following steps.

1. Enter the following:

```
# rpm -q nsp-nfmp-semvalidator ↵
```

If the package is installed, the following is displayed:

```
nsp-nfmp-semvalidator-version
```

If the package is not installed, the following is displayed:

```
package nsp-nfmp-semvalidator is not installed
```

2. If the package is installed, enter the following:

```
# dnf remove nsp-nfmp-semvalidator ↵
```

The package is removed.

40

Navigate to the NFM-P software directory.

Note: Ensure that the directory contains only the installation files.

41

Enter the following:

```
# chmod +x * ↵
```

42

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

43

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

Start PKI server

44

Start the PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 4.10 “To configure and enable a PKI server” (p. 113).

Note: The PKI server is required for internal system configuration purposes.

Configure standalone main server

45

Enter the following; see 14.9 “NFM-P samconfig utility” (p. 432) 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>
```

46

Enter the following:

```
<main> configure ↵
```

The prompt changes to `<main configure>`.

47

To apply a new or updated NFM-P license, 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 the *NSP System Administrator Guide*.

```
<main configure> license license_file back ↵
```

where *license_file* is the absolute path and file name of the NSP license bundle

48

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; see 14.9 “NFM-P samconfig utility” (p. 432) for information about using the samconfig utility.

3. Configure one or more parameters, if required.

   Note: The NFM-P uses the database backup settings to initialize the database during installation only. To change the backup settings after installation, you must use the Database Manager form in the NFM-P client GUI, as described in the *NSP System Administrator Guide*.

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

   ```
   <main configure> back ↵
   ```

   The prompt changes to `<main>`.

49

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

50

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

51

If the NFM-P is part of a shared-mode NSP system and you want to enable mTLS for internal Kafka authentication using two-way TLS, perform the following steps.

Note: Enabling mTLS for internal Kafka authentication is supported only in an NSP deployment that uses separate interfaces for internal and client communication.

Note: The parameter you must configure is displayed only if the ip-list parameter is set to a remote address.

Note: The parameter is configurable only if the **secure** and **internal-certs** parameters in the **nspos** section are set to true.

1. Enter the following:

   ```
   # samconfig -m main ↵
   ```

   The following is displayed:

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

2. Enter the following:

   ```
   # configure nspos mtls-kafka-enabled back ↵
   ```

3. Enter the following:

   ```
   <main> apply ↵
   ```

   The configuration is applied.

4. Enter the following:

   ```
   <main> exit ↵
   ```

   The samconfig utility closes.

Restore embedded nspOS, independent deployment

52

In an independent NFM-P deployment, you must restore the embedded Neo4j and PostgreSQL databases. Otherwise, if the NFM-P is integrated with an NSP cluster, go to Step 58.

53

Enter the following:

```
# mkdir /opt/nsp/os/backup ↵
```

54

Enter the following:

```
# chown nsp:nsp /opt/nsp/os/backup ↵
```

55

Copy the Neo4j and PostgreSQL backup files saved in Step 24 of 16.8 “To prepare for an NFM-P system upgrade from Release 22.9 or later” (p. 824) to the /opt/nsp/os/backup directory.

56

Restore the Neo4j database.

1. Enter the following:

   ```
   # cd /opt/nsp/os/install/tools/database ↵
   ```

2. Enter the following:

   ```
   # ./db-restore.sh --target IP_address ↵
   ```

   where *IP_address* is the main server IP address

   The following message and prompt are displayed:

   ```
   Verifying prerequisites...
   Starting database restore ...
   Backupset file to restore (.tar.gz format):
   ```

3. Enter the following and press ↵:

   ```
   path/nspos-neo4j_backup_timestamp.tar.gz
   ```

   where

   path is the absolute path of the Neo4j backup file

   timestamp is the backup creation time

   Note: Neo4j backup files are stored in the following locations on a main server, depending on the backup type:

- scheduled backup—/opt/nsp/os/backup/backupset_*n*
- manual backup—/opt/nsp/os/backup/manual_*timestamp*

The following messages and prompt are displayed:

```
PLAY [all] *************************************************

TASK [dbrestore : Create temporary directory] ***************

changed: [server_IP]

[dbrestore : pause]

Do you want to restore the nspOS Neo4j db from file:
path/nspos-neo4j_backup_timestamp.tar.gz? Press return to continue,
or Ctrl+C to abort:
```

4. Press ↵.

   The restore operation begins, and messages like the following are displayed:

```
TASK [dbrestore : Copy backupset] ***************************

changed: [server_IP]

TASK [dbrestore : Running nspdctl stop] *********************

changed: [server_IP]

TASK [dbrestore : Ensure database service is stopped] *******

changed: [server_IP]

TASK [dbrestore : Perform database restore] *****************

changed: [server_IP]

TASK [dbrestore : Delete temporary directory] ***************

changed: [server_IP]

PLAY RECAP *************************************************

server_IP     : ok=n   changed=n    unreachable=n   failed=n
```

5. If the `failed` value is greater than zero, a restore failure has occurred; contact technical support for assistance.

57

Restore the PostgreSQL database.

1. Enter the following:

   `# ./db-restore.sh --target IP_address ↵`

   where *IP_address* is the main server IP address

   The following message and prompt are displayed:

```
Verifying prerequisites...

Starting database restore ...

Backupset file to restore (.tar.gz format):
```

2. Enter the following and press ↵:

```
path/nspos-postgresql_backup_timestamp.tar.gz
```

where

path is the absolute path of the PostgreSQL backup file

timestamp is the backup creation time

Note: PostgreSQL backup files are stored in the following locations on a main server, depending on the backup type:

- scheduled backup—/opt/nsp/os/backup/backupset_*n*
- manual backup—/opt/nsp/os/backup/manual_*timestamp*

The following messages and prompt are displayed:

```
PLAY [all] **************************************************

[dbrestore : pause]

Do you want to restore the nspOS PostgreSQL db from file:
path/nspos-postgresql_backup_timestamp.tar.gz? Press return to
continue, or Ctrl+C to abort:
```

3. Press ↵.

   The restore operation begins, and messages like the following are displayed:

```
TASK [dbrestore : Running nspdctl stop] *********************

changed: [server_IP]

TASK [dbrestore : Perform database restore] *****************

changed: [server_IP]

TASK [dbrestore : Delete temporary directory] ***************

changed: [server_IP]

PLAY RECAP **************************************************

server_IP      : ok=n   changed=n    unreachable=n   failed=n
```

4. If the `failed` value is greater than zero, a restore failure has occurred; contact technical support for assistance.

Enable Windows Active Directory access

58

If you intend to use Windows Active Directory, or AD, for single-sign-on client access, you must configure LDAP remote authentication for AD; otherwise, go to Step 77.

Open the following file as a reference for use in subsequent steps:

/opt/nsp/os/install/examples/config.yml

Note: Consider the following.

- The NFM-P does not assign a default user group to users of a remote authentication source that you define for Windows AD; the authentication source must provide the user group attributes.
- Windows AD supports the following LDAP server types for remote authentication:

  AD—The user group of an AD user is derived from the group_base_dn attribute in the server configuration; group search filters are not supported.

AUTHENTICATED—The server configuration must include bind credentials; group search filters are supported. After NFM-P initialization, you add the AD server bind credentials to the NSP password vault using the NSP Session Manager REST API.

59

Locate the section that begins with the following lines:

```
#   ldap:
#     enabled: true
#     servers:
#       - type: AUTHENTICATED/AD/ANONYMOUS
#         url: ldaps://ldap.example.com:636
#         security: SSL/STARTTLS/NONE
```

60

Open the following file using a plain-text editor such as vi:

/opt/nsp/os/install/config.json

61

Locate the section that begins with the following line:

```
"sso": {
```

The section has one subsection for each type of SSO access.

Note: You can enable multiple remote authentication methods such as LDAP and RADIUS in the config.json file, or by using the NFM-P GUI. Using the GUI also allows you to specify the order in which the methods are tried during login attempts; however, no ordering is applied to multiple methods enabled in the config.json file.

62

In the **sso** section, create an **ldap** subsection as shown below using the parameter names from the **ldap** section of config.yml and the required values for your configuration.

The following example shows the LDAP configuration for two AD servers:

```
"ldap": {
"enabled": true,
"servers": [
{
"type": "auth_type",
"url": "ldaps://server1:port",
"server1_parameter_1": "value",
"server1_parameter_2": "value",
.
.
"server1_parameter_n": "value",
},
{
"type": "auth_type",
"url": "ldaps://server2:port",
"server2_parameter_1": "value",
"server2_parameter_2": "value",
.
.
"server2_parameter_n": "value",
},
}]
}
```

where *auth_type* is AD or AUTHENTICATED

63

Save and close the files.

64

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

65

Enter the following:

```
<main> apply ↵
```

The AD LDAP configuration is applied.

66

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Enable CAC access

67

If you do not intend to enable Common Access Card, or CAC, technology for NFM-P client access, go to Step 77.

68

Download the federationmetadata.xml from the following ADFS link:

https://*ADFS_server_name*/FederationMetadata/2007-06/federationmetadata.xml

where *ADFS_server_name* is the ADFS server FQDN

69

Add an ADFS server entry to the /etc/hosts file on the main server.

1. Open the /etc/hosts file using a plain-text editor such as vi.
2. Add the following line below the line that contains the main server IP address:

   ```
   IP_address FQDN
   ```

   where

   IP_address is the IP address of the ADFS server

   FQDN is the FQDN of the ADFS server
3. Save and close the file.

70

In order to enable CAC for client access, you must configure Active Directory Federation Services, or ADFS.

Open the following file using a plain-text editor such as vi:

/opt/nsp/os/install/config.json

71

In the **sso** section, create an **saml2** subsection as shown below using the parameter names from the **saml2** section of config.yml and the required values for your configuration.

The following example shows the ADFS configuration.

Note: You must preserve the lead spacing of each line.

```
  "sso" : {
    "saml2": {
       "enabled": true,
       "service_provider_entity_id": "NFM-P_identifier",
       "service_provider_metadata_filename": "casmetadata.xml",
       "maximum_authentication_lifetime": 3600,
       "accepted_skew": 300,
       "destination_binding": "urn:oasis:names:tc:SAML:2.0:bindings:
HTTP-Redirect",
       "identity_provider_metadata_path": "ADFS_metadata_file",
       "authn_context_class_ref": "urn:oasis:names:tc:SAML:2.0:ac:
classes:TLSClient",
       "authn_context_comparison_type": "minimum",
       "name_id_policy_format": "urn:oasis:names:tc:SAML:1.1:
nameid-format:unspecified",
       "force_auth": true,
```

```
       "passive": false,
       "wants_assertions_signed": false,
       "wants_responses_signed": false,
       "all_signature_validation_disabled": false,
       "sign_service_provider_metadata": false,
       "principal_id_attribute": "UPN",
       "use_name_qualifier": false,
       "provider_name": "ADFS_server_URI",
       "requested_attributes": [{
         "name": "http://schemas.xmlsoap.
org/ws/2005/05/identity/claims/emailaddress",
          "friendly_name": "E-Mail Address",
          "name_format": "urn:oasis:names:tc:SAML:2.0:attrname-format:
uri",
          "required": false
      } ],
       "mapped_attributes": [{
           "name": "http://schemas.xmlsoap.org/claims/Group",
           "mapped_to": "authorizationProfile"
      }, {
           "name": "http://schemas.xmlsoap.
org/ws/2005/05/identity/claims/upn",
           "mapped_to": "upn"
      } ]
    },
```

72

Configure the following parameters; leave all other parameters at the default:

- "service_provider_entity_id": "*NFM-P_identifier*"
- "identity_provider_metadata_path": "*ADFS_metadata_file*"
- "provider_name": "*ADFS_server_name*"

NFM-P_identifier is the unique ADFS Relying Trust Party identifier

*ADFS_metadata_fil*e is the absolute path of the ADFS metadata XML file, for example, /opt/federationmetadata.xml

ADFS_server_name is the ADFS server FQDN

73

Save and close the files.

74

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

75

Enter the following:

```
<main> apply ↵
```

The ADFS configuration is applied.

76

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Configure WS-NOC integration

77

If the NFM-P is integrated with an WS-NOC system, open the following file with a plain-text editor such as vi; otherwise, go to Step 87.

/opt/nsp/os/install/examples/config.json

See "WS-NOC and NSP integration" (p. 340) for comprehensive information about NFM-P integration with the WS-NOC.

78

Copy the following section:

```
  "nfmt": {
    "primary_ip": "",
    "standby_ip": "",
    "username": "",
    "password": "",
    "cert_provided": false
  },
```

79

Close the file.

80

Open the following file with a plain-text editor such as vi:

/opt/nsp/os/install/config.json

81

Paste in the copied section.

82

Configure the required parameters to enable the WS-NOC integration:

- primary_ip—the primary WS-NOC server IP address
- standby_ip—the standby WS-NOC server IP address
- username—the username required for WS-NOC access
- password—the password required for WS-NOC access
- cert_provided—whether a TLS certificate is used

83

Save and close the file.

84

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

85

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

86

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Upgrade auxiliary servers

87

If the system includes one or more auxiliary servers, perform 16.15 “To upgrade a Release 22.9 or later NFM-P auxiliary server” (p. 940) on each auxiliary server station.

Upgrade NSP Flow Collector Controllers, Flow Collectors

88

If the system includes one or more NSP Flow Collectors, upgrade each NSP Flow Collector Controller and Flow Collector as described in "NSP Flow Collector and Flow Collector Controller upgrade from Release 22.9 or later" (p. 799).

Upgrade auxiliary database

89

If the system includes an auxiliary database, perform 16.16 "To upgrade a Release 22.9 or later NFM-P auxiliary database cluster" (p. 944).

Start auxiliary servers

90

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

91

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 the *NSP 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.

92

If you have enabled CAC for NFM-P client access, download the casmetadata.xml file from the following URL, and then import the file into the ADFS server relying-trust-party:

https://*server*/cas/sp/metadata

where *server* is the main server IP address or hostname

After the download, the casmetadata.xml file is available in the following directory on the main server:

/opt/nsp/os/tomcat/conf/cas/saml

93

If you have enabled Windows Active Directory access using the AUTHENTICATED type of LDAP server, perform the following steps.

1. Use the NSP Session Manager REST API to add the LDAP server bind credentials; see the Network Developer Portal for information.
2. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to restart the local nspos-tomcat service:

Note: The service restart may take a few minutes, during which NFM-P GUI and REST client access is degraded. General NFM-P operation is unaffected.

```
# systemctl restart nspos-tomcat ↵
```

94

Specify the memory requirement for GUI clients based on the type of network that the NFM-P is to manage.

1. Enter the following:

```
bash$ ./nmsdeploytool.bash clientmem -option ↵
```

where *option* is one of the following:

- m—medium, for management of limited-scale network
- l—large, for a network of 15 000 or more NEs

2. Record the setting, which is not preserved through an upgrade, for future use.
3. Enter the following to commit the configuration change:

```
bash$ ./nmsdeploytool.bash deploy ↵
```

95

Close the console window.

Check post-upgrade disk space

96

If you are performing a trial upgrade on a lab system in advance of a live upgrade, you must check the available capacity of the disk partitions on each component against the values recorded in Step 1.

Perform the following steps on each of the following stations:

- main server
- auxiliary server
- main database
- auxiliary database

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following:

   ```
   # df -kh ↵
   ```

   The usage information for each partition is displayed.
4. Record the information for each NFM-P partition; see the tables in Chapter 2, “NSP disk setup and partitioning” for the partition names and required capacities.
5. Compare the partition values with the values recorded in Step 1.
6. If the disk usage on an NFM-P partition approaches 80% or has increased substantially, you may need to add disk capacity before you attempt the upgrade on a live system. Contact technical support for assistance.

Upgrade NSP analytics servers

97

If the system includes one or more NSP analytics servers, upgrade each analytics server as described in “NSP analytics server upgrade from Release 22.9 or later” (p. 807).

Install or upgrade single-user GUI clients

98

As required, install or upgrade additional single-user GUI clients; see the following for information:

- “NFM-P single-user GUI client installation” (p. 585)
- “NFM-P single-user GUI client upgrade from Release 22.9 or later” (p. 955)

Install or upgrade client delegate servers

99

As required, install or upgrade client delegate servers; see the following for information:

- "NFM-P client delegate server installation" (p. 591)
- "NFM-P client delegate server upgrade from Release 22.9 or later" (p. 963)

Stop PKI server

100

If no other components are to be deployed, stop the PKI server by entering Ctrl+C in the console window.

Restore TLS version and cipher support configuration

101

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, see the *NSP System Administrator Guide* for information about how to restore the TLS version and cipher support settings.

Note: TLS 1.0 and 1.1 are disabled by default after an upgrade. If either version is enabled before an NFM-P system upgrade and required after the upgrade, you must re-enable the version support after the upgrade.

Configure and enable firewalls

102

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 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 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 upgrade from Release 22.9 or later

16.12 Component references

16.12.1 Description

CAUTION

Service Disruption

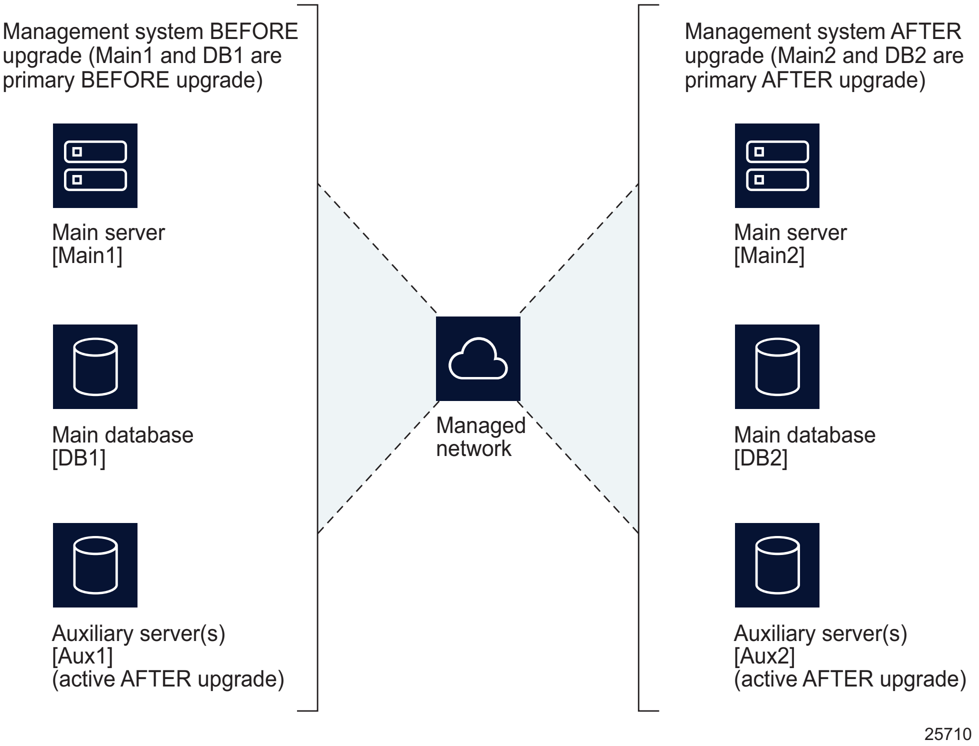
A redundant NFM-P system upgrade involves a network management outage.

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.

Figure 16-1 NFM-P component reference diagram


Management system BEFORE upgrade (Main1 and DB1 are primary BEFORE upgrade)
Main server [Main1]
Main database [DB1]
Auxiliary server(s) [Aux1] (active AFTER upgrade)
Managed network
Management system AFTER upgrade (Main2 and DB2 are primary AFTER upgrade)
Main server [Main2]
Main database [DB2]
Auxiliary server(s) [Aux2] (active AFTER upgrade)
25710

16.13 Workflow to upgrade a redundant Release 22.9 or later NFM-P system

16.13.1 Description

The following is the sequence of high-level actions required to upgrade a redundant NFM-P system at Release 22.9 or later.

16.13.2 Stages

Note: The “Upgrade redundant system” (p. 871) links lead to sections in 16.14 “To upgrade a redundant Release 22.9 or later NFM-P system” (p. 877).

Prepare system for upgrade

1

Perform 16.8 “To prepare for an NFM-P system upgrade from Release 22.9 or later” (p. 824).

Upgrade redundant system

2

Check the available disk space; see "Check pre-upgrade disk space" (p. 878).

3

Stop and disable the standby main server; see "Stop and disable standby main server [Main2]" (p. 878).

4

If the system includes auxiliary servers, stop the [Aux2] auxiliary servers; see "Stop auxiliary servers [Aux2]" (p. 880).

5

Disable the system redundancy functions; see "Disable database redundancy" (p. 880).

6

Upgrade the standby main database, which becomes the new primary main database; see "Upgrade standby main database [DB2]" (p. 881).

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.

7

Upgrade the standby main server; see "Upgrade standby main server [Main2]" (p. 888).

8

Start the PKI server; see "Start PKI server" (p. 890).

9

Configure the new primary main server; see "Configure new primary main server [Main2]" (p. 890).

10

If the NFM-P is not in a shared-mode NSP deployment, restore the local NSP databases on the new primary main server; see "Restore embedded nspOS, independent deployment" (p. 892).

11

If required, enable Windows Active Directory for client access; see "Enable Windows Active Directory access" (p. 894).

12

If required, configure ADFS to enable Common Access Card, or CAC, client access; see "Enable CAC access" (p. 896).

13

If the NFM-P is integrated with an WS-NOC system, configure the integration; see "Configure WS-NOC integration" (p. 899).

14

If the NFM-P system includes one or more NSP analytics servers or Flow Collectors, stop each; see "Stop NSP analytics servers, NSP Flow Collectors" (p. 900).

15

If the NFM-P system includes auxiliary servers, upgrade the [Aux2] auxiliary servers; see "Upgrade auxiliary servers [Aux2]" (p. 901).

16

If the system includes redundant auxiliary database clusters, verify the most recent data synchronization; see "Verify auxiliary database synchronization" (p. 901).

17

If the system includes redundant auxiliary database clusters, enable cluster maintenance mode; see "Enable maintenance mode on auxiliary database agent" (p. 903).

18

If the system includes redundant auxiliary database clusters, upgrade the standby cluster; see "Upgrade standby auxiliary database cluster" (p. 904).

19

Stop and disable the original primary main server; see "Stop and disable original primary main server [Main1]" (p. 905).

Note: This stage marks the beginning of the network management outage.

20

If the system includes one or more NSP Flow Collectors, upgrade each NSP Flow Collector Controller and Flow Collector; see "Upgrade NSP Flow Collector Controllers, Flow Collectors" (p. 906).

21

If the NFM-P system includes auxiliary servers, stop the [Aux1] auxiliary servers; see "Stop auxiliary servers [Aux1]" (p. 906).

22

Stop the original primary main database; see “Stop original primary main database [DB1]” (p. 906).

23

If the system includes a standalone auxiliary database cluster, upgrade the cluster; see “Upgrade auxiliary database, if not redundant” (p. 907).

24

If the system includes redundant auxiliary database clusters, enable maintenance mode for the former primary cluster; see “Enable maintenance mode for auxiliary database agent” (p. 907).

25

If the system includes redundant auxiliary database clusters, stop the former primary cluster; see “Stop former primary auxiliary database cluster” (p. 908).

26

Start the new primary main server; see “Start new primary main server [Main2]” (p. 908).

27

If the system includes auxiliary servers, start the [Aux2] auxiliary servers; see “Start auxiliary servers [Aux2]” (p. 910).

28

If the system includes redundant auxiliary database clusters, activate the upgraded former standby cluster, see “Activate upgraded former standby auxiliary database cluster” (p. 910).

29

If the system includes one or more NSP analytics servers, upgrade each analytics server; see “Upgrade analytics servers” (p. 912).

30

Upgrade or install at least one NFM-P single-user client or client delegate server; see “Enable GUI client” (p. 912).

Note: This stage marks the end of the network management outage.

31

Perform sanity testing on the NFM-P system using a GUI client; see “Test upgraded system using GUI client” (p. 912).

32

Uninstall the original primary main database; see “Uninstall original primary database [DB1]” (p. 912).

33

Install the new standby main database; see “Install new standby main database [DB1]” (p. 913).

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.

34

Reinstantiate the standby database; see “Reinstantiate standby database” (p. 919).

35

If the NSP system includes redundant auxiliary database clusters, upgrade the former primary cluster; see “Upgrade former primary auxiliary database cluster” (p. 919).

36

Upgrade the original primary main server as the new standby main server; see “Upgrade original primary main server [Main1]” (p. 920).

37

Configure the new standby main server; see “Configure new standby main server [Main1]” (p. 921).

38

If required, enable Windows Active Directory for client access; see “Enable Windows Active Directory access” (p. 926).

39

If required, configure ADFS to enable Common Access Card, or CAC, client access; see “Enable CAC access” (p. 928).

40

If the NFM-P is integrated with an WS-NOC system, configure the integration; see “Configure WS-NOC integration” (p. 931).

41

Start the new standby main server; see “Start new standby main server [Main1]” (p. 932).

42

If the system includes auxiliary servers, upgrade the [Aux1] auxiliary servers; see “Upgrade auxiliary servers [Aux1]” (p. 933).

43

If the system includes auxiliary servers, start the [Aux1] auxiliary servers; see "Start auxiliary servers [Aux1]" (p. 934).

44

If the system includes redundant auxiliary database clusters, activate each cluster; see "Disable maintenance mode for auxiliary database agents" (p. 934).

45

If the system includes an auxiliary database, verify that the auxiliary database is functioning correctly; see "Verify auxiliary database status" (p. 935).

46

Recheck the available disk space; see "Check post-upgrade disk space" (p. 937).

47

Install or upgrade single-user GUI clients, as required; see "Install or upgrade single-user GUI clients" (p. 938).

48

Install or upgrade client delegate servers, as required; see "Install or upgrade client delegate servers" (p. 938).

49

Stop the PKI server; see "Stop PKI server" (p. 938).

50

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. 938).

51

Configure and enable firewalls, if required; see "Configure and enable firewalls" (p. 938).

16.13.3 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 16-2 Workflow for concurrent task execution during redundant upgrade

System redundancy mode	Operator A actions	Operator B actions
DUPLEX	Stage 1 — Actions described in 16.8 “To prepare for an NFM-P system upgrade from Release 22.9 or later” (p. 824)	
	Stage 2 — “Check pre-upgrade disk space” (p. 878) Stage 3 — “Stop and disable standby main server [Main2]” (p. 878)	Stage 4 — “Stop auxiliary servers [Aux2]” (p. 880) Stage 5 — “Disable database redundancy” (p. 880)
SIMPLEX	Stage 6 — “Upgrade standby main database [DB2]” (p. 881)	Stage 7 — “Upgrade standby main server [Main2]” (p. 888)
	Stage 8 — “Start PKI server” (p. 890) Stage 9 — “Configure new primary main server [Main2]” (p. 890) Stage 10 — “Restore embedded nspOS, independent deployment” (p. 892)	Stage 11 — “Enable Windows Active Directory access” (p. 894) Stage 12 — “Enable CAC access” (p. 896) Stage 13 — “Configure WS-NOC integration” (p. 899)
	Stage 14 — “Stop NSP analytics servers, NSP Flow Collectors” (p. 900)	Stage 16 — “Verify auxiliary database synchronization” (p. 901) Stage 17 — “Enable maintenance mode on auxiliary database agent” (p. 903) Stage 18 — “Upgrade standby auxiliary database cluster” (p. 904)
	Stage 15 — “Upgrade auxiliary servers [Aux2]” (p. 901)	
OUTAGE	Stage 19 — “Stop and disable original primary main server [Main1]” (p. 905)	Stage 23 — “Upgrade auxiliary database, if not redundant” (p. 907)
	Stage 20 — “Upgrade NSP Flow Collector Controllers, Flow Collectors” (p. 906)	Stage 24— “Enable maintenance mode for auxiliary database agent” (p. 907)
	Stage 21 — “Stop auxiliary servers [Aux1]” (p. 906)	Stage 25— “Stop former primary auxiliary database cluster” (p. 908)
	Stage 22 — “Stop original primary main database [DB1]” (p. 906)	Stage 27 — “Start auxiliary servers [Aux2]” (p. 910)
	Stage 26 — “Start new primary main server [Main2]” (p. 908) **Note:** The outage persists until device discovery completes.	Stage 28 — “Activate upgraded former standby auxiliary database cluster” (p. 910)

Table 16-2 Workflow for concurrent task execution during redundant upgrade (continued)

System redundancy mode	Operator A actions	Operator B actions
SIMPLEX	Stage 29 — "Upgrade analytics servers" (p. 912)	Stage 30 — "Enable GUI client" (p. 912)
	Stage 31 — "Test upgraded system using GUI client" (p. 912)	
	Stage 32 — "Uninstall original primary database [DB1]" (p. 912) Stage 33 — "Install new standby main database [DB1]" (p. 913)	—
	Stage 34 — "Reinstantiate standby database" (p. 919) Stage 36 — "Upgrade original primary main server [Main1]" (p. 920)	Stage 35 — "Upgrade former primary auxiliary database cluster" (p. 919)
	Stage 37 — "Configure new standby main server [Main1]" (p. 921) Stage 38 — "Enable Windows Active Directory access" (p. 926) Stage 39 — "Enable CAC access" (p. 928)	Stage 40 — "Configure WS-NOC integration" (p. 931)
	Stage 41 — "Start new standby main server [Main1]" (p. 932)	Stage 42 — "Upgrade auxiliary servers [Aux1]" (p. 933) Stage 43 — "Start auxiliary servers [Aux1]" (p. 934) Stage 44 — "Disable maintenance mode for auxiliary database agents" (p. 934) Stage 45 — "Verify auxiliary database status" (p. 935)
DUPLEX	Stage 46 — "Check post-upgrade disk space" (p. 937) Stage 47 — "Install or upgrade single-user GUI clients" (p. 938)	Stage 48 — "Install or upgrade client delegate servers" (p. 938)
	Stage 49 — "Stop PKI server" (p. 938) Stage 50 — "Restore TLS version and cipher support configuration" (p. 938)	Stage 51 — "Configure and enable firewalls" (p. 938)

16.14 To upgrade a redundant Release 22.9 or later NFM-P system

16.14.1 Description

The following steps describe how to upgrade a collocated or distributed Release 22.9 or later 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:

- on each server station in the system — 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

16.14.2 Steps

Check pre-upgrade disk space

1

As part of the trial upgrade on a lab system in advance of a live upgrade, you must ensure that the available disk capacity on each NFM-P component remains within tolerance.

Note: If the disk usage on an NFM-P partition approaches or exceeds 80% after the trial upgrade, you may need to add disk capacity before you attempt the upgrade on a live system.

Perform the following steps on each of the following stations:

- main server
- auxiliary server
- main database
- auxiliary database

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following:

   ```
   # df -kh ↵
   ```

   The usage information for each partition is displayed.
4. Record the information for each NFM-P partition; see the tables in Chapter 2, “NSP disk setup and partitioning” for the partition names and required capacities.

Stop and disable standby main server [Main2]

2

Open a GUI client to monitor the network during the upgrade.

3

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.

6. Enter the following to switch to the root user:

   ```
   bash$ su ↵
   ```

7. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to display the nspOS service status:

   ```
   # nspdctl status ↵
   ```

   Information like the following is displayed.

   ```
   Mode:     DR
   Role:     redundancy_role
   DC-Role:  dc_role
   DC-Name:  dc_name
   Registry: IP_address:port
   State:    stopped
   Uptime:   0s
   SERVICE           STATUS
   service_a         inactive
   service_b         inactive
   service_c         inactive
   ```

   You must not proceed to the next step until all NSP services are stopped; if the State is not ‘stopped’, or the STATUS indicator of each listed service is not ‘inactive’, repeat this substep.

4

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:

   ```
   # systemctl disable nspos-nspd.service ↵
   ```

2. Enter the following:

   ```
   # systemctl disable nfmp-main-config.service ↵
   ```

3. Enter the following:

   ```
   # systemctl disable nfmp-main.service ↵
   ```

Stop auxiliary servers [Aux2]

5

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

6

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 ↵
   ```

4. Make a backup copy of the nms-server.xml file.
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:

   ```
   <db
   ```

7. Locate the following line in the section:

   ```
   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:

   ```
   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:

    ```
    redundancyEnabled="true"
    ```

    to read:

    ```
    redundancyEnabled="false"
    ```

12. Save and close the nms-server.xml file.
13. Enter the following:

    ```
    bash$ /opt/nsp/nfmp/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]

7

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.

8

Open a console window.

9

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 ↵
```

10

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.
6. Click Properties. The Aggregation Rule (multiple instances) [Edit] form opens.
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.

11

Perform the following steps.

1. Perform 3.4 “To apply a RHEL update to an NSP image-based OS” (p. 67)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 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 ↵
   ```

12

Log in as the root user on the main database [DB2] station.

Note: After the upgrade, the station is the new primary main database station.

13

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 collocated 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. You must remove the semvalidator package if it is installed; otherwise, the upgrade is blocked.

   Enter the following:

```
# rpm -q nsp-nfmp-semvalidator ↵
```

If the package is installed, the following is displayed:

```
nsp-nfmp-semvalidator-version
```

If the package is not installed, the following is displayed:

```
package nsp-nfmp-semvalidator is not installed
```

3. If the package is installed, enter the following:

```
# dnf remove nsp-nfmp-semvalidator ↵
```

The package is removed.

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
   - nsp-nfmp-nodeexporter-*R*.*r*.*p*-rel.*v*.rpm, if downloaded

   Note: In subsequent steps, the directory is called the NFM-P software directory.

14

Transfer the following downloaded file to an empty directory on the main database station:

- OracleSw_PreInstall.sh

15

Navigate to the directory that contains the OracleSw_PreInstall.sh file.

16

Enter the following:

```
# chmod +x OracleSw_PreInstall.sh ↵
```

17

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]:
```

18

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):
```

19

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/oracle19...
Checking user username... usermod: no changes
Changing ownership of the directory /opt/nsp/nfmp/oracle19 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 21.

20

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 17.

21

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]:
```

22

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
```

23

When the script execution is complete, enter the following to reboot the main database station:

```
# systemctl reboot ↵
```

The station reboots.

24

When the reboot is complete, log in to the main database [DB2] station as the root user.

25

Open a console window.

26

Navigate to the NFM-P software directory.

Note: Ensure that the directory contains only the installation files.

27

Enter the following:

```
# chmod +x * ↵
```

28

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf 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
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
```

```
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

30

Enter the following to upgrade the database:

Note: A database upgrade takes considerable time that varies, depending on the release from which you are upgrading.

```
# samupgradeDb ↵
```

The following prompt is displayed:

```
Enter the password for the "SAMUSER" database user (terminal echo is
off):
```

31

Enter the database user password.

The database upgrade begins, and messages like the following are displayed:

```
Validation succeeded.

Upgrade log is /opt/nsp/nfmp/db/install/NFM-P_Main_Database.upgrade.
timestamp.stdout.txt

Performing Step 1 of n - Initializing ..........

Performing NFM-P database upgrade will take time...

Executing PreOraUpgrade.sql ............

Executing ShutdownDBUpgrade.sql ....

Executing StartupDB.sql .....

Executing DbJavaReload.sql ................
```

The database upgrade is complete when the following is displayed:

```
DONE
```

32

Verify the database configuration and create the database.

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; see 14.9 “NFM-P samconfig utility” (p. 432) for information about using samconfig.
4. Configure one or more parameters, if required, and then enter **back** ↵.
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]

33

If the [Main2] main server and database are on separate stations, and the [Main2] main server is deployed in a VM created using an NSP RHEL OS disk image, perform 3.4 “To apply a RHEL update to an NSP image-based OS” (p. 67) on the standby [Main2] main server station.

34

Log in as the root user on the initial standby main server [Main2] station.

Note: After the upgrade, the station is the new primary main server station.

35

Open a console window.

36

Perform one of the following.

a. If the main server and database are collocated on one station, go to Step 43.

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
- nsp-nfmp-nodeexporter-*R.r.p*-rel.*v*.rpm, if downloaded

Note: In subsequent steps, the directory is called the NFM-P software directory.

37

You must remove the semvalidator package if it is installed; otherwise, the upgrade is blocked.

Perform the following steps.

1. Enter the following:

   ```
   # rpm -q nsp-nfmp-semvalidator ↵
   ```

   If the package is installed, the following is displayed:

   ```
   nsp-nfmp-semvalidator-version
   ```

   If the package is not installed, the following is displayed:

   ```
   package nsp-nfmp-semvalidator is not installed
   ```

2. If the package is installed, enter the following:

   ```
   # dnf remove nsp-nfmp-semvalidator ↵
   ```

   The package is removed.

38

Navigate to the NFM-P software directory.

39

Enter the following:

```
# chmod +x * ↵
```

40

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

41

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

Start PKI server

42

Start the PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 4.10 “To configure and enable a PKI server” (p. 113).

Note: The PKI server is required for internal system configuration purposes.

Configure new primary main server [Main2]

43

Enter the following; see 14.9 “NFM-P samconfig utility” (p. 432) 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>
```

44

Enter the following:

```
<main> configure ↵
```

The prompt changes to `<main configure>`.

45

To apply a new or updated NFM-P license, 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 the *NSP System Administrator Guide*.

```
<main configure> license license_file back ↵
```

where *license_file* is the path and file name of the NSP license bundle

46

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; see 14.9 “NFM-P samconfig utility” (p. 432) for information about using the samconfig utility.

3. Configure one or more parameters, if required.

   Note: The NFM-P uses the database backup settings to initialize the database during installation only. To change the backup settings after installation, you must use the Database Manager form in the NFM-P client GUI, as described in the *NSP System Administrator Guide*.

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

   ```
   <main configure> back ↵
   ```

   The prompt changes to `<main>`.

47

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

48

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

49

If the NFM-P is part of a shared-mode NSP system and you want to enable mTLS for internal Kafka authentication using two-way TLS, perform the following steps.

ℹ **Note:** Enabling mTLS for internal Kafka authentication is supported only in an NSP deployment that uses separate interfaces for internal and client communication.

ℹ **Note:** The parameter you must configure is displayed only if the ip-list parameter is set to a remote address.

ℹ **Note:** The parameter is configurable only if the **secure** and **internal-certs** parameters in the **nspos** section are set to true.

1. Enter the following:

   ```
   # samconfig -m main ↵
   ```

   The following is displayed:

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

2. Enter the following:

   ```
   # configure nspos mtls-kafka-enabled back ↵
   ```

3. Enter the following:

   ```
   <main> apply ↵
   ```

   The configuration is applied.

4. Enter the following:

   ```
   <main> exit ↵
   ```

   The samconfig utility closes.

Restore embedded nspOS, independent deployment

50

In an independent NFM-P deployment, you must restore the embedded Neo4j and PostgreSQL databases. Otherwise, if the NFM-P is integrated with an NSP cluster, go to Step 56.

51

Enter the following:

```
# mkdir /opt/nsp/os/backup ↵
```

52

Enter the following:

```
# chown nsp:nsp /opt/nsp/os/backup ↵
```

53

Copy the Neo4j and PostgreSQL backup files saved in Step 24 of 16.8 “To prepare for an NFM-P system upgrade from Release 22.9 or later” (p. 824) to the /opt/nsp/os/backup directory.

54

Restore the Neo4j database.

1. Enter the following:

   ```
   # cd /opt/nsp/os/install/tools/database ↵
   ```

2. Enter the following:

   ```
   # ./db-restore.sh --target IP_address ↵
   ```

   where *IP_address* is the main server IP address

   The following message and prompt are displayed:

   ```
   Verifying prerequisites...
   Starting database restore ...
   Backupset file to restore (.tar.gz format):
   ```

3. Enter the following and press ↵:

   ```
   path/nspos-neo4j_backup_timestamp.tar.gz
   ```

   where

   path is the absolute path of the Neo4j backup file

   timestamp is the backup creation time

   Note: Neo4j backup files are stored in the following locations on a main server, depending on the backup type:

- scheduled backup—/opt/nsp/os/backup/backupset_*n*
- manual backup—/opt/nsp/os/backup/manual_*timestamp*

The following messages and prompt are displayed:

```
PLAY [all] **************************************************

TASK [dbrestore : Create temporary directory] ***************

changed: [server_IP]

[dbrestore : pause]

Do you want to restore the nspOS Neo4j db from file:
path/nspos-neo4j_backup_timestamp.tar.gz? Press return to continue,
or Ctrl+C to abort:
```

4. Press ↵.

   The restore operation begins, and messages like the following are displayed:

```
TASK [dbrestore : Copy backupset] ***************************

changed: [server_IP]

TASK [dbrestore : Running nspdctl stop] *********************

changed: [server_IP]

TASK [dbrestore : Ensure database service is stopped] *******

changed: [server_IP]

TASK [dbrestore : Perform database restore] *****************

changed: [server_IP]

TASK [dbrestore : Delete temporary directory] ***************

changed: [server_IP]

PLAY RECAP **************************************************

server_IP      : ok=n   changed=n    unreachable=n   failed=n
```

5. If the `failed` value is greater than zero, a restore failure has occurred; contact technical support for assistance.

55

Restore the PostgreSQL database.

1. Enter the following:

```
# ./db-restore.sh --target IP_address ↵
```

   where *IP_address* is the main server IP address

   The following message and prompt are displayed:

```
Verifying prerequisites...

Starting database restore ...

Backupset file to restore (.tar.gz format):
```

2. Enter the following and press ↵:

```
path/nspos-postgresql_backup_timestamp.tar.gz
```

where

path is the absolute path of the PostgreSQL backup file

timestamp is the backup creation time

Note: PostgreSQL backup files are stored in the following locations on a main server, depending on the backup type:

- scheduled backup—/opt/nsp/os/backup/backupset_*n*
- manual backup—/opt/nsp/os/backup/manual_*timestamp*

The following messages and prompt are displayed:

```
PLAY [all] *************************************************
[dbrestore : pause]
Do you want to restore the nspOS PostgreSQL db from file:
path/nspos-postgresql_backup_timestamp.tar.gz? Press return to
continue, or Ctrl+C to abort:
```

3. Press ↵.

   The restore operation begins, and messages like the following are displayed:

```
TASK [dbrestore : Running nspdctl stop] *********************
changed: [server_IP]
TASK [dbrestore : Perform database restore] *****************
changed: [server_IP]
TASK [dbrestore : Delete temporary directory] ***************
changed: [server_IP]
PLAY RECAP *************************************************
server_IP     : ok=n   changed=n    unreachable=n   failed=n
```

4. If the `failed` value is greater than zero, a restore failure has occurred; contact technical support for assistance.

Enable Windows Active Directory access

56

If you intend to use Windows Active Directory, or AD, for single-sign-on client access, you must configure LDAP remote authentication for AD; otherwise,go to Step 75.

Open the following file as a reference for use in subsequent steps:

/opt/nsp/os/install/examples/config.yml

Note: Consider the following.

- The NFM-P does not assign a default user group to users of a remote authentication source that you define for Windows AD; the authentication source must provide the user group attributes.
- Windows AD supports the following LDAP server types for remote authentication:

  AD—The user group of an AD user is derived from the group_base_dn attribute in the server configuration; group search filters are not supported.

AUTHENTICATED—The server configuration must include bind credentials; group search filters are supported. After NFM-P initialization, you add the AD server bind credentials to the NSP password vault using the NSP Session Manager REST API.

57

Locate the section that begins with the following lines:

```
#   ldap:
#     enabled: true
#     servers:
#       - type: AUTHENTICATED/AD/ANONYMOUS
#         url: ldaps://ldap.example.com:636
#         security: SSL/STARTTLS/NONE
```

58

Open the following file using a plain-text editor such as vi:

/opt/nsp/os/install/config.json

59

Locate the section that begins with the following line:

```
"sso": {
```

The section has one subsection for each type of SSO access.

Note: You can enable multiple remote authentication methods such as LDAP and RADIUS in the config.json file, or by using the NFM-P GUI. Using the GUI also allows you to specify the order in which the methods are tried during login attempts; however, no ordering is applied to multiple methods enabled in the config.json file.

60

In the **sso** section, create an **ldap** subsection as shown below using the parameter names from the **ldap** section of config.yml and the required values for your configuration.

The following example shows the LDAP configuration for two AD servers:

```
"ldap": {
"enabled": true,
"servers": [
{
"type": "auth_type",
"url": "ldaps://server1:port",
"server1_parameter_1": "value",
"server1_parameter_2": "value",
.
.
"server1_parameter_n": "value",
},
{
"type": "auth_type",
"url": "ldaps://server2:port",
"server2_parameter_1": "value",
"server2_parameter_2": "value",
.
.
"server2_parameter_n": "value",
},
}]
}
```

where *auth_type* is AD or AUTHENTICATED

61

Save and close the files.

62

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

63

Enter the following:

```
<main> apply ↵
```

The AD LDAP configuration is applied.

64

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Enable CAC access

65

If you do not intend to enable Common Access Card, or CAC, technology for NFM-P client access, go to Step 75.

66

Download the federationmetadata.xml from the following ADFS link:

https://*ADFS_server_name*/FederationMetadata/2007-06/federationmetadata.xml

where *ADFS_server_name* is the ADFS server FQDN

67

Add an ADFS server entry to the /etc/hosts file on the main server.

1. Open the /etc/hosts file using a plain-text editor such as vi.
2. Add the following line below the line that contains the main server IP address:

   ```
   IP_address FQDN
   ```

   where

   IP_address is the IP address of the ADFS server

   FQDN is the FQDN of the ADFS server
3. Save and close the file.

68

In order to enable CAC for client access, you must configure Active Directory Federation Services, or ADFS.

Open the following file using a plain-text editor such as vi:

/opt/nsp/os/install/config.json

69

In the **sso** section, create an **saml2** subsection as shown below using the parameter names from the **saml2** section of config.yml and the required values for your configuration.

The following example shows the ADFS configuration.

Note: You must preserve the lead spacing of each line.

```
  "sso" : {
    "saml2": {
       "enabled": true,
       "service_provider_entity_id": "NFM-P_identifier",
       "service_provider_metadata_filename": "casmetadata.xml",
       "maximum_authentication_lifetime": 3600,
       "accepted_skew": 300,
       "destination_binding": "urn:oasis:names:tc:SAML:2.0:bindings:
HTTP-Redirect",
       "identity_provider_metadata_path": "ADFS_metadata_file",
       "authn_context_class_ref": "urn:oasis:names:tc:SAML:2.0:ac:
classes:TLSClient",
       "authn_context_comparison_type": "minimum",
       "name_id_policy_format": "urn:oasis:names:tc:SAML:1.1:
nameid-format:unspecified",
       "force_auth": true,
```

```
        "passive": false,
        "wants_assertions_signed": false,
        "wants_responses_signed": false,
        "all_signature_validation_disabled": false,
        "sign_service_provider_metadata": false,
        "principal_id_attribute": "UPN",
        "use_name_qualifier": false,
        "provider_name": "ADFS_server_URI",
        "requested_attributes": [{
          "name": "http://schemas.xmlsoap.
org/ws/2005/05/identity/claims/emailaddress",
           "friendly_name": "E-Mail Address",
           "name_format": "urn:oasis:names:tc:SAML:2.0:attrname-format:
uri",
           "required": false
       } ],
        "mapped_attributes": [{
            "name": "http://schemas.xmlsoap.org/claims/Group",
            "mapped_to": "authorizationProfile"
       }, {
            "name": "http://schemas.xmlsoap.
org/ws/2005/05/identity/claims/upn",
            "mapped_to": "upn"
       } ]
     },
```

70

Configure the following parameters; leave all other parameters at the default:

- "service_provider_entity_id": "*NFM-P_identifier*"
- "identity_provider_metadata_path": "*ADFS_metadata_file*"
- "provider_name": "*ADFS_server_name*"

NFM-P_identifier is the unique ADFS Relying Trust Party identifier

*ADFS_metadata_fil*e is the absolute path of the ADFS metadata XML file, for example, /opt/federationmetadata.xml

ADFS_server_name is the ADFS server FQDN

71

Save and close the files.

72

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

73

Enter the following:

```
<main> apply ↵
```

The ADFS configuration is applied.

74

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Configure WS-NOC integration

75

If the NFM-P is integrated with a WS-NOC system, open the following file with a plain-text editor such as vi:

/opt/nsp/os/install/examples/config.json

Otherwise, go to Step 85.

76

Copy the following section:

```
  "nfmt": {
    "primary_ip": "",
    "standby_ip": "",
    "username": "",
    "password": "",
    "cert_provided": false
  },
```

77

Close the file.

78

Open the following file with a plain-text editor such as vi:

/opt/nsp/os/install/config.json

79

Paste in the copied section.

80

Configure the required parameters to enable the WS-NOC integration:

- primary_ip—the primary WS-NOC server IP address
- standby_ip—the standby WS-NOC server IP address
- username—the username required for WS-NOC access
- password—the password required for WS-NOC access
- cert_provided—whether a TLS certificate is used

81

Save and close the file.

82

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

83

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

84

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Stop NSP analytics servers, NSP Flow Collectors

85

If the system includes one or more NSP 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/analytics/bin/AnalyticsAdmin.sh stop ↵
```

The following is displayed:

```
Stopping Analytics Application
```

When the analytics server is completely stopped, the following message is displayed:

```
Analytics Application is not running
```

86

If the system includes one or more NSP Flow Collector Controllers and Flow Collectors, stop each NSP Flow Collector Controller.

Note: If the NSP Flow Collector Controller is collocated on a station with an NSP Flow Collector, stopping the NSP Flow Collector Controller also stops the Flow Collector.

1. Log in to the NSP Flow Collector Controller station as the nsp user.
2. Open a console window.
3. Enter the following:

   ```
   bash$ /opt/nsp/flow/fcc/bin/flowCollectorController.bash stop ↵
   ```

   The NSP Flow Collector Controller stops.

87

If the system includes one or more NSP Flow Collectors that are not collocated on a station with a Flow Collector Controller, stop each such NSP Flow Collector.

1. Log in to the NSP Flow Collector station as the nsp user.
2. Open a console window.
3. Enter the following:

   ```
   bash$ /opt/nsp/flow/fc/bin/flowCollector.bash stop ↵
   ```

   The NSP Flow Collector stops.

Upgrade auxiliary servers [Aux2]

88

If the system includes auxiliary servers, perform 16.15 “To upgrade a Release 22.9 or later NFM-P auxiliary server” (p. 940) on each appropriate auxiliary server station [Aux2].

Verify auxiliary database synchronization

89

If the system does not include redundant auxiliary database clusters, go to Step 94.

90

If you are upgrading the first redundant auxiliary database cluster, you must verify the success of the most recent copy-cluster operation, which synchronizes the database data between the redundant clusters.

Note: You must not proceed to the next step until the copy-cluster operation is complete and successful.

Perform one of the following periodically to check the copy-cluster status.

a. If the NFM-P is in a shared-mode NSP deployment, issue the following REST API call:

Note: In order to issue a REST API call, you require a REST token; see this tutorial on the Network Developer Portal for information.

```
GET https://address:8545/restconf/data/auxdb:/auxdb-agent
```

where *address* is the advertised address of the primary NSP cluster

The call returns a status of SUCCESS, as shown below, for a successfully completed copy-cluster operation:

```
<HashMap>
      <auxdb-agent>
         <name>nspos-auxdb-agent</name>
         <application-mode>ACTIVE</application-mode>
         <copy-cluster>
            <source-cluster>cluster_M</source-cluster>
            <target-cluster>cluster_N</target-cluster>
            <time-started>timestamp</time-started>
            <status>SUCCESS</status>
         </copy-cluster>
      </auxdb-agent>
</HashMap>
```

b. If the NFM-P is not in a shared-mode NSP deployment, enter the following as the root user on the primary main server station [Main1]:

```
# /opt/nsp/os/nspd/nspdctl auxdb agent-status ↵
```

The command returns output like the following for a successfully completed copy-cluster operation:

```
     DC-ROLE HOST APPLICATION-MODE
     active leader 203.0.113.101 ACTIVE
     Copy Cluster Details
     SOURCE TARGET TIME-STARTED STATUS
     cluster_1 cluster_2 2022-03-14T15:09:26.535Z SUCCESS
```

Enable maintenance mode on auxiliary database agent

91

Perform one of the following to enable nspos-auxdb-agent maintenance mode.

a. If the NFM-P is in a shared-mode NSP deployment, perform the following steps.

1. Log in as the root user on the NSP cluster host in the primary data center.
2. Enter the following to set the nspos-auxdb-agent mode to maintenance:

   ```
   # kubectl patch configmap/nspos-auxdb-agent-overrides --type=merge
   -p '{"data":{"nspos-auxdb-agent-overrides.json":"{\"auxDbAgent\":
   {\"config\":{\"maintenance-mode\":true}}}"}}' ↵
   ```

3. Enter the following to restart the nspos-auxdb-agent pod:

   ```
   # kubectl delete pod `kubectl describe pods | grep -P ^^Name: |
   grep -oP nspos-auxdb-agent[-a-zA-Z0-9]+` ↵
   ```

4. Issue the following REST API call against the primary NSP cluster to verify that the agent is in maintenance mode:

   NOTE: In order to issue a REST API call, you require a REST token; see this tutorial on the Network Developer Portal for information.

   ```
   GET https://address:8545/restconf/data/auxdb:/auxdb-agent
   ```

   where *address* is the advertised address of the primary NSP cluster

   The call returns information like the following:

   ```
   {
       "auxdb-agent": {
           "name": "nspos-auxdb-agent",
           "application-mode": "MAINTENANCE",
           "copy-cluster": {
               "source-cluster": "cluster_2",
               "target-cluster": "cluster_1",
               "time-started": "timestamp",
               "status": "SUCCESS"
           }
       }
   }
   ```

   The agent is in maintenance mode if the application-mode is MAINTENANCE, as shown in the example.

5. Log in as the root user on the NSP cluster host in the standby data center.
6. Enter the following to set the nspos-auxdb-agent mode to maintenance:

   ```
   # kubectl patch configmap/nspos-auxdb-agent-overrides --type=merge
   -p '{"data":{"nspos-auxdb-agent-overrides.json":"{\"auxDbAgent\":
   {\"config\":{\"maintenance-mode\":true}}}"}}' ↵
   ```

b. If the NFM-P is not in a shared-mode NSP deployment, perform the following steps.

1. Log in as the root user on the NSP cluster host in the primary data center.
2. Enter the following to set the nspos-auxdb-agent mode to maintenance:

   ```
   # sed -i -r 's/("maintenance-mode"\s*:\s*)false/\1true/g'
   /opt/nsp/os/auxdb-agent/conf/nspos-auxdb-agent-overrides.json ↵
   ```
3. Enter the following to verify that the nspos-auxdb-agent is in maintenance mode:

   ```
   # /opt/nsp/os/nspd/nspdctl auxdb agent-status ↵
   DC-ROLE          HOST             APPLICATION-MODE
   active leader    203.0.113.101    MAINTENANCE
   standby leader   203.0.113.102    inactive
   ```

   The agent is in maintenance mode if the APPLICATION-MODE of the active leader is MAINTENANCE, as shown in the example.
4. Log in as the root user on the NSP cluster host in the standby data center.
5. Enter the following to set the nspos-auxdb-agent mode to maintenance:

   ```
   # sed -i -r 's/("maintenance-mode"\s*:\s*)false/\1true/g'
   /opt/nsp/os/auxdb-agent/conf/nspos-auxdb-agent-overrides.json ↵
   ```

Upgrade standby auxiliary database cluster

92

If you are upgrading the first redundant auxiliary database cluster, perform the following steps to stop the database proxy on each station in each auxiliary database cluster.

1. Enter the following sequence of commands as the root user on each auxiliary database station in the standby data center:

   ```
   # systemctl stop nfmp-auxdbproxy.service ↵
   # systemctl disable nfmp-auxdbproxy.service ↵
   ```

   The proxy stops, and is disabled.
2. Enter the following sequence of commands as the root user on each auxiliary database station in the primary data center:

   ```
   # systemctl stop nfmp-auxdbproxy.service ↵
   # systemctl disable nfmp-auxdbproxy.service ↵
   ```

   The proxy stops, and is disabled.

93

Perform 16.16 “To upgrade a Release 22.9 or later NFM-P auxiliary database cluster” (p. 944) to upgrade the standby auxiliary database cluster.

Stop and disable original primary main server [Main1]

94

Stop the original primary main server.

ℹ **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$ 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. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to display the nspOS service status:

   ```
   # nspdctl status ↵
   ```

   Information like the following is displayed.

   ```
   Mode:      DR
   Role:      redundancy_role
   DC-Role:   dc_role
   DC-Name:   dc_name
   Registry:  IP_address:port
   State:     stopped
   Uptime:    0s
   SERVICE            STATUS
   service_a          inactive
   service_b          inactive
   service_c          inactive
   ```

   You must not proceed to the next step until all NSP services are stopped; if the State is not ‘stopped’, or the STATUS indicator of each listed service is not ‘inactive’, repeat this substep.

95

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:

   ```
   # systemctl disable nspos-nspd.service ↵
   ```

2. Enter the following:

   ```
   # systemctl disable nfmp-main-config.service ↵
   ```

3. Enter the following:

   ```
   # systemctl disable nfmp-main.service ↵
   ```

Upgrade NSP Flow Collector Controllers, Flow Collectors

96

If the system includes one or more NSP Flow Collectors, upgrade each NSP Flow Collector Controller and Flow Collector as described in "NSP Flow Collector and Flow Collector Controller upgrade from Release 22.9 or later" (p. 799).

Stop auxiliary servers [Aux1]

97

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 auxstop ↵
   ```

   The auxiliary server stops.

Stop original primary main database [DB1]

98

Log in to the original primary main database [DB1] station as the root user.

99

Open a console window.

100

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 ↵
```

101

Perform the following steps.

1. Perform 3.4 “To apply a RHEL update to an NSP image-based OS” (p. 67)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 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 ↵
```

Upgrade auxiliary database, if not redundant

102

If the system does not include an auxiliary database, go to Step 106.

103

If the system includes a standalone auxiliary database, perform the following steps.

1. Perform 16.16 “To upgrade a Release 22.9 or later NFM-P auxiliary database cluster” (p. 944).
2. Go to Step 106.

Enable maintenance mode for auxiliary database agent

104

If the system includes redundant auxiliary database clusters, and the NFM-P is not in a shared-mode NSP deployment, enter the following as the root user on the newly upgraded main server [Main2]:

```
# sed -i -r 's/("maintenance-mode"\s*:\s*)false/\1true/g'
/opt/nsp/os/auxdb-agent/conf/nspos-auxdb-agent-overrides.json ↵
```

The auxiliary database cluster enters maintenance mode within approximately one minute.

Stop former primary auxiliary database cluster

105

If the system includes redundant auxiliary database clusters, perform the following steps on one station in the upgraded former primary cluster.

1. Log in as the root user.
2. Open a console window.
3. Enter the following:

   ```
   # cd /opt/nsp/nfmp/auxdb/install/bin ↵
   ```
4. Enter the following to stop the auxiliary database:

   ```
   # ./auxdbAdmin.sh stop ↵
   ```
5. Enter the following to display the auxiliary database status:

   ```
   # ./auxdbAdmin.sh status ↵
   ```

   Information like the following is displayed:

   ```
   Database status
   Node       | Host           | State | Version | DB
   ------------+---------------+-------+---------+-------
   node_1 | internal_IP_1 | STATE | version | db_name
   node_2 | internal_IP_2 | STATE | version | db_name
   .
   .
   .
   node_n | internal_IP_n | STATE | version | db_name
         Output captured in log_file
   ```

   The cluster is stopped when each *STATE* entry reads DOWN.
6. Repeat substep 5 periodically until the cluster is stopped.

   Note: You must not proceed to the next step until the cluster is stopped.

Start new primary main server [Main2]

106

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 the *NSP 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.

107

If you have enabled CAC for NFM-P client access, download the casmetadata.xml file from the following URL, and then import the file into the ADFS server relying-trust-party:

https://*server*/cas/sp/metadata

where *server* is the main server IP address or hostname

After the download, the casmetadata.xml file is available in the following directory on the main server:

/opt/nsp/os/tomcat/conf/cas/saml

108

If you have enabled Windows Active Directory access using the AUTHENTICATED type of LDAP server, perform the following steps.

1. Use the NSP Session Manager REST API to add the LDAP server bind credentials; see the Network Developer Portal for information.

2. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to restart the local nspos-tomcat service:

   Note: The service restart may take a few minutes, during which NFM-P GUI and REST client access is degraded. General NFM-P operation is unaffected.

   ```
   # systemctl restart nspos-tomcat ↵
   ```

109

Specify the memory requirement for GUI clients based on the type of network that the NFM-P is to manage.

1. Enter the following:

   ```
   bash$ ./nmsdeploytool.bash clientmem -option ↵
   ```

   where *option* is one of the following:
   - m—medium, for management of limited-scale network
   - l—large, for a network of 15 000 or more NEs
2. Record the setting, which is not preserved through an upgrade, for future use.
3. Enter the following to commit the configuration change:

   ```
   bash$ ./nmsdeploytool.bash deploy ↵
   ```

Start auxiliary servers [Aux2]

110

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.

Activate upgraded former standby auxiliary database cluster

111

If the system does not include redundant auxiliary database clusters, go to Step 114.

112

Perform the following steps on each station in the upgraded former standby auxiliary database cluster.

1. Log in as the root user on the station.
2. Open a console window.

3. Enter the following sequence of commands to enable the database services:

   ```
   # systemctl enable nspos-auxdb.service ↵
   # systemctl enable nspos-auxdbproxy.service ↵
   # systemctl enable vertica_agent.service ↵
   # systemctl enable verticad.service ↵
   ```

   The services are enabled.

4. Enter the following to start the database proxy:

   ```
   # systemctl start nspos-auxdbproxy.service ↵
   ```

   The proxy starts.

113

Perform one of the following to activate the former standby auxiliary database cluster, after which the cluster assumes the primary role.

a. If the NFM-P is in a shared-mode NSP deployment, issue the following REST API call:

   Note: In order to issue a REST API call, you require a REST token; see this tutorial on the Network Developer Portal for information.

   ```
   POST https://{{address}}:8545/restconf/data/auxdb:/clusters/cluster=cluster_N/activate
   ```

   where

   address is the advertised address of the primary NSP cluster

   N is the auxiliary database cluster number

   The following is the request body:

   ```
   {
     "auxdb:input" : {
       "force": true
     }
   }
   ```

   The cluster is activated.

b. If the NFM-P is not in a shared-mode NSP deployment, enter the following as the root user on the new primary main server station:

   ```
   # nspdctl auxdb activate cluster_N --force ↵
   ```

   where *N* is the auxiliary database

   A message like the following is displayed:

   ```
   Auxiliary database activation request submitted for [cluster_N]
   ```

Upgrade analytics servers

114

If the system includes one or more NSP analytics servers, upgrade each analytics server as described in "NSP analytics server upgrade from Release 22.9 or later" (p. 807).

Enable GUI client

115

You require an NFM-P GUI client to complete the procedure; see the following for information:

Note: A client delegate server installation typically takes more time than the other options. A single-user client or client delegate server upgrade is recommended if your maintenance period is limited.

- "NFM-P single-user GUI client installation" (p. 585)
- "NFM-P single-user GUI client upgrade from Release 22.9 or later" (p. 955)
- "NFM-P client delegate server installation" (p. 591)
- "NFM-P client delegate server upgrade from Release 22.9 or later" (p. 963)

Test upgraded system using GUI client

116

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].

Uninstall original primary database [DB1]

117

Enter the following to uninstall the original primary main database:

```
# dnf remove nsp-nfmp-main-db nsp-nfmp-oracle ↵
```

The dnf utility resolves any dependencies and displays the following prompt:

```
Installed size: nn G
Is this ok [y/N]:
```

118

Enter y. The following is displayed as the packages are removed:

```
Downloading Packages:
```

```
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
Uninstalling the NFM-P package...
```

As each package removal completes, the following is displayed:

```
Complete!
```

Install new standby main database [DB1]

119

Log in as the root user on the initial primary main database [DB1] station.

Note: After the upgrade, the station is the new standby main database station.

120

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 collocated 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. You must remove the semvalidator package if it is installed; otherwise, the upgrade is blocked.

   Enter the following:

   ```
   # rpm -q nsp-nfmp-semvalidator ↵
   ```

   If the package is installed, the following is displayed:

   ```
   nsp-nfmp-semvalidator-version
   ```

   If the package is not installed, the following is displayed:

   ```
   package nsp-nfmp-semvalidator is not installed
   ```
3. If the package is installed, enter the following:

   ```
   # dnf remove nsp-nfmp-semvalidator ↵
   ```

   The package is removed.

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
- nsp-nfmp-nodeexporter-*R*.*r*.*p*-rel.*v*.rpm, if downloaded

Note: In subsequent steps, the directory is called the NFM-P software directory.

121

Transfer the following downloaded file to an empty directory on the main database station:

- OracleSw_PreInstall.sh

122

Open a console window.

123

Navigate to the directory that contains the OracleSw_PreInstall.sh file.

124

Enter the following:

```
# chmod +x OracleSw_PreInstall.sh ↵
```

125

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 R.r Rn database.

Do you want to continue? [Yes/No]:
```

126

Enter Yes. The following prompt is displayed:

```
Enter the Oracle dba group name [group]:
```

127

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]:
```

128

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]:
```

129

Enter Yes.

The following messages and prompt are displayed:

```
Checking or Creating the Oracle user home directory
/opt/nsp/nfmp/oracle19...

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/oracle19 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]:
```

130

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]:
```

131

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
```

132

When the script execution is complete, enter the following to reboot the station:

```
# systemctl reboot ↵
```

The station reboots.

133

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.

134

Open a console window.

135

Navigate to the NFM-P software directory.

Note: Ensure that the directory contains only the installation files.

136

Enter the following:

```
# chmod +x * ↵
```

137

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

138

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

139

Configure the database as a standby database; see 14.9 “NFM-P samconfig utility” (p. 432) for information about using samconfig.

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>`.

140

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; see 14.9 “NFM-P samconfig utility” (p. 432) for information about using the samconfig utility.

3. Configure one or more parameters, if required.

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

   ```
   <db configure> back ↵
   ```

   The prompt changes to `<db>`.

141

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.
```

142

When the database creation is complete, enter the following:

```
<db> exit ↵
```

The samconfig utility closes.

Reinstantiate standby database

143

Log in to an NFM-P GUI client as the admin user.

144

Choose Administration→System Information from the main menu. The System Information form opens.

145

Click Re-Instantiate Standby.

146

Click Yes to confirm the action. The reinstantiation begins, and the GUI status bar displays reinstantiation information.

Note: Database reinstantiation 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.

147

When the reinstantiation is complete, close the System Information form.

Upgrade former primary auxiliary database cluster

148

If the system includes redundant auxiliary database clusters, perform 16.16 “To upgrade a Release 22.9 or later NFM-P auxiliary database cluster” (p. 944) on the former primary auxiliary database cluster.

Upgrade original primary main server [Main1]

149

If the [Main1] main server and database are on separate stations, and the [Main1] main server is deployed in a VM created using an NSP RHEL OS disk image, perform 3.4 “To apply a RHEL update to an NSP image-based OS” (p. 67) on the original primary [Main1] main server station.

150

Log in as the root user on the main server [Main1] station.

Note: After the upgrade, the station is the new standby main server station.

151

Open a console window.

152

Perform one of the following.

a. If the main server and database are collocated on one station, go to Step 158.

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
   - nsp-nfmp-nodeexporter-*R.r.p*-rel.*v*.rpm, if downloaded

   Note: In subsequent steps, the directory is called the NFM-P software directory.

153

You must remove the semvalidator package if it is installed; otherwise, the upgrade is blocked.

Perform the following steps.

1. Enter the following:

   ```
   # rpm -q nsp-nfmp-semvalidator ↵
   ```

   If the package is installed, the following is displayed:

   ```
   nsp-nfmp-semvalidator-version
   ```

   If the package is not installed, the following is displayed:

   ```
   package nsp-nfmp-semvalidator is not installed
   ```

2. If the package is installed, enter the following:

   ```
   # dnf remove nsp-nfmp-semvalidator ↵
   ```

   The package is removed.

154

Navigate to the NFM-P software directory.

155

Enter the following:

```
# chmod +x * ↵
```

156

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

157

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

Configure new standby main server [Main1]

158

Enter the following; see 14.9 “NFM-P samconfig utility” (p. 432) 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>
```

159

Enter the following:

```
<main> configure ↵
```

The prompt changes to `<main configure>`.

160

To apply a new or updated NFM-P license, 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 the *NSP System Administrator Guide*.

```
<main configure> license license_file back ↵
```

where *license_file* is the path and file name of the NSP license bundle

161

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; see 14.9 “NFM-P samconfig utility” (p. 432) for information about using the samconfig utility.
3. Configure one or more parameters, if required.

   Note: The NFM-P uses the database backup settings to initialize the database during installation only. To change the backup settings after installation, you must use the Database Manager form in the NFM-P client GUI, as described in the *NSP System Administrator Guide*.
4. When you are certain that the configuration is correct, enter the following:

   ```
   <main configure> back ↵
   ```

   The prompt changes to `<main>`.

162

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

163

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Note: This station is the new standby main server station.

164

If the NFM-P is part of a shared-mode NSP system and you want to enable mTLS for internal Kafka authentication using two-way TLS, perform the following steps.

Note: Enabling mTLS for internal Kafka authentication is supported only in an NSP deployment that uses separate interfaces for internal and client communication.

Note: The parameter you must configure is displayed only if the ip-list parameter is set to a remote address.

Note: The parameter is configurable only if the **secure** and **internal-certs** parameters in the **nspos** section are set to true.

1. Enter the following:

   ```
   # samconfig -m main ↵
   ```

   The following is displayed:

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

2. Enter the following:

   ```
   # configure nspos mtls-kafka-enabled back ↵
   ```

3. Enter the following:

   ```
   <main> apply ↵
   ```

   The configuration is applied.

4. Enter the following:

   ```
   <main> exit ↵
   ```

   The samconfig utility closes.

Restore embedded nspOS, independent deployment

165

In an independent NFM-P deployment, you must restore the embedded Neo4j and PostgreSQL databases. Otherwise, if the NFM-P is integrated with an NSP cluster, go to Step 171.

166

Enter the following:

```
# mkdir /opt/nsp/os/backup ↵
```

167

Enter the following:

```
# chown nsp:nsp /opt/nsp/os/backup ↵
```

168

Copy the Neo4j and PostgreSQL backup files saved in Step 24 of 16.8 “To prepare for an NFM-P system upgrade from Release 22.9 or later” (p. 824) to the /opt/nsp/os/backup directory.

169

Restore the Neo4j database.

1. Enter the following:

   ```
   # cd /opt/nsp/os/install/tools/database ↵
   ```

2. Enter the following:

   ```
   # ./db-restore.sh --target IP_address ↵
   ```

   where *IP_address* is the main server IP address

   The following message and prompt are displayed:

   ```
   Verifying prerequisites...
   Starting database restore ...
   Backupset file to restore (.tar.gz format):
   ```

3. Enter the following and press ↵:

   ```
   path/nspos-neo4j_backup_timestamp.tar.gz
   ```

   where

   path is the absolute path of the Neo4j backup file

   timestamp is the backup creation time

   Note: Neo4j backup files are stored in the following locations on a main server, depending on the backup type:

   - scheduled backup—/opt/nsp/os/backup/backupset_*n*
   - manual backup—/opt/nsp/os/backup/manual_*timestamp*

   The following messages and prompt are displayed:

   ```
   PLAY [all] *************************************************
   TASK [dbrestore : Create temporary directory] ***************
   changed: [server_IP]
   [dbrestore : pause]
   Do you want to restore the nspOS Neo4j db from file:
   path/nspos-neo4j_backup_timestamp.tar.gz? Press return to continue,
   or Ctrl+C to abort:
   ```

4. Press ↵.

   The restore operation begins, and messages like the following are displayed:

   ```
   TASK [dbrestore : Copy backupset] ***************************
   changed: [server_IP]
   TASK [dbrestore : Running nspdctl stop] *********************
   changed: [server_IP]
   TASK [dbrestore : Ensure database service is stopped] *******
   ```

```
changed: [server_IP]
TASK [dbrestore : Perform database restore] ****************
changed: [server_IP]
TASK [dbrestore : Delete temporary directory] **************
changed: [server_IP]
PLAY RECAP ************************************************
server_IP      : ok=n   changed=n    unreachable=n   failed=n
```

5. If the `failed` value is greater than zero, a restore failure has occurred; contact technical support for assistance.

170

Restore the PostgreSQL database.

1. Enter the following:

   `# ./db-restore.sh --target IP_address ↵`

   where *IP_address* is the main server IP address

   The following message and prompt are displayed:

   ```
   Verifying prerequisites...
   Starting database restore ...
   Backupset file to restore (.tar.gz format):
   ```

2. Enter the following and press ↵:

   `path/nspos-postgresql_backup_timestamp.tar.gz`

   where

   path is the absolute path of the PostgreSQL backup file

   timestamp is the backup creation time

   Note: PostgreSQL backup files are stored in the following locations on a main server, depending on the backup type:

   - scheduled backup—/opt/nsp/os/backup/backupset_*n*
   - manual backup—/opt/nsp/os/backup/manual_*timestamp*

   The following messages and prompt are displayed:

   ```
   PLAY [all] ************************************************
   [dbrestore : pause]
   Do you want to restore the nspOS PostgreSQL db from file:
   path/nspos-postgresql_backup_timestamp.tar.gz? Press return to
   continue, or Ctrl+C to abort:
   ```

3. Press ↵.

   The restore operation begins, and messages like the following are displayed:

   ```
   TASK [dbrestore : Running nspdctl stop] ********************
   changed: [server_IP]
   TASK [dbrestore : Perform database restore] ****************
   ```

```
changed: [server_IP]
TASK [dbrestore : Delete temporary directory] ***************
changed: [server_IP]
PLAY RECAP ************************************************
server_IP     : ok=n   changed=n    unreachable=n   failed=n
```

4. If the `failed` value is greater than zero, a restore failure has occurred; contact technical support for assistance.

Enable Windows Active Directory access

171

If you intend to use Windows Active Directory, or AD, for single-sign-on client access, you must configure LDAP remote authentication for AD; otherwise, go to Step 190.

Open the following file as a reference for use in subsequent steps:

/opt/nsp/os/install/examples/config.yml

Note: Consider the following.

- The NFM-P does not assign a default user group to users of a remote authentication source that you define for Windows AD; the authentication source must provide the user group attributes.
- Windows AD supports the following LDAP server types for remote authentication:

  AD—The user group of an AD user is derived from the group_base_dn attribute in the server configuration; group search filters are not supported.

  AUTHENTICATED—The server configuration must include bind credentials; group search filters are supported. After NFM-P initialization, you add the AD server bind credentials to the NSP password vault using the NSP Session Manager REST API.

172

Locate the section that begins with the following lines:

```
#   ldap:
#     enabled: true
#     servers:
#       - type: AUTHENTICATED/AD/ANONYMOUS
#         url: ldaps://ldap.example.com:636
#         security: SSL/STARTTLS/NONE
```

173

Open the following file using a plain-text editor such as vi:

/opt/nsp/os/install/config.json

174

Locate the section that begins with the following line:

```
"sso": {
```

The section has one subsection for each type of SSO access.

Note: You can enable multiple remote authentication methods such as LDAP and RADIUS in the config.json file, or by using the NFM-P GUI. Using the GUI also allows you to specify the order in which the methods are tried during login attempts; however, no ordering is applied to multiple methods enabled in the config.json file.

175

In the **sso** section, create an **ldap** subsection as shown below using the parameter names from the **ldap** section of config.yml and the required values for your configuration.

The following example shows the LDAP configuration for two AD servers:

```
"ldap": {
"enabled": true,
"servers": [
{
"type": "auth_type",
"url": "ldaps://server1:port",
"server1_parameter_1": "value",
"server1_parameter_2": "value",
.
.
"server1_parameter_n": "value",
},
{
"type": "auth_type",
"url": "ldaps://server2:port",
"server2_parameter_1": "value",
"server2_parameter_2": "value",
.
.
"server2_parameter_n": "value",
},
}]
}
```

where *auth_type* is AD or AUTHENTICATED

176

Save and close the files.

177

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

178

Enter the following:

```
<main> apply ↵
```

The AD LDAP configuration is applied.

179

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Enable CAC access

180

If you do not intend to enable Common Access Card, or CAC, technology for NFM-P client access, go to Step 190.

181

Download the federationmetadata.xml from the following ADFS link:

https://*ADFS_server_name*/FederationMetadata/2007-06/federationmetadata.xml

where *ADFS_server_name* is the ADFS server FQDN

182

Add an ADFS server entry to the /etc/hosts file on the main server.

1. Open the /etc/hosts file using a plain-text editor such as vi.
2. Add the following line below the line that contains the main server IP address:

   ```
   IP_address FQDN
   ```

   where

   IP_address is the IP address of the ADFS server

   FQDN is the FQDN of the ADFS server
3. Save and close the file.

183

In order to enable CAC for client access, you must configure Active Directory Federation Services, or ADFS.

Open the following file using a plain-text editor such as vi:

/opt/nsp/os/install/config.json

184

In the **sso** section, create an **saml2** subsection as shown below using the parameter names from the **saml2** section of config.yml and the required values for your configuration.

The following example shows the ADFS configuration.

Note: You must preserve the lead spacing of each line.

```
  "sso" : {
    "saml2": {
       "enabled": true,
       "service_provider_entity_id": "NFM-P_identifier",
       "service_provider_metadata_filename": "casmetadata.xml",
       "maximum_authentication_lifetime": 3600,
       "accepted_skew": 300,
       "destination_binding": "urn:oasis:names:tc:SAML:2.0:bindings:
HTTP-Redirect",
       "identity_provider_metadata_path": "ADFS_metadata_file",
       "authn_context_class_ref": "urn:oasis:names:tc:SAML:2.0:ac:
classes:TLSClient",
       "authn_context_comparison_type": "minimum",
       "name_id_policy_format": "urn:oasis:names:tc:SAML:1.1:
nameid-format:unspecified",
       "force_auth": true,
       "passive": false,
       "wants_assertions_signed": false,
       "wants_responses_signed": false,
       "all_signature_validation_disabled": false,
       "sign_service_provider_metadata": false,
       "principal_id_attribute": "UPN",
       "use_name_qualifier": false,
       "provider_name": "ADFS_server_URI",
       "requested_attributes": [{
         "name": "http://schemas.xmlsoap.
org/ws/2005/05/identity/claims/emailaddress",
          "friendly_name": "E-Mail Address",
          "name_format": "urn:oasis:names:tc:SAML:2.0:attrname-format:
uri",
          "required": false
```

```
        } ],
         "mapped_attributes": [{
             "name": "http://schemas.xmlsoap.org/claims/Group",
             "mapped_to": "authorizationProfile"
        }, {
             "name": "http://schemas.xmlsoap.
org/ws/2005/05/identity/claims/upn",
             "mapped_to": "upn"
        } ]
      },
```

185

Configure the following parameters; leave all other parameters at the default:

- "service_provider_entity_id": "*NFM-P_identifier*"
- "identity_provider_metadata_path": "*ADFS_metadata_file*"
- "provider_name": "*ADFS_server_name*"

NFM-P_identifier is the unique ADFS Relying Trust Party identifier

*ADFS_metadata_fil*e is the absolute path of the ADFS metadata XML file, for example, /opt/federationmetadata.xml

ADFS_server_name is the ADFS server FQDN

186

Save and close the files.

187

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

188

Enter the following:

```
<main> apply ↵
```

The ADFS configuration is applied.

189

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Configure WS-NOC integration

190

If the NFM-P is integrated with an WS-NOC system, open the following file with a plain-text editor such as vi; otherwise, go to Step 200:

/opt/nsp/os/install/examples/config.json

191

Copy the following section:

```
"nfmt": {
  "primary_ip": "",
  "standby_ip": "",
  "username": "",
  "password": "",
  "cert_provided": false
},
```

192

Close the file.

193

Open the following file with a plain-text editor such as vi:

/opt/nsp/os/install/config.json

194

Paste in the copied section.

195

Configure the required parameters to enable the WS-NOC integration:

- primary_ip—the primary WS-NOC server IP address
- standby_ip—the standby WS-NOC server IP address
- username—the username required for WS-NOC access
- password—the password required for WS-NOC access
- cert_provided—whether a TLS certificate is used

196

Save and close the file.

197

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

198

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

199

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Start new standby main server [Main1]

200

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 the *NSP 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.

201

If you have enabled CAC for NFM-P client access, download the casmetadata.xml file from the following URL, and then import the file into the ADFS server relying-trust-party:

https://*server*/cas/sp/metadata

where *server* is the main server IP address or hostname

After the download, the casmetadata.xml file is available in the following directory on the main server:

/opt/nsp/os/tomcat/conf/cas/saml

202

If you have enabled Windows Active Directory access using the AUTHENTICATED type of LDAP server, perform the following steps.

1. Use the NSP Session Manager REST API to add the LDAP server bind credentials; see the Network Developer Portal for information.
2. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to restart the local nspos-tomcat service:

   Note: The service restart may take a few minutes, during which NFM-P GUI and REST client access is degraded. General NFM-P operation is unaffected.

   ```
   # systemctl restart nspos-tomcat ↵
   ```

203

Specify the memory requirement for GUI clients based on the type of network that the NFM-P is to manage.

1. Enter the following:

   ```
   bash$ ./nmsdeploytool.bash clientmem -option ↵
   ```

   where *option* is one of the following:
   - m—medium, for management of limited-scale network
   - l—large, for a network of 15 000 or more NEs
2. Record the setting, which is not preserved through an upgrade, for future use.
3. Enter the following to commit the configuration change:

   ```
   bash$ ./nmsdeploytool.bash deploy ↵
   ```

204

Close the console window.

Upgrade auxiliary servers [Aux1]

205

If the system includes auxiliary servers, perform 16.15 “To upgrade a Release 22.9 or later NFM-P auxiliary server” (p. 940) on each [Aux1] auxiliary server station.

Start auxiliary servers [Aux1]

206

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.

Disable maintenance mode for auxiliary database agents

207

If the system does not include an auxiliary database, go to Step 211.

208

If the system includes redundant auxiliary database clusters, perform one of the following to put each agent in active mode.

a. If the NFM-P is in a shared-mode NSP deployment, perform the following steps.

   1. Log in as the root user on the NSP cluster host in the primary data center.
   2. Enter the following to set the nspos-auxdb-agent mode to active:

      ```
      # kubectl patch configmap/nspos-auxdb-agent-overrides --type=merge
      -p '{"data":{"nspos-auxdb-agent-overrides.json":"{\"auxDbAgent\":
      {\"config\":{\"maintenance-mode\":false}}}"}}' ↵
      ```

   3. Enter the following to restart the nspos-auxdb-agent:

      ```
      # kubectl delete pod `kubectl describe pods | grep -P ^^Name: |
      grep -oP nspos-auxdb-agent[-a-zA-Z0-9]+` ↵
      ```

   4. Log in as the root user on the NSP cluster host in the standby data center.
   5. Enter the following to set the nspos-auxdb-agent mode to active:

      ```
      # kubectl patch configmap/nspos-auxdb-agent-overrides --type=merge
      -p '{"data":{"nspos-auxdb-agent-overrides.json":"{\"auxDbAgent\":
      {\"config\":{\"maintenance-mode\":false}}}"}}' ↵
      ```

b. If the NFM-P is not in a shared-mode NSP deployment, enter the following as the root user on the new primary main server [Main2]:

   ```
   # sed -i -r 's/("maintenance-mode"\s*:\s*)true/\1false/g'
   /opt/nsp/os/auxdb-agent/conf/nspos-auxdb-agent-overrides.json ↵
   ```

   The cluster enters active mode within approximately one minute.

Verify auxiliary database status

209

You must verify that the standalone or new primary auxiliary database cluster is in active mode.

a. If the NFM-P is in a shared-mode NSP deployment, issue the following REST API call:

> ℹ **Note:** In order to issue a REST API call, you require a REST token; see this tutorial on the Network Developer Portal for information.

```
GET /data/auxdb:/auxdb-agent HTTP/1.1
```

Request body:

```
    Host: address:8545
    Content-Type: application/json
    Authorization: bearer_and_token_from_session_manager
```

where *address* is the advertised address of the primary NSP cluster

The cluster is in active mode if the REST response includes ACTIVE.

b. If the NFM-P is not in a shared-mode NSP deployment, enter the following as the root user on the new primary main server [Main2]:

```
# /opt/nsp/os/nspd/nspdctl auxdb agent-status ↵
```

A status message is displayed.

The cluster is in active mode if the message includes ACTIVE.

210

Perform one of the following to verify the auxiliary database operation.

a. If the NFM-P is in a shared-mode NSP deployment, issue the following REST API call:

> ℹ **Note:** In order to issue a REST API call, you require a REST token; see this tutorial on the Network Developer Portal for information.

```
GET https://{{address}}:8545/restconf/data/auxdb:/clusters
```

where *address* is the advertised address of the primary NSP cluster

The call returns auxiliary database cluster status information like the following, which is the output for redundant clusters; if each mode and status value are not as shown below, contact technical support.

```
<HashMap>
    <clusters>
        <cluster>
            <name>cluster_M</name>
            <mode>ACTIVE</mode>
            <status>UP</status>
            <nodes>
```

```
                <external-ip>203.0.113.101</external-ip>
                <internal-ip>10.1.2.101</internal-ip>
                <status>UP</status>
            </nodes>
            <nodes>
                <external-ip>203.0.113.102</external-ip>
                <internal-ip>10.1.2.102</internal-ip>
                <status>UP</status>
            </nodes>
            <nodes>
                <external-ip>203.0.113.103</external-ip>
                <internal-ip>10.1.2.103</internal-ip>
                <status>UP</status>
            </nodes>
        </cluster>
        <cluster>
            <name>cluster_N</name>
            <mode>STANDBY</mode>
            <status>ON_STANDBY</status>
            <nodes>
                <external-ip>203.0.113.104</external-ip>
                <internal-ip>10.1.2.104</internal-ip>
                <status>READY</status>
            </nodes>
            <nodes>
                <external-ip>203.0.113.105</external-ip>
                <internal-ip>10.1.2.105</internal-ip>
                <status>READY</status>
            </nodes>
            <nodes>
                <external-ip>203.0.113.106</external-ip>
                <internal-ip>10.1.2.106</internal-ip>
                <status>READY</status>
            </nodes>
        </cluster>
    </clusters>
</HashMap>
```

b. If the NFM-P is not in a shared-mode NSP deployment, enter the following as the root user on the primary main server [Main2]:

```
# nspdctl auxdb status ↵
```

Cluster status information such as the following is displayed.

Note: The Output for a standalone auxiliary database shows only one cluster.

```
CLUSTER     DC-ROLE    STATE
cluster_M  ACTIVE     UP
NODE             INTERNAL IP    STATE
203.0.113.101  10.1.2.101     UP
203.0.113.102  10.1.2.102     UP
203.0.113.103  10.1.2.103     UP
CLUSTER     DC-ROLE    STATE
cluster_N  STANDBY    ON_STANDBY
NODE             INTERNAL IP     STATE
203.0.113.104  10.1.2.104      READY
203.0.113.105  10.1.2.105      READY
203.0.113.106  10.1.2.106      READY
```

If each STATE value is not as shown above, contact technical support.

Check post-upgrade disk space

211

If you are performing a trial upgrade on a lab system in advance of a live upgrade, you must check the available capacity of the disk partitions on each component against the values recorded in Step 1.

Perform the following steps on each of the following stations:

- main server
- auxiliary server
- main database
- auxiliary database

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following:

   ```
   # df -kh ↵
   ```

   The usage information for each partition is displayed.
4. Record the information for each NFM-P partition; see the tables in Chapter 2, “NSP disk setup and partitioning” for the partition names and required capacities.
5. Compare the partition values with the values recorded in Step 1.

6. If the disk usage on an NFM-P partition approaches 80% or has increased substantially, you may need to add disk capacity before you attempt the upgrade on a live system. Contact technical support for assistance.

Install or upgrade single-user GUI clients

212

As required, install or upgrade additional single-user GUI clients; see the following for information:

- “NFM-P single-user GUI client installation” (p. 585)
- “NFM-P single-user GUI client upgrade from Release 22.9 or later” (p. 955)

Install or upgrade client delegate servers

213

As required, install or upgrade client delegate servers; see the following for information:

- “NFM-P client delegate server installation” (p. 591)
- “NFM-P client delegate server upgrade from Release 22.9 or later” (p. 963)

Stop PKI server

214

If no other components are to be deployed, stop the PKI server by entering Ctrl+C in the console window.

Restore TLS version and cipher support configuration

215

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, see the *NSP System Administrator Guide* for information about how to restore the TLS version and cipher support settings.

Note: TLS 1.0 and 1.1 are disabled by default after an upgrade. If either version is enabled before an NFM-P system upgrade and required after the upgrade, you must re-enable the version support after the upgrade.

Configure and enable firewalls

216

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 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 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 from Release 22.9 or later

16.15 To upgrade a Release 22.9 or later NFM-P auxiliary server

16.15.1 Description

The following steps describe how to upgrade the Release 22.9 or later 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 performs only SNMP statistics 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

16.15.2 Steps

1

If the auxiliary server is deployed in a VM created using an NSP RHEL OS disk image, perform 3.4 “To apply a RHEL update to an NSP image-based OS” (p. 67) on the auxiliary server station.

2

Log in as the root user on the auxiliary server station.

3

Open a console window.

4

Enter the following sequence of commands to disable the auxiliary server services:

```
# systemctl disable nfmp-aux.service ↵
# systemctl disable nfmp-aux-config.service ↵
```

5

If the auxiliary server is running, stop the auxiliary server.

1. Enter the following to switch to the nsp user:

   ```
   # su - nsp ↵
   ```

2. Enter the following:

```
bash$ cd /opt/nsp/nfmp/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.

5. Enter the following to switch back to the root user:

```
# exit ↵
```

6

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
- nsp-nfmp-nodeexporter-*R*.*r*.*p*-rel.*v*.rpm, if the NFM-P is in a shared-mode deployment and you want to forward NFM-P system metrics to the NSP

where

R.*r*.*p* is the NSP release identifier, in the form *MAJOR*.*minor*.*patch*

v is a version identifier

7

Navigate to the directory that contains the NFM-P installation files.

Note: Ensure that the directory contains only the installation files.

8

Enter the following:

```
# chmod +x * ↵
```

9

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf 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
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

11

Enter the following; see 14.9 “NFM-P samconfig utility” (p. 432) for information about using samconfig:

```
# samconfig -m aux ↵
```

The following is displayed:

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

12

Enter the following:

```
<aux> configure ↵
```

The prompt changes to `<aux configure>`.

13

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; see 14.9 “NFM-P samconfig utility” (p. 432) for information about using the samconfig utility.
3. If required, modify one or more parameter values, and then enter **back** ↵.
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.

14

Close the console window.

END OF STEPS

Auxiliary database upgrade from Release 22.9 or later

16.16 To upgrade a Release 22.9 or later NFM-P auxiliary database cluster

16.16.1 Description

The following procedure is performed as part of a standalone or redundant system upgrade from Release 22.9 or later.

In a redundant NFM-P system upgrade, the standby components are upgraded while the primary components remain operational. The upgraded standby components then assume the primary role while the former primary components are upgraded.

If a redundant system includes a redundant auxiliary database, the network outage during a redundant system upgrade is limited to the initialization time of the upgraded former standby components.

If a redundant system includes a standalone auxiliary database, the network outage during a redundant system upgrade includes the auxiliary database upgrade duration.

Note: CPU frequency scaling 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” CPU frequency scaling governor on a station.

Setting CPU frequency scaling to “performance” effectively disables the function, so may result in greater energy consumption by a station.

Note: Enabling TLS on an auxiliary database is not supported during an upgrade.

Note: You require the following user privileges on each auxiliary database station:

- root
- samauxdb

Note: Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

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

16.16.2 Steps

Obtain software

1

Download the following installation files to an empty local directory on a station that is reachable by each auxiliary database station in the cluster:

- nspos-auxdb-*R.r.p*-rel.*v*.rpm
- VerticaSw_PreInstall.sh
- nspos-jre-*R.r.p*-rel.*v*.rpm
- vertica-*R.r.p*-rel.tar

where

R.r.p is the NSP release identifier, in the form *MAJOR.minor.patch*

v is a version number

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.

If you are upgrading a standalone auxiliary database, or the standby cluster in a redundant auxiliary database, 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 1 Gb/s link to the location is required; if achievable, a higher-capacity link is recommended.

For auxiliary database backup information, see the *NSP System Administrator Guide* for the installed release.

Stop cluster

3

Log in as the root user on an auxiliary database station in the cluster that is being upgraded.

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 ↵
```

Information like the following is displayed:

```
Database status
Node        | Host           | State | Version | DB
------------+---------------+-------+---------+-------
node_1 | internal_IP_1 | STATE | version | db_name
node_2 | internal_IP_2 | STATE | version | db_name
.
.
.
node_n | internal_IP_n | STATE | version | db_name
      Output captured in log_file
```

The cluster is stopped when each *STATE* entry reads DOWN.

8

Repeat Step 7 periodically until the cluster is stopped.

Note: You must not proceed to the next step until the cluster is stopped.

Prepare all stations for upgrade

9

Perform Step 11 to Step 28 on each auxiliary database station in the cluster that is being upgraded.

10

Go to Step 29.

Prepare individual station for upgrade

11

If the auxiliary database station is deployed in a VM created using an NSP RHEL OS disk image, perform 3.4 "To apply a RHEL update to an NSP image-based OS" (p. 67).

12

Log into the auxiliary database station as the root user.

13

Open a console window.

14

Enter the following sequence of commands to stop the auxiliary database services:

```
# systemctl stop nfmp-auxdb.service ↵
# systemctl stop vertica_agent.service ↵
# systemctl stop verticad.service ↵
```

15

Enter the following sequence of commands to disable the database services:

```
# systemctl disable nfmp-auxdb.service ↵
# systemctl disable nfmp-auxdbproxy.service ↵
# systemctl disable vertica_agent.service ↵
# systemctl disable verticad.service ↵
```

16

Transfer the downloaded installation files to an empty directory on the station.

ℹ **Note:** In subsequent steps, the directory is called the software directory.

17

Navigate to the software directory.

ℹ **Note:** Ensure that the directory contains only the installation files.

18

Enter the following:

```
# chmod +x * ↵
```

19

Enter the following:

# ./VerticaSw_PreInstall.sh ↵

Information like the following is displayed:

```
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...
```

20

Enter the following to reboot the station:

```
# systemctl reboot ↵
```

The station reboots.

21

When the reboot is complete, log in to the station as the root user.

22

Open a console window.

23

Enter the following:

```
# cd /opt/nsp/nfmp/auxdb/install/bin ↵
```

24

Enter the following to display the auxiliary database status:

```
# ./auxdbAdmin.sh status ↵
```

Information like the following is displayed:

```
Database status
Node       | Host          | State | Version | DB
------------+---------------+-------+---------+-------
node_1 | internal_IP_1 | STATE | version | db_name
node_2 | internal_IP_2 | STATE | version | db_name
.
.
.
node_n | internal_IP_n | STATE | version | db_name
      Output captured in log_file
```

25

if any *STATE* entry is not DOWN, perform the following steps.

1. Enter the following to stop the auxiliary database:

   ```
   # ./auxdbAdmin.sh stop ↵
   ```

2. Repeat Step 24 periodically until each *STATE* entry reads DOWN.

   Note: You must not proceed to the next step until each *STATE* entry reads DOWN.

26

Navigate to the software directory.

27

Enter the following:

```
# dnf install nspos-*.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt for each package:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

28

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

Upgrade database

29

Log in as the root user on an auxiliary database station in the cluster that is being upgraded.

30

Open a console window.

31

Enter the following:

```
# cd /opt/nsp/nfmp/auxdb/install/bin ↵
```

32

Enter the following:

```
# ./auxdbAdmin.sh upgrade tar_file ↵
```

where *tar_file* is the absolute path and filename of the vertica-*R.r.p*-rel.tar file in the software directory

The following prompt is displayed:

```
Updating Vertica - Please perform a backup before proceeding with this
option
```

```
Do you want to proceed (YES/NO)?
```

33

Enter YES ↵.

The following prompt is displayed:

```
Please enter auxiliary database dba password [if you are doing initial
setup for auxiliary database, press enter]:
```

34

Enter the dba password.

The following prompt is displayed:

```
Please verify auxiliary database dba password:
```

35

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
```

36

Enter the following to display the auxiliary database status:

```
# ./auxdbAdmin.sh status ↵
```

Information like the following is displayed:

```
Database status
Node       | Host           | State | Version | DB
------------+---------------+-------+---------+-------
node_1 | internal_IP_1 | STATE | version | db_name
node_2 | internal_IP_2 | STATE | version | db_name
.
.
.
node_n | internal_IP_n | STATE | version | db_name
      Output captured in log_file
```

The cluster is running when each *STATE* entry reads UP.

37

Repeat Step 36 periodically until the cluster is running.

i **Note:** You must not proceed to the next step until the cluster is running.

Update database schema

38

Update the NFM-P database schema.

i **Note:** The schema update may take considerable time.

1. Log in as the nsp user on the NFM-P main server.
2. Open a console window.
3. Enter the following:

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

4. Enter the following:

```
bash$ ./nmsserver.bash upgradeAuxDbSchema ↵
```

   The following prompt is displayed:

```
Auxiliary database clusters:
1: IP_a,IP_b,IP_c
2: IP_x,IP_y,IP_z
Select auxiliary database to upgrade:
```

5. Enter the number that corresponds to the cluster you are upgrading.

   The following messages and prompt are displayed:

```
WARNING: About to upgrade samdb schema on the auxiliary database
cluster [IP_a,IP_b,IP_c].
It is recommended that a database backup is performed before
proceeding.
Type "YES" to continue
```

6. Enter YES.

   The following prompt is displayed:

```
Please enter the auxiliary database port [5433]:
```

7. Enter the auxiliary database port number; press Enter to accept the default of 5433.

   The following prompt is displayed:

```
Please enter the auxiliary database user password:
```

8. Enter the required password.

   The following messages are displayed as the upgrade begins:

```
INFO: Database upgrade can take a very long time on large
databases.
INFO: logs are stored under /opt/nsp/nfmp/server/nms/log/auxdb.
Check the logs for progress.
INFO: Node Name[v_samdb_node0001]->IP[IP_address]->Status[UP]
```

```
INFO: About to perform upgrade
```

Synchronize auxiliary database password

39

If the NFM-P is in a shared-mode NSP system, perform the following steps.

1. Log on as the root user on the NSP cluster host.
2. Open a console window.
3. Enter the following:

   ```
   # cd /opt ↵
   ```
4. Enter the following:

   ```
   # sftp root@deployer_IP ↵
   ```

   where *deployer_IP* is the NSP deployer host IP address

   The prompt changes to `sftp>`.
5. Enter the following:

   ```
   sftp> cd
   /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/database ↵
   ```
6. Enter the following:

   ```
   sftp> get sync-auxdb-password.bash ↵
   ```
7. Enter the following:

   ```
   sftp> quit ↵
   ```
8. Enter the following:

   ```
   # chmod 777 sync-auxdb-password.bash ↵
   ```
9. Enter the following:

   ```
   # ./sync-auxdb-password.bash ↵
   ```
10. If the command in substep 9 succeeds, output like the following is displayed:

    ```
    timestamp: Synchronizing password for Auxiliary DB Output...
    timestamp: deployment.apps/tlm-vertica-output scaled
    timestamp: secret/tlm-vertica-output patched
    timestamp: deployment.apps/tlm-vertica-output scaled
    timestamp: Synchronization completed.
    ```
11. If the command output is not as expected, the NFM-P initialization may not be complete; wait 30 minutes, and then return to substep 9. Several attempts may be required.

40

Perform the following steps on each station in the auxiliary database cluster.

1. Log in as the root user.
2. Open a console window.

3. Enter the following sequence of commands to enable the database services:

```
systemctl enable nspos-auxdb.service
systemctl enable nspos-auxdbproxy.service
systemctl enable vertica_agent.service
systemctl enable verticad.service
```

41

If you are upgrading the standby cluster in a redundant deployment, go to Step 43.

42

Enter the following on each station in the cluster to start the database proxy:

```
# systemctl start nspos-auxdbproxy.service ↵
```

43

Close the open console windows.

END OF STEPS

NFM-P single-user GUI client upgrade from Release 22.9 or later

16.17 Upgrading a Release 22.9 or later single-user GUI client

16.17.1 Introduction

This section describes how to upgrade a Release 22.9 or later NFM-P single-user GUI client in a standalone or redundant NFM-P deployment.

You must comply with the general requirements in "NFM-P deployment configuration" (p. 370), and any specific requirements in this section, before you attempt to upgrade an NFM-P single-user GUI client.

Post-upgrade client connection to multiple NFM-P systems

You can configure a single-user client to connect to multiple NFM-P systems. For information , see 13.19 "To configure a GUI client login form to list multiple NFM-P systems" (p. 394).

16.17.2 Platform requirements

Single-user GUI client deployment is supported on the following platforms:

- Mac OS X
- Microsoft Windows
- RHEL

General

The following are the security requirements for single-user client upgrade:

- An upgrade requires only local user privileges.
- Only the user that deploys the client software, or a user with sufficient privileges, such as root or a local administrator, can start a single-user client.

i **Note:** Single-user client upgrade requires a supported web browser on the client station. See the *NSP Planning Guide* for browser support information.

Mac OS

See the *NSP Planning Guide* for the Mac OS single-user client deployment requirements.

Microsoft Windows

See the *NSP Planning Guide* for the Microsoft Windows single-user client deployment requirements.

RHEL

A RHEL single-user GUI client station must have:

- a supported OS release and patch level, as described in the *NSP Planning Guide*
- the required RHEL OS configuration and packages, as described in Chapter 3, "RHEL OS deployment for the NSP"

Optionally, for greater system security, you can remove the world permissions from RHEL compiler executable files; see A.1 “Resetting GCC-compiler file permissions” (p. 1093) for information.

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

16.18 To upgrade a Release 22.9 or later NFM-P single-user GUI client

16.18.1 Purpose

The following steps describe how to upgrade the Release 22.9 or later NFM-P software on a single-user GUI client station in a standalone or redundant NFM-P deployment.

Note: The main server to which the client connects must be upgraded and running when you perform the 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

Note: A leading `bash$` in a CLI command line represents the RHEL prompt, and is not to be included in the command.

16.18.2 Steps

1

Log in to the client station.

2

Close the client GUI, if it is open.

3

Use a browser to open the NSP sign-in page.

4

Enter the required login credentials and click SIGN IN. The NSP UI is displayed.

5

If one of the following is true, perform the following steps.

- The client is configured to connect to only one NFM-P system.
- The client is configured to connect to multiple NFM-P systems, and you do not want to keep the current client version.

Note: If the client is configured to connect to multiple NFM-P systems, and after the upgrade you select a non-upgraded system in the Server drop-down list of the client, you are prompted to downgrade the client. A client downgrade erases the multiple-system client configuration. If you want to preserve the Server drop-down options, do not downgrade the client.

1. Double-click on the NSP NFM-P Client desktop icon.
2. Go to Step 8.

6

Perform the following steps if the following conditions are true:

- The client is configured to connect to multiple NFM-P systems.
- You want to keep the current client version for connection to a system that is not yet upgraded.
- The system is the first of the multiple NFM-P systems to be upgraded.

If the conditions are true, you must remove the upgraded system from the configuration on the client station, and must not use the desktop icon to open the client.

a. On a Windows station:

1. Open the Registry Editor.
2. Navigate to the following key:

   Computer\HKEY_CURRENT_USER\SOFTWARE\JavaSoft\Prefs
3. Select and delete the IP address or hostname of each upgraded NFM-P main server.
4. Close the Registry Editor.
5. Edit the following file to remove the <j2ee and <systemMode lines for the upgraded NFM-P system.

   install_dir\nms\config\nms-client.xml

   where *install_dir* is the client installation directory
6. Edit the following file to replace all occurrences of the upgraded system, if present, with the IP address or hostname of a system that is not yet upgraded:

   Note: It is recommended to use the address or hostname of the system that is to be upgraded last.

   Note: For a redundant system, you must replace both main server addresses or hostnames.

   install_dir\nms\bin\locallaunch.jnlp
7. Right-click the desktop icon, select Properties, and change the name on the General tab to the IP address or hostname of a different NFM-P system.

   Note: It is recommended to use the address or hostname of the system that is to be upgraded last.
8. From the Java Control Panel, clear the Java cache of any entries for the recently upgraded system.
9. Right-click the client desktop icon, select Properties, and change the name on the General tab to the IP address or hostname of a different NFM-P system.
10. Install a new client instance.

ℹ **Note:** You must specify a new client installation location, and not the current location.

b. On a RHEL station:

1. Open the following file using a plain-text editor such as vi:

   ~/.java/.userPrefs/prefs.xml

2. Select and delete the IP address or hostname of each upgradedNFM-P main server.
3. Save and close the file.
4. Edit the following file to remove the <j2ee and <systemMode lines for the upgraded NFM-P system.

   install_dir/nms/config/nms-client.xml

   where *install_dir* is the client installation directory

5. Edit the following file to replace all occurrences of the upgraded system, if present, with the IP address or hostname of a system that is not yet upgraded:

   Note: It is recommended to use the address or hostname of the system that is to be upgraded last.

   Note: For a redundant system, you must replace both main server addresses or hostnames.

   install_dir/nms/bin/locallaunch.jnlp

6. Edit the desktop icon file to replace each occurrence of the upgraded system with the IP address or hostname of a system that is not yet upgraded.

   Note: It is recommended to use the address or hostname of the system that is to be upgraded last.

7. From the Java Control Panel, clear the Java cache of any entries for the recently upgraded system.
8. Install a new client instance.

ℹ **Note:** You must specify a new client installation location, and not the current location.

7

If the client is configured to connect to multiple NFM-P systems, and the upgraded system is not the first to be upgraded, perform the following steps.

a. For a Windows client:

1. Edit the following file to add <j2ee and <systemMode lines for each main server in the upgraded NFM-P system:

   new_install_dir\nms\config\nms-client.xml

   where *new_install_dir* is the installation directory of the new client installed in Step 6

2. Use the new client desktop icon to open the GUI for the upgraded system.

b. For a RHEL client:

1. Edit the following file to add <j2ee and <systemMode lines for each main server in the upgraded NFM-P system:

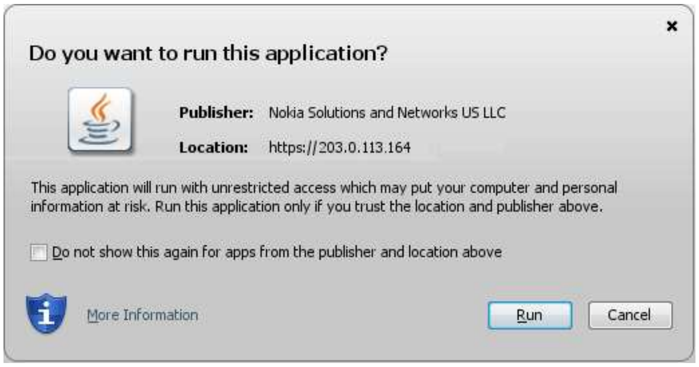
   new_install_dir/nms/config/nms-client.xml where *new_install_dir* is the installation directory of the new client installed in Step 6

2. Use the new client desktop icon to open the GUI for the upgraded system.

8

A form like the following is displayed.

Figure 16-2 Do you want to run this application?



Do you want to run this application?

Publisher: Nokia Solutions and Networks US LLC

Location: https://203.0.113.164

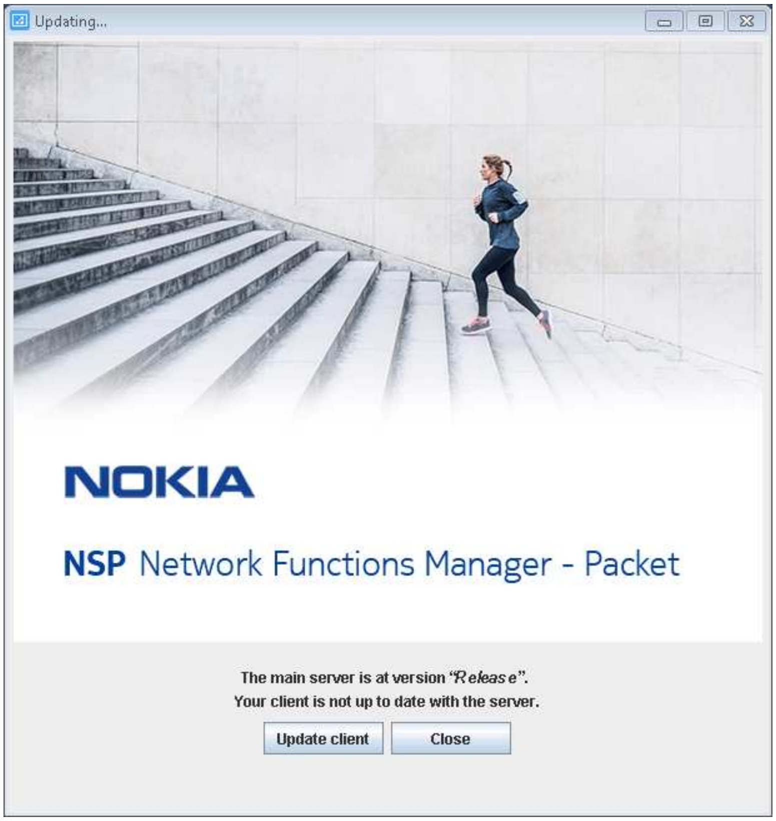
This application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the location and publisher above.

□ Do not show this again for apps from the publisher and location above

Click Run.

The panel shown in Figure 16-3, “Updating...” (p. 960) is displayed.

Figure 16-3 Updating...



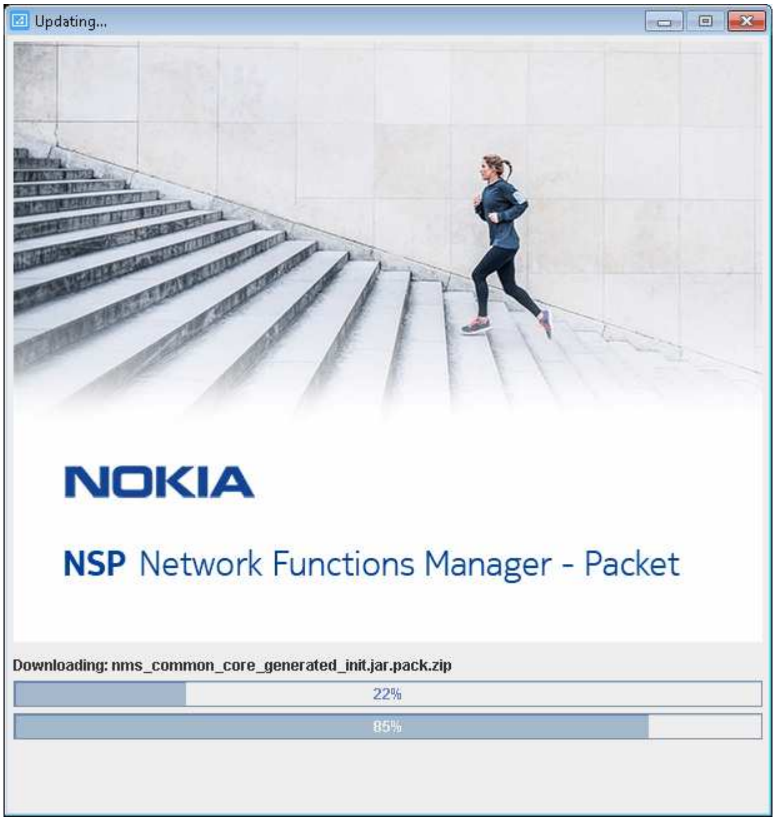
The main server is at version “Release”.
Your client is not up to date with the server.

9

Click Update client.

The client upgrade begins, and the panel shown in Figure 16-4, “Updating...” (p. 961) is displayed. The panel uses separate bars to indicate the overall and current task progress.

Figure 16-4 Updating...



Downloading: nms_common_core_generated_init.jar.pack.zip

10

If the client is installed on Mac OS X, perform the following steps.

1. Open a console window.
2. Navigate to the following directory:

   /Applications/NFMPclient.*IP_address*.app/Contents/Resources/nms/bin
3. Enter the following:

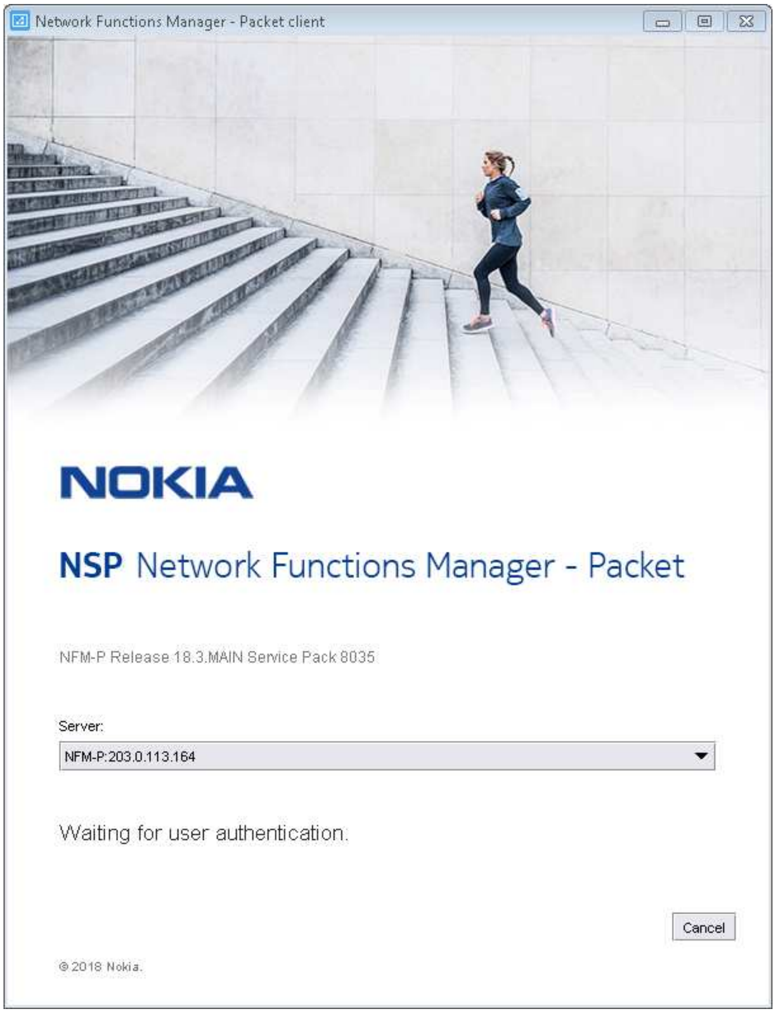
   chmod +x nmsclient.bash ↵

11

If you are not currently logged in, the splash screen shown in Figure 16-5, “Waiting for user authentication” (p. 962) opens, and the NSP sign-in page is displayed.

Enter the required login credentials on the NSP sign-in page and click SIGN IN. The NSP UI is displayed, and the client GUI opens.

Figure 16-5 Waiting for user authentication



Network Functions Manager - Packet client
NOKIA
NSP Network Functions Manager - Packet
Cancel
© 2018 Nokia.

NFM-P Release 18.3.MAIN Service Pack 8035

Server:
NFM-P:203.0.113.164

Waiting for user authentication.

12

Verify that the GUI is operational and correctly displayed.

END OF STEPS

NFM-P client delegate server upgrade from Release 22.9 or later

16.19 Upgrading a Release 22.9 or later client delegate server

16.19.1 Introduction

This section describes how to upgrade a Release 22.9 or later NFM-P client delegate server in a standalone or redundant NFM-P deployment.

You must comply with the general requirements in “NFM-P deployment configuration” (p. 370), and any specific requirements in this section, before you attempt to upgrade an NFM-P client delegate server.

16.19.2 Platform requirements

Client delegate server deployment is supported on the following platforms:

- RHEL
- Microsoft Windows

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 Planning Guide* for a list of the ports that must be open on each component.

Note: Client delegate server deployment requires a supported web browser on the client delegate server station. See the *NSP Planning Guide* for browser support information.

Microsoft Windows

See the *NSP Planning Guide* for the supported Microsoft Windows versions for client delegate server deployment.

Note: Client delegate server deployment on Windows requires local Administrator privileges.

RHEL

A RHEL client delegate server station must have:

- a supported OS release and patch level, as described in the *NSP Planning Guide*
- the required RHEL OS configuration and packages, as described in Chapter 3, “RHEL OS deployment for the NSP”
- the required Oracle JRE version; see the *NSP Planning Guide* for information

Optionally, for greater system security, you can remove the world permissions from RHEL compiler executable files; see A.1 “Resetting GCC-compiler file permissions” (p. 1093) for information.

Note: Client delegate server deployment on RHEL requires root user privileges.

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

16.20 To upgrade a Release 22.9 or later NFM-P client delegate server

16.20.1 Purpose

The following steps describe how to upgrade the Release 22.9 or later NFM-P software on a client delegate server station in a standalone or redundant NFM-P deployment.

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:

- Microsoft Windows—local Administrator
- RHEL—root

16.20.2 Steps

1

Close each remote client GUI session that the client delegate server hosts.

2

Log in to the client delegate server station.

3

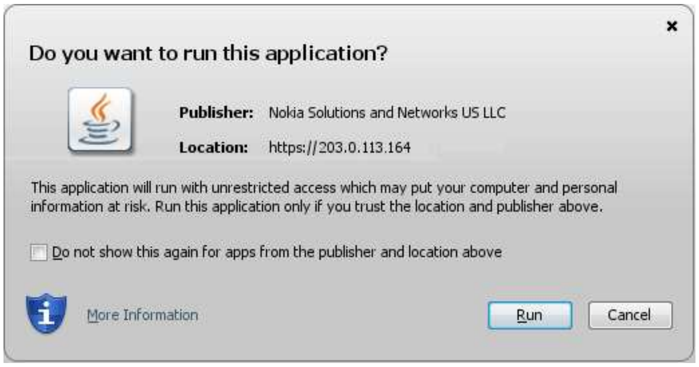
Close the local client GUI, if it is open.

4

Double-click on the NSP NFM-P Client desktop icon.

A form like the following is displayed.

Figure 16-6 Do you want to run this application?



Do you want to run this application?

Publisher: Nokia Solutions and Networks US LLC

Location: https://203.0.113.164

This 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.

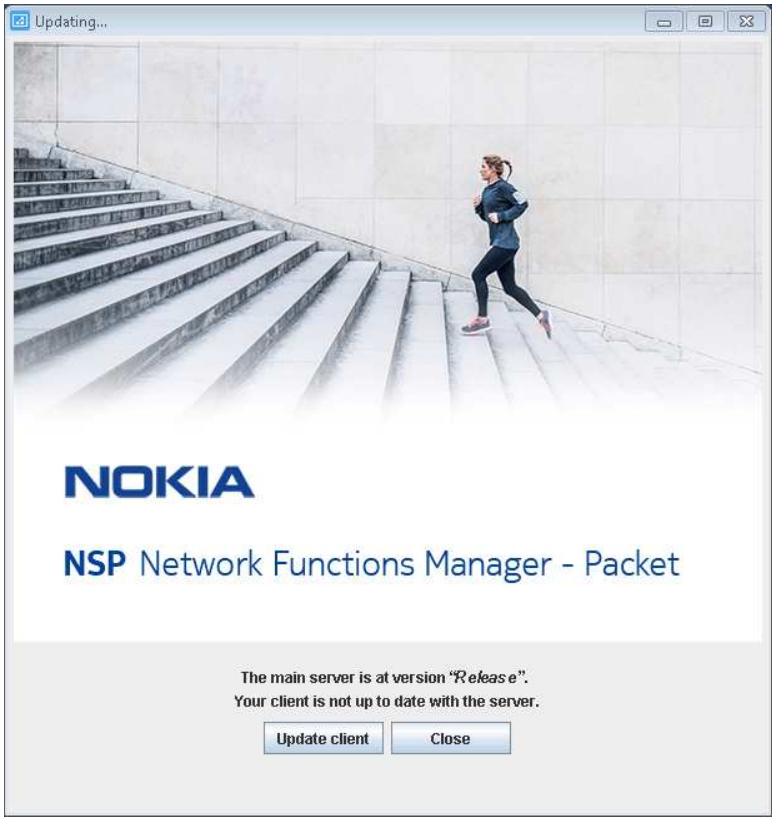
□ Do not show this again for apps from the publisher and location above

5

Click Run.

The panel shown in Figure 16-7, “Updating...” (p. 964) is displayed.

Figure 16-7 Updating...



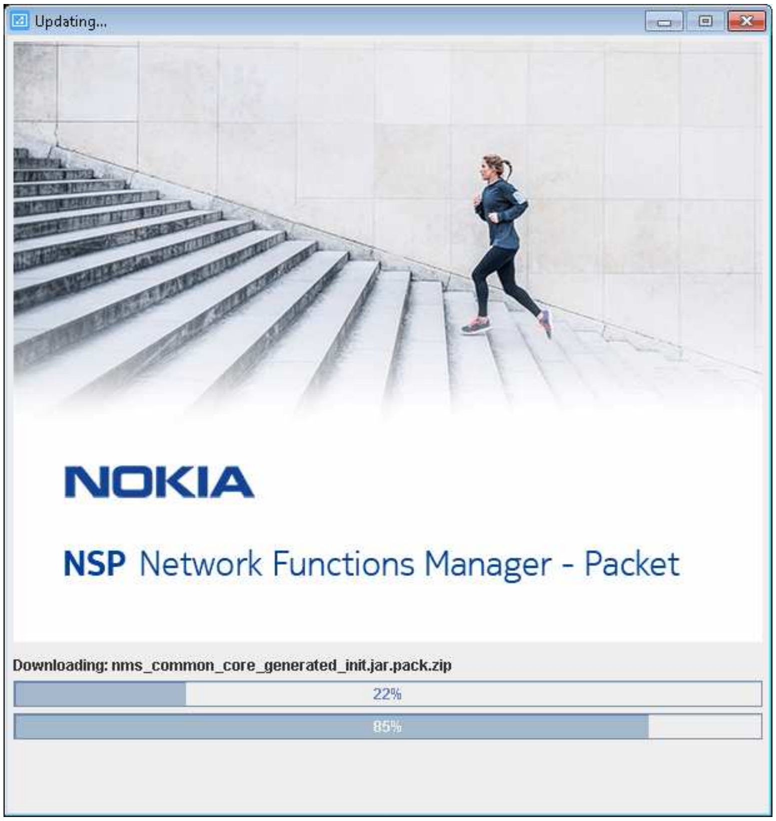
The main server is at version “Release”.
Your client is not up to date with the server.

6

Click Update client.

The client delegate server upgrade begins, and the panel shown in Figure 16-8, “Updating...” (p. 966) is displayed. The panel uses separate bars to indicate the overall and current task progress.

Figure 16-8 Updating...



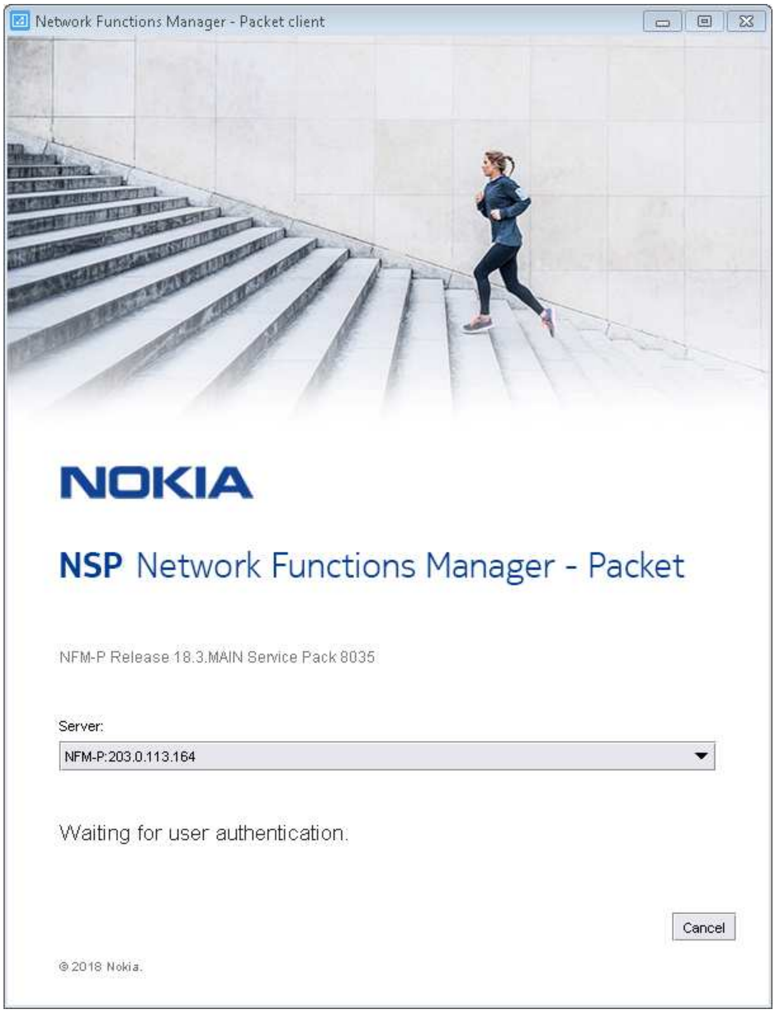
Downloading: nms_common_core_generated_init.jar.pack.zip

7

If you are not currently logged in, the splash screen shown in Figure 16-9, “Waiting for user authentication” (p. 967) opens, and the NSP sign-in page is displayed.

Enter the required login credentials on the NSP sign-in page and click SIGN IN. The NSP UI is displayed, and the client GUI opens.

Figure 16-9 Waiting for user authentication


Network Functions Manager - Packet client
NOKIA
NSP Network Functions Manager - Packet
Cancel
© 2018 Nokia.

NFM-P Release 18.3.MAIN Service Pack 8035

Server:
NFM-P:203.0.113.164

Waiting for user authentication.

8

Verify that the GUI is operational and correctly displayed.

END OF STEPS

17 NSP component conversion

17.1 Overview

17.1.1 Purpose

This chapter describes how to convert an NSP component deployed outside the NSP cluster to a different deployment type, for example, from standalone to redundant.

17.1.2 Contents

Converting NSP components

17.2 Introduction

17.2.1 Component conversion support

As a result of a conversion operation, you may need to update the configuration of other NSP components to support the modified deployment, for example, if a component IP address changes. Before you attempt a component conversion, ensure that each other component or system that is dependent on the component supports the planned conversion. See the *NSP Planning Guide* for component compatibility information.

NSP component conversion procedures

17.3 To enable redundancy support on an NSP analytics server

17.3.1 Purpose

When you convert a standalone NSP or NFM-P system to redundancy, and the system includes one or more NSP analytics servers, you must reconfigure each analytics server to support the redundant deployment, as described in the following steps.

Note: You must perform the steps on each NSP analytics server station in the system.

17.3.2 Steps

Stop analytics server

1

Log in to the NSP analytics server station as the nsp user.

2

Open a console window.

3

Enter the following:

```
bash$ cd /opt/nsp/analytics/bin ↵
```

4

Enter the following:

```
bash$ ./AnalyticsAdmin.sh stop ↵
```

The analytics server stops.

5

Start the PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 4.10 “To configure and enable a PKI server” (p. 113).

Note: The PKI server is required for internal system configuration purposes.

Update analytics server configuration

6

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
```

7

Enter YES. The script displays the first in a series of prompts.

8

Configure or update the following parameters, as required; for each other parameter, press ↵ to accept the current value:

- Primary Oracle Data Source DB Host
- Primary Oracle Data Source DB Name
- Primary Oracle Data Source DB Port
- Secondary Oracle Data Source DB Host
- Secondary Oracle Data Source DB Name
- Secondary Oracle Data Source DB Port
- Primary PostgreSQL Repository Database Host
- Secondary PostgreSQL Repository Database Host
- Zookeeper Connection String
- Use NFM-P-only mode

For information about a parameter, see Table 14-2, “NSP analytics server parameters” (p. 419).

Start analytics server

9

Enter the following:

```
bash$ ./AnalyticsAdmin.sh start ↵
```

The analytics server starts.

10

If no other components are to be deployed, stop the PKI server by entering Ctrl+C in the console window.

11

Close the open console windows.

12

Close the console window.

END OF STEPS

NFM-P system conversion to IPv6

17.4 Converting an NFM-P system to IPv6

17.4.1 Introduction

CAUTION

Service Disruption

An NFM-P system conversion 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 Planning Guide, and the NSP 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 NSP professional services 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.

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.

This section describes the conversion of inter-component communication from IPv4 to IPv6 in a standalone or redundant NFM-P system.

The NFM-P samconfig utility is used for component configuration and deployment. See 14.9 “NFM-P samconfig utility” (p. 432) for information about using the samconfig utility.

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

17.4.2 IPv6 conversion requirements

The following must be true before you attempt a system conversion to IPv6.

- 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 and functional; an upgraded main server performs crucial upgrade-specific tasks during startup.
- Each component in the NFM-P system is operational.

17.4.3 IPv6 conversion restrictions

An NFM-P system conversion from IPv4 to IPv6 is not supported during a system upgrade or conversion to redundancy.

17.5 NFM-P conversion to IPv6 workflow

17.5.1 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.

17.5.2 Stages

1

Perform the pre-conversion tasks; see 17.6 “To perform the pre-conversion tasks” (p. 973).

2

To convert a standalone NFM-P system to IPv6, perform 17.7 “To convert a standalone NFM-P system to IPv6” (p. 978) .

3

To convert a redundant NFM-P system to IPv6, perform 17.8 “To convert a redundant NFM-P system to IPv6” (p. 992) .

17.6 To perform the pre-conversion tasks

17.6.1 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:

- 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

17.6.2 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 "NSP TLS configuration" (p. 108).

Clear failed deployments

2

Clear all outstanding failed deployments; see the *NSP NFM-P User Guide* for information about how to view and manage failed deployments.

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
- nsp 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.

2. Choose Administration→Security→NFM-P User Security from the main menu. The NFM-P User Security - Security Management (Edit) form opens.
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.
9. Close the NFM-P User Security - Security Management (Edit) form.

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 reinstantiation begins, and the GUI status bar displays reinstantiation information.

   Note: Database reinstantiation 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.
6. When the reinstantiation 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 IP Address and Hostname values in the Primary Database Server panel and the Preferred DB setting in the Primary Server panel.
3. If the Preferred DB value does not match the IP Address value, perform a database switchover. See the database management chapter of the *NSP 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.

Back up the main database from the client GUI or a CLI; see the *NSP System Administrator Guide* for information.

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

17.7 To convert a standalone NFM-P system to IPv6

17.7.1 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

17.7.2 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 nspos-nspd.service ↵
   ```
4. Enter the following:
   ```
   # systemctl disable nfmp-main-config.service ↵
   ```
5. 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:

```
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.

5. Enter the following to switch to the root user:

   ```
   bash$ su ↵
   ```

6. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to display the nspOS service status:

   ```
   # nspdctl status ↵
   ```

   Information like the following is displayed.

   ```
   Mode:     standalone
   Role:     leader
   DC-Role:  active
   DC-Name:  dc_name
   Registry: IP_address:port
   State:    stopped
   Uptime:   0s
   SERVICE           STATUS
   service_a         inactive
   service_b         inactive
   service_c         inactive
   ```

   You must not proceed to the next step until all NSP services are stopped; if the State is not ‘stopped’, or the STATUS indicator of each listed service is not ‘inactive’, repeat this substep.

Update auxiliary database IP addresses

3

If the NFM-P includes an auxiliary database, perform the *NSP System Administrator Guide* procedure that describes changing the auxiliary database external IP addresses.

Stop main database

4

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

5

Enter the following:

```
# samconfig -m db ↵
```

The following is displayed:

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

6

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>`.

7

To enable IP validation, which restricts the server components that have access to the main database; configure the parameters in the following table, and then enter **`back`** ↵.

ℹ **Note:** For security reasons, it is strongly recommended that you enable IP validation.

ℹ **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 17-1 Standalone database parameters — ip-validation

Parameter	Description
main-one	Public IPv6 address of main server Configuring the parameter enables IP validation.
remote-servers	Comma-separated list of the IPv6 address of each of the following components that must connect to the database: • auxiliary servers • NSP Flow Collectors • NSP analytics servers

8

To enable the forwarding of NFM-P system metrics to the NSP; configure the parameters in the following table, and then enter **`back`** ↵.

Note: The parameters are required only for a distributed main database, so are not shown or configurable if the main server and database are collocated.

Table 17-2 Standalone database parameters — tls

Parameter	Description
keystore-pass	The TLS keystore password Default: available from technical support
pki-server	The PKI server IP address or hostname You must configure the parameter. Default: —
pki-server-port	The TCP port on which the PKI server listens for and services requests Default: 2391

9

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 14.9 “NFM-P samconfig utility” (p. 432) 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>`.

10

Enter the following to apply the configuration changes:

```
<db> apply ↵
```

The changes are applied.

11

Enter the following:

```
<db> exit ↵
```

The samconfig utility closes.

Configure auxiliary servers

12

If the NFM-P system includes auxiliary servers, perform Step 13 to Step 23 on each auxiliary server station. Otherwise, go to Step 24.

13

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.

14

Enter the following to switch to the root user:

```
bash$ su - ↵
```

15

Enter the following:

```
# samconfig -m aux ↵
```

The following is displayed:

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

16

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>`.

17

Enter the following, and then enter **back** ↵.

```
<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

18

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>`.

19

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

20

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

21

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 14.9 “NFM-P samconfig utility” (p. 432) 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>`.

22

Enter the following:

```
<aux> apply ↵
```

The configuration is applied.

23

Enter the following:

```
<aux> exit ↵
```

The samconfig utility closes.

Configure main server

24

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

25

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>`.

26

As required, configure the `client` parameters as described in the following table, and then enter **back** ↵.

Table 17-3 Standalone main server parameters — client

Parameter	Description
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.
public-ip	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.
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.

27

Enter the following, and then enter **back** ↵.

```
<main configure> database ip address ↵
```

where *address* is the IPv6 address of the database

28

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>`.

29

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 ↵
```

30

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 17-4 Standalone main server parameters — aux

Parameter	Description
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: —

31

Configure the `tls` parameters in the following table, and then enter **back** ↵.

Table 17-5 Standalone main server parameters — tls

Parameter	Description
keystore-file	The absolute path of the TLS keystore file To enable automated TLS deployment, enter `no keystore-file`. Default: —

Table 17-5 Standalone main server parameters — tls (continued)

Parameter	Description
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
alias	The alias specified during keystore generation You must configure the parameter. Default: —
pki-server	The PKI server IP address or hostname Default: —
pki-server-port	The TCP port on which the PKI server listens for and services requests Default: 2391
hsts-enabled	Whether HSTS browser security is enabled Default: false

32

If the NFM-P includes an auxiliary database, enter the following, and then enter **`back`** ↵:

Note: In a geo-redundant auxiliary database deployment, the order of the IP addresses must be the same on each main server in the geo-redundant system.

```
<main configure> auxdb ip-list cluster_1_IP1,cluster_1_IP2,cluster_1_IPn;cluster_2_IP1,cluster_2_IP2,cluster_2_IPn ↵
```

where

cluster_1_IP1, *cluster_1_IP2*,*cluster_1_IPn* are the external IPv6 addresses of the stations in one cluster

cluster_2_IP1, *cluster_2_IP2*,*cluster_2_IPn* are the external IPv6 addresses of the stations in the geo-redundant cluster; required only for geo-redundant auxiliary database

33

Configure the `nspos` parameters in the following table, and then enter **`back`** ↵.

Table 17-6 Standalone main server parameters — nspos

Parameter	Description
ip-list	The nspOS-server IP addresses, separated by a semicolon Specify only one IP address for a standalone NSP system. • If the NFM-P system is in a shared-mode NSP deployment specify the advertised address of each NSP cluster. • If the NSP system includes only the NFM-P, specify the main server private IP address. Default: —
address-to-nspos	The main server IP address that is reachable by the nspOS server Default: —
secure	Whether communication with the nspOS servers is secured using TLS Default: false
internal-certs	Whether internal certificates are used to secure nspOS communication between components; the parameter is configurable when the **secure** parameter is set to true. The parameter is deprecated, and must be set to the same value as the **secure** parameter. Default: false
dc-name	The nspOS DR data center name for aligning NSP components with the local NFM-P main server; must match the dcName value in the NSP configuration file The parameter is required only in a redundant deployment; however, in a shared-mode deployment, it is recommended that you configure the parameter, regardless of the NFM-P deployment type. Default: —

34

Configure the `remote-syslog` parameters in the following table, and then enter **`back`** ↵.

Table 17-7 Standalone main server parameters — remote-syslog

Parameter	Description
enabled	Enable the forwarding of the NFM-P User Activity logs in syslog format to a remote server Default: disabled
syslog-host	Remote syslog server hostname or IP address Default: —

Table 17-7 Standalone main server parameters — remote-syslog (continued)

Parameter	Description
syslog-port	Remote server TCP port Default: —
ca-cert-path	Absolute local path of public CA TLS certificate copied from remote server

35

Configure the `server-logs-to-remote-syslog` parameters in the following table, and then enter **`back`** ↵.

Table 17-8 Standalone main server parameters — server-logs-to-remote-syslog

Parameter	Description
enabled	Enable the forwarding of the NFM-P server logs in syslog format to a remote server Default: disabled
secured	Whether the communication with the remote server is TLS-secured Default: disabled
syslog-host	Remote syslog server hostname or IP address Default: —
syslog-port	Remote server TCP port Default: —
ca-cert-path	Absolute local path of public CA TLS certificate copied from remote server

36

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 14.9 “NFM-P samconfig utility” (p. 432) 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>`.

37

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

38

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Enable Windows Active Directory access

39

If you use Windows Active Directory for single-sign-on client access to the NFM-P, open the following file with a plain-text editor such as vi:

/opt/nsp/os/install/config.json

Otherwise, go to Step 45.

40

Change the IPv4 addresses to IPv6 addresses, as required.

41

Save and close the file.

42

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

43

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

44

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Start main server

45

Enter the following to enable the main server startup:

```
# systemctl enable nfmp-main.service ↵
```

46

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.

47

If Windows Active Directory access is configured to use the AUTHENTICATED type of LDAP server, and the NFM-P is not part of a shared-mode NSP deployment, enter the following to restart the local nspos-tomcat service:

Note: The service restart may take a few minutes, during which NFM-P GUI and REST client access is degraded. General NFM-P operation is unaffected.

```
# systemctl restart nspos-tomcat ↵
```

Start auxiliary servers

48

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:

   ```
   bash$ /opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash auxstart ↵
   ```

   The auxiliary server starts.

Verify converted system using GUI client

49

Use an NFM-P GUI client to perform sanity testing of the converted system.

ℹ **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.

END OF STEPS

17.8 To convert a redundant NFM-P system to IPv6

17.8.1 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.

ℹ **Note:** You require the following user privileges:

- on each main and auxiliary server station — 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

17.8.2 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 nspos-nspd.service ↵
   ```
4. Enter the following:
   ```
   # systemctl disable nfmp-main-config.service ↵
   ```
5. Enter the following:
   ```
   # systemctl disable nfmp-main.service ↵
   ```

Stop standby main server

2

Stop the standby 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.

5. Enter the following to switch back to the root user:

   ```
   bash$ su ↵
   ```

6. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to display the nspOS service status:

   ```
   # nspdctl status ↵
   ```

   Information like the following is displayed.

   ```
   Mode:     DR
   Role:     redundancy_role
   DC-Role:  dc_role
   DC-Name:  dc_name
   Registry: IP_address:port
   State:    stopped
   Uptime:   0s
   SERVICE           STATUS
   service_a         inactive
   service_b         inactive
   service_c         inactive
   ```

   You must not proceed to the next step until all NSP services are stopped; if the State is not ‘stopped’, or the STATUS indicator of each listed service is not ‘inactive’, repeat this substep.

Stop reserved auxiliary servers

3

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 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 standby main database

4

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:

   ```
   # systemctl stop nfmp-oracle-proxy.service ↵
   ```

4. Enter the following to stop the main database:

   ```
   # 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 nspos-nspd.service ↵
   ```

4. Enter the following:

   ```
   # systemctl disable nfmp-main-config.service ↵
   ```

5. Enter the following:

   ```
   # systemctl disable nfmp-main.service ↵
   ```

Stop primary main server

6

Stop the primary main server.

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.

5. Enter the following to switch back to the root user:

   ```
   bash$ su ↵
   ```

6. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to display the nspOS service status:

   ```
   # nspdctl status ↵
   ```

   Information like the following is displayed.

   ```
   Mode:      DR
   Role:      redundancy_role
   DC-Role:   dc_role
   DC-Name:   dc_name
   Registry:  IP_address:port
   State:     stopped
   Uptime:    0s
   SERVICE            STATUS
   service_a          inactive
   service_b          inactive
   service_c          inactive
   ```

   You must not proceed to the next step until all NSP services are stopped; if the State is not ‘stopped’, or the STATUS indicator of each listed service is not ‘inactive’, repeat this substep.

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 ↵
   ```

Update auxiliary database IP addresses

9

If the NFM-P includes an auxiliary database, perform the *NSP System Administrator Guide* procedure that describes changing the auxiliary database external IP addresses.

Configure primary main database

10

Enter the following:

```
# samconfig -m db ↵
```

The following is displayed:

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

11

Enter the following:

```
<db> configure ip address ↵
```

where *address* is the IPv6 address of this database

The prompt changes to `<db configure>`.

12

Enter the following, and then enter **back** ↵:

```
<db configure> redundant ip address ↲
```

where *address* is the IPv6 address of the peer database

13

To enable IP validation, which restricts the server components that have access to the main database; configure the parameters in the following table, and then enter **`back`** ↲.

ℹ **Note:** For security reasons, it is strongly recommended that you enable IP validation.

ℹ **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 17-9 Primary database parameters — ip-validation

Parameter	Description
main-one	Public IPv6 address of primary main server Configuring the parameter enables IP validation.
main-two	Public IPv6 address of standby main server
remote-servers	Comma-separated list of the IPv6 address of each of the following components that must connect to the database: • auxiliary servers • NSP Flow Collectors • NSP analytics servers

14

To enable the forwarding of NFM-P system metrics to the NSP; configure the parameters in the following table, and then enter **`back`** ↲.

ℹ **Note:** The parameters are required only for a distributed main database, so are not shown or configurable if the main server and database are collocated.

Table 17-10 Primary database parameters — tls

Parameter	Description
keystore-pass	The TLS keystore password Default: available from technical support
pki-server	The PKI server IP address or hostname You must configure the parameter. Default: —

Table 17-10 Primary database parameters — tls (continued)

Parameter	Description
pki-server-port	The TCP port on which the PKI server listens for and services requests Default: 2391

15

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 14.9 “NFM-P samconfig utility” (p. 432) 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>`.

16

Enter the following to apply the configuration changes:

```
<db> apply ↵
```

The changes are applied.

17

Enter the following:

```
<db> exit ↵
```

The samconfig utility closes.

18

Enter the following:

```
# ssh-keyscan -t rsa standby_database_IPv6_address
>>/opt/nsp/nfmp/oracle19/.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

19

Log in as the root user on the primary main server station.

20

Open a console window.

21

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

22

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>`.

23

As required, configure the `client` parameters as described in the following table, and then enter **back** ↵.

Table 17-11 Primary main server parameters — client

Parameter	Description
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.
public-ip	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.

Table 17-11 Primary main server parameters — client (continued)

Parameter	Description
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.

24

Enter the following, and then enter **back** ↵:

```
<main configure> database ip address ↵
```

where *address* is the IPv6 address of the primary database

25

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

26

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 ↵
   ```

   The prompt changes to `<main configure>`.

27

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 17-12 Primary main server parameters — aux

Parameter	Description
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: —

28

If required, configure the `tls` parameters in the following table, and then enter **`back`** ↵.

Table 17-13 Primary main server parameters — tls

Parameter	Description
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
alias	The alias specified during keystore generation You must configure the parameter. Default: —
pki-server	The PKI server IP address or hostname Default: —

Table 17-13 Primary main server parameters — tls (continued)

Parameter	Description
pki-server-port	The TCP port on which the PKI server listens for and services requests Default: 2391
hsts-enabled	Whether HSTS browser security is enabled Default: false

29

If the NFM-P includes an auxiliary database, enter the following, and then enter **`back`** ↵:

Note: In a geo-redundant auxiliary database deployment, the order of the IP addresses must be the same on each main server in the geo-redundant system.

```
<main configure> auxdb ip-list cluster_1_IP1,cluster_1_IP2,cluster_1_
IPn;cluster_2_IP1,cluster_2_IP2,cluster_2_IPn ↵
```

where

cluster_1_IP1, *cluster_1_IP2*,*cluster_1_IPn* are the external IPv6 addresses of the stations in one cluster

cluster_2_IP1, *cluster_2_IP2*,*cluster_2_IPn* are the external IPv6 addresses of the stations in the geo-redundant cluster; required only for geo-redundant auxiliary database

30

Enter the following:

```
<main configure> redundancy enabled ↵
```

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

31

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

32

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

33

Enter the following, and then enter **`back`** ↵:

```
<main configure redundancy> database ip address ↵
```

where *address* is the IPv6 address of the standby database

34

Configure the `peer-server` redundancy parameters in the following table, and then enter **back** ↵.

Table 17-14 Primary main server parameters — redundancy, peer-server

Parameter	Description
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 23. 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 23. 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

35

Enter the following:

```
<main configure redundancy> back ↵
```

The prompt changes to `<main configure>`.

36

Configure the `nspos` parameters in the following table, and then enter **`back`** ↵.

Table 17-15 Primary main server parameters — nspos

Parameter	Description
ip-list	The nspOS-server IP addresses, separated by a semicolon Specify only one IP address for a standalone NSP system. • If the NFM-P system is in a shared-mode NSP deployment specify the advertised address of each NSP cluster. • If the NSP system includes only the NFM-P, specify the main server private IP address. Default: —
address-to-nspos	The main server IP address that is reachable by the nspOS server Default: —
secure	Whether communication with the nspOS servers is secured using TLS Default: false
internal-certs	Whether internal certificates are used to secure nspOS communication between components; the parameter is configurable when the **secure** parameter is set to true. The parameter is deprecated, and must be set to the same value as the **secure** parameter. Default: false
dc-name	The nspOS DR data center name for aligning NSP components with the local NFM-P main server; must match the dcName value in the NSP configuration file The parameter is required only in a redundant deployment; however, in a shared-mode deployment, it is recommended that you configure the parameter, regardless of the NFM-P deployment type. Default: —

37

Configure the `remote-syslog` parameters in the following table, and then enter **`back`** ↵.

Table 17-16 Standalone main server parameters — remote-syslog

Parameter	Description
enabled	Enable the forwarding of the NFM-P User Activity logs in syslog format to a remote server Default: disabled

Table 17-16 Standalone main server parameters — remote-syslog (continued)

Parameter	Description
syslog-host	Remote syslog server hostname or IP address Default: —
syslog-port	Remote server TCP port Default: —
ca-cert-path	Absolute local path of public CA TLS certificate copied from remote server

38

Configure the `server-logs-to-remote-syslog` parameters in the following table, and then enter **back** ↵.

Table 17-17 Standalone main server parameters — server-logs-to-remote-syslog

Parameter	Description
enabled	Enable the forwarding of the NFM-P server logs in syslog format to a remote server Default: disabled
secured	Whether the communication with the remote server is TLS-secured Default: disabled
syslog-host	Remote syslog server hostname or IP address Default: —
syslog-port	Remote server TCP port Default: —
ca-cert-path	Absolute local path of public CA TLS certificate copied from remote server

39

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 14.9 “NFM-P samconfig utility” (p. 432) 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>`.

40

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

41

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Enable Windows Active Directory access

42

If you use Windows Active Directory for single-sign-on client access to the NFM-P, open the following file with a plain-text editor such as vi:

/opt/nsp/os/install/config.json

Otherwise, go to Step 48.

43

Change the IPv4 addresses to IPv6 addresses, as required.

44

Save and close the file.

45

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

46

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

47

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Configure preferred auxiliary servers

48

If the NFM-P system does not include auxiliary servers, go to Step 63. Otherwise, perform Step 49 to Step 61 on each preferred auxiliary server station.

49

Log in as the root user.

50

Open a console window.

51

Enter the following:

```
# samconfig -m aux ↵
```

The following is displayed:

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

52

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>`.

53

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>`.

54

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

55

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>`.

56

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

57

Configure the `tls` parameters in the following table, and then enter **back** ↵.

Table 17-18 Auxiliary server parameters — tls

Parameter	Description
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
pki-server	The PKI server IP address or hostname Default: —
pki-server-port	The TCP port on which the PKI server listens for and services requests Default: 2391

58

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

The prompt changes to `<aux configure oss>`.

59

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 14.9 “NFM-P samconfig utility” (p. 432) 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>`.

60

Enter the following:

```
<aux> apply ↵
```

The configuration is applied.

61

Enter the following:

```
<aux> exit ↵
```

The samconfig utility closes.

Start preferred auxiliary servers

62

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 auxstart ↵
```

The auxiliary server starts.

Enable automatic startup, primary main server

63

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:

```
# systemctl enable nfmp-main.service ↵
```

Start primary main server

64

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:

   ```
   # 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.

Configure standby main database

65

Log in as the root user on the standby main database station.

66

Open a console window.

67

Enter the following:

```
# samconfig -m db ↵
```

The following is displayed:

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

68

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>`.

69

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>`.

70

Enter the following, and then enter **`back`** ↵:

```
<db configure redundant> instance instance_name ↵
```

where *`instance_name`* is the primary database instance name

71

To enable IP validation, which restricts the server components that have access to the main database; configure the parameters in the following table, and then enter **`back`** ↵.

Note: For security reasons, it is strongly recommended that you enable IP validation.

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 17-19 Standby database parameters — ip-validation

Parameter	Description
main-one	Public IPv6 address of standby main server Configuring the parameter enables IP validation.
main-two	Public IPv6 address of primary main server
remote-servers	Comma-separated list of the IPv6 address of each of the following components that must connect to the database: • auxiliary servers • NSP Flow Collectors • NSP analytics servers

72

To enable the forwarding of NFM-P system metrics to the NSP; configure the parameters in the following table, and then enter **`back`** ↵.

Note: The parameters are required only for a distributed main database, so are not shown or configurable if the main server and database are collocated.

Table 17-20 Standby database parameters — tls

Parameter	Description
keystore-pass	The TLS keystore password Default: available from technical support
pki-server	The PKI server IP address or hostname You must configure the parameter. Default: —
pki-server-port	The TCP port on which the PKI server listens for and services requests Default: 2391

73

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 14.9 “NFM-P samconfig utility” (p. 432) 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>`.

74

Enter the following to apply the configuration changes:

```
<db> apply ↵
```

The changes are applied.

75

Enter the following:

```
<db> exit ↵
```

The samconfig utility closes.

76

Enter the following:

```
# ssh-keyscan -t rsa primary_database_IPv6_address
>>/opt/nsp/nfmp/oracle19/.ssh/known_hosts
```

where *primary_database_IPv6_address* is the IPv6 address of the primary main database

Configure standby main server

77

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

78

Open a console window.

79

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

80

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>`.

81

As required, configure the `client` parameters as described in the following table, and then enter **back** ↵.

Table 17-21 Standby main server parameters — client

Parameter	Description
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 17-21 Standby main server parameters — client (continued)

Parameter	Description
public-ip	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.
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.

82

Enter the following, and then enter **back** ↵:

```
<main configure> database ip address ↵
```

where *address* is the IPv6 address of the standby database

83

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

84

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 ↵
   ```

85

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 17-22 Standby main server parameters — aux

Parameter	Description
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: —

86

Configure the `tls` parameters in the following table, and then enter **back** ↵.

Table 17-23 Standby main server parameters — tls

Parameter	Description
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 17-23 Standby main server parameters — tls (continued)

Parameter	Description
alias	The alias specified during keystore generation You must configure the parameter. Default: —
pki-server	The PKI server IP address or hostname Default: —
pki-server-port	The TCP port on which the PKI server listens for and services requests Default: 2391
hsts-enabled	Whether HSTS browser security is enabled Default: false

87

If the NFM-P includes an auxiliary database, enter the following, and then enter **back** ↵:

Note: In a geo-redundant auxiliary database deployment, the order of the IP addresses must be the same on each main server in the geo-redundant system.

```
<main configure> auxdb ip-list cluster_1_IP1,cluster_1_IP2,cluster_1_
IPn;cluster_2_IP1,cluster_2_IP2,cluster_2_IPn ↵
```

where

cluster_1_IP1, *cluster_1_IP2*,*cluster_1_IPn* are the external IPv6 addresses of the stations in one cluster

cluster_2_IP1, *cluster_2_IP2*,*cluster_2_IPn* are the external IPv6 addresses of the stations in the geo-redundant cluster; required only for geo-redundant auxiliary database

88

Enter the following:

```
<main configure> redundancy enabled ↵
```

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

89

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

90

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

91

Enter the following, and then enter **`back`** ↵:

```
<main configure redundancy> database ip address ↵
```

where *address* is the IPv6 address of the primary database

92

Configure the `peer-server` redundancy parameters in the following table, and then enter **`back`** ↵.

Table 17-24 Standby main server parameters — redundancy, peer-server

Parameter	Description
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 81. 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 81. 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

93

Enter the following:

```
<main configure redundancy> back ↵
```

The prompt changes to `<main configure>`.

94

Configure the `nspos` parameters in the following table, and then enter **`back`** ↵.

Table 17-25 Standby main server parameters — nspos

Parameter	Description
ip-list	The nspOS-server IP addresses, separated by a semicolon Specify only one IP address for a standalone NSP system. • If the NFM-P system is in a shared-mode NSP deployment specify the advertised address of each NSP cluster. • If the NSP system includes only the NFM-P, specify the main server private IP address. Default: —
address-to-nspos	The main server IP address that is reachable by the nspOS server Default: —
secure	Whether communication with the nspOS servers is secured using TLS Default: false
internal-certs	Whether internal certificates are used to secure nspOS communication between components; the parameter is configurable when the **secure** parameter is set to true. The parameter is deprecated, and must be set to the same value as the **secure** parameter. Default: false
dc-name	The nspOS DR data center name for aligning NSP components with the local NFM-P main server; must match the dcName value in the NSP configuration file The parameter is required only in a redundant deployment; however, in a shared-mode deployment, it is recommended that you configure the parameter, regardless of the NFM-P deployment type. Default: —

95

Configure the `remote-syslog` parameters in the following table, and then enter **`back`** ↵.

Table 17-26 Standby main server parameters — remote-syslog

Parameter	Description
enabled	Enable the forwarding of the NFM-P User Activity logs in syslog format to a remote server Default: disabled
syslog-host	Remote syslog server hostname or IP address Default: —
syslog-port	Remote server TCP port Default: —
ca-cert-path	Absolute local path of public CA TLS certificate copied from remote server

96

Configure the `server-logs-to-remote-syslog` parameters in the following table, and then enter **back** ↵.

Table 17-27 Standby main server parameters — server-logs-to-remote-syslog

Parameter	Description
enabled	Enable the forwarding of the NFM-P server logs in syslog format to a remote server Default: disabled
secured	Whether the communication with the remote server is TLS-secured Default: disabled
syslog-host	Remote syslog server hostname or IP address Default: —
syslog-port	Remote server TCP port Default: —
ca-cert-path	Absolute local path of public CA TLS certificate copied from remote server

97

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 14.9 “NFM-P samconfig utility” (p. 432) 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>`.

98

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

99

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Enable Windows Active Directory access

100

If you use Windows Active Directory for single-sign-on client access to the NFM-P, open the following file with a plain-text editor such as vi:

/opt/nsp/os/install/config.json

Otherwise, go to Step 106.

101

Change the IPv4 addresses to IPv6 addresses, as required.

102

Save and close the file.

103

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

104

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

105

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Configure reserved auxiliary servers

106

If the NFM-P system does not include auxiliary servers, go to Step 120. Otherwise, perform Step 107 to Step 118 on each reserved auxiliary server station.

107

Log in as the root user.

108

Enter the following:

```
# samconfig -m aux ↵
```

The following is displayed:

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

109

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>`.

110

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>`.

111

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

112

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>`.

113

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

114

Configure the `tls` parameters in the following table, and then enter **back** ↵.

Table 17-28 Auxiliary server parameters — tls

Parameter	Description
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
pki-server	The PKI server IP address or hostname Default: —
pki-server-port	The TCP port on which the PKI server listens for and services requests Default: 2391

115

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

116

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 14.9 “NFM-P samconfig utility” (p. 432) 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>`.

117

Enter the following:

```
<aux> apply ↵
```

The configuration is applied.

118

Enter the following:

```
<aux> exit ↵
```

The samconfig utility closes.

Start reserved auxiliary servers

119

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

120

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:

   ```
   # systemctl enable nfmp-main.service ↵
   ```

Start standby main server

121

Start the standby 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.

122

If Windows Active Directory access is configured to use the AUTHENTICATED type of LDAP server, and the NFM-P is not part of a shared-mode NSP deployment, enter the following to restart the local nspos-tomcat service:

Note: The service restart may take a few minutes, during which NFM-P GUI and REST client access is degraded. General NFM-P operation is unaffected.

```
# systemctl restart nspos-tomcat ↵
```

Verify converted system using GUI client

123

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.

End of steps

NFM-P system conversion to redundancy

17.9 Converting an NFM-P system to redundancy

17.9.1 Introduction

CAUTION

Service Disruption

An NFM-P system conversion to redundancy 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 Planning Guide, and the NSP 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 NSP professional services 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.

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.

This section describes the conversion of a standalone NFM-P system to a redundant NFM-P system.

You require an NFM-P license file for the new standby main server, or an updated license file that includes the standby main server information. Contact technical support for information about obtaining or updating an NFM-P license.

The NFM-P samconfig utility is used for component configuration and deployment. See 14.9 “NFM-P samconfig utility” (p. 432) for information about the samconfig utility.

Note: It is strongly recommended that you verify the GPG signature of each RPM file that you download from Nokia to ensure that each file has a valid Nokia signature.

Note: It is strongly recommended that you verify the message digest of each NSP image file or software bundle that you download from the Nokia Support portal. The download page includes the MD5, SHA256, and SHA512 checksums for comparison with the output of the RHEL md5sum, sha256sum, or sha512sum command. See the associated RHEL man page for command usage information.

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

17.9.2 Redundancy conversion requirements

The following must be true before you attempt a system conversion to redundancy.

- 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 and functional; an upgraded main server performs crucial upgrade-specific tasks during startup.
- Each component in the standalone NFM-P system is operational.

17.9.3 Redundancy conversion restrictions

An NFM-P system conversion to redundancy is not supported during a system upgrade.

17.9.4 TLS considerations

The following options are available for implementing TLS on the new redundant system components:

- **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.

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 NSP cluster
- public IP address or hostname of each NFM-P main server

17.10 System conversion to redundancy workflow

17.10.1 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 17.11 “To convert a standalone NFM-P system to a redundant system” (p. 1028).

17.10.2 Stages

1

Configure TLS and firewalls, as required; see “Perform security preconfiguration” (p. 1029).

2

Back up the NFM-P configuration files; see “Back up configuration files” (p. 1029).

3

Download the required installation files; see “Download installation files” (p. 1030).

4

Gather the system information required for the conversion; see "Gather required information" (p. 1030).

5

Close the unrequired NFM-P client sessions; see "Close client sessions" (p. 1032).

6

Back up the main database; see "Back up database" (p. 1032).

7

Stop the main server; see "Stop main server" (p. 1033).

8

Convert the standalone database to a primary database; see "Convert standalone database to primary database" (p. 1034).

9

Convert the standalone server to a primary main server; see "Convert standalone main server to primary main server" (p. 1036).

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. 1042).

11

Install the standby database; see "Install standby database" (p. 1045).

12

Install the standby main server; see "Install standby main server" (p. 1049).

13

If required, enable Windows Active Directory for client access; see "Enable Windows Active Directory access" (p. 1062).

14

If required, configure ADFS to enable Common Access Card, or CAC, client access;; see "Enable CAC access" (p. 1064).

15

If required, configure WS-NOC integration with the NFM-P; see "Configure WS-NOC integration" (p. 1067).

16

Start the standby main server; see “Start standby main server” (p. 1068).

17

Reinstantiate the standby database; see “Reinstantiate standby database” (p. 1070).

18

Use an NFM-P GUI client to perform sanity testing on the newly redundant NFM-P system.

19

Configure and enable firewalls, if required; see “Configure and enable firewalls” (p. 1070).

17.11 To convert a standalone NFM-P system to a redundant system

17.11.1 Description

The following steps describe how to convert an NFM-P system in a standalone deployment to a redundant system. This involves 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 nsp 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, nsp
- 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 nsp 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.

17.11.2 Steps

Perform security preconfiguration

1

Start the PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 4.10 “To configure and enable a PKI server” (p. 113).

Note: The PKI server is required for internal system configuration purposes.

2

If you are using the manual TLS deployment method, generate and distribute the required TLS files for the system, as described in “NSP TLS configuration” (p. 108).

3

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 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 Planning Guide*, which describes using NFM-P templates for rule creation.

b. Disable each firewall; see the external firewall documentation, or perform 3.19 “To disable the RHEL firewalld service” (p. 91).

Back up configuration files

4

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.

Download installation files

5

Download the following NFM-P installation files for the installed release to an empty directory on a station that is not affected by the conversion activity:

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

Gather required information

6

Obtain the following information from the main server station and record it for use during the conversion:

- hostname, which is one of the following:
  - the hostname specified for the main server station during the previous NFM-P software installation or upgrade
  - the local hostname, if an IP address was specified for the main server station during the previous NFM-P software installation or upgrade
- IP addresses
  - IP address that the current and new main databases require to reach the main server
  - IP address that the NFM-P GUI and XML API clients require to reach the main server (public IP address, if NAT is used)
  - IP address that NFM-P auxiliary servers require to reach the main server
  - private IP address (if NAT is used)
- root user password

7

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

8

If the system includes one or more auxiliary servers, click on the Auxiliary Servers tab; otherwise, go to Step 10.

A list of auxiliary servers is displayed.

9

Perform the following steps for each auxiliary server listed on the form.

1. Select the auxiliary server and click Properties. The Auxiliary Server [Edit] form 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 [Edit] form.

10

If the NFM-P system includes one or more client delegate servers, perform the following steps. Otherwise, go to Step 12.

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.

11

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.

12

Close the System Information form, if it is open.

Close LogViewer utility

13

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

14

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.
2. Choose Administration→Security→NFM-P User Security from the main menu. The NFM-P User Security - Security Management (Edit) form opens.
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.
9. Close the NFM-P User Security - Security Management (Edit) form.

Back up database

15

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.

Back up the main database from the client GUI or a CLI; see the *NSP System Administrator Guide* for information.

Add hostname mappings

16

As the root user, update the /etc/hosts file on each standalone and new standby component station to include an entry for each peer component. See 13.9.3 “Management network configuration example” (p. 380) for a configuration example.

Stop main server

17

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.
6. Enter the following to switch to the root user:

   ```
   bash$ su ↵
   ```
7. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to display the nspOS service status:

   ```
   # nspdctl status ↵
   ```

   Information like the following is displayed.

   ```
   Mode:     standalone
   Role:     leader
   DC-Role:  active
   DC-Name:  dc_name
   ```

```
Registry: IP_address:port
State:    stopped
Uptime:   0s
SERVICE            STATUS
service_a          inactive
service_b          inactive
service_c          inactive
```

You must not proceed to the next step until all NSP services are stopped; if the State is not ‘stopped’, or the STATUS indicator of each listed service is not ‘inactive’, repeat this substep.

18

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:

   ```
   # systemctl disable nspos-nspd.service ↵
   ```

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

19

Log in to the standalone main database station as the root user.

20

Open a console window.

21

Enter the following:

```
# samconfig -m db ↵
```

The following is displayed:

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

22

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>`.

23

To enable IP validation, which restricts the server components that have access to the main database; configure the parameters in the following table, and then enter **`back`** ↵.

Note: For security reasons, it is strongly recommended that you enable IP validation.

Note: When you enable IP validation on an NFM-P system that includes auxiliary servers, NSP Flow Collectors, or NSP analytics servers, you must configure the `remote-servers` parameter; otherwise, the servers cannot reach the database.

Table 17-29 Primary database parameters — ip-validation

Parameter	Description
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: —

24

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 14.9 “NFM-P samconfig utility” (p. 432) 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>`.

25

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.
```

26

When the database conversion is complete, enter the following:

```
<db> exit ↵
```

The samconfig utility closes.

Convert standalone main server to primary main server

27

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

28

Open a console window.

29

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.

30

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

31

Enter the following:

```
<main> configure redundancy enabled ↵
```

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

32

Configure the general `redundancy` parameters in the following table.

Table 17-30 Primary main server parameters — redundancy

Parameter	Description
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

33

Configure the `database` redundancy parameters in the following table, and then enter **`back`** ↵.

Table 17-31 Primary main server parameters — redundancy, database

Parameter	Description
ip	The IP address that the primary main server must use to reach the standby database Default: —
instance	Standby database instance name Default: —
backup-sync	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 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

Table 17-31 Primary main server parameters — redundancy, database (continued)

Parameter	Description
alignment	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 *NSP System Administrator Guide*. Default: false
preferred-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: —
reinstantiation-delay	The delay, in minutes, between the completion of a database failover and the automatic reinstantiation of the standby database A value of 0 disables automatic database reinstantiation. Default: 60

34

Configure the `peer-server` redundancy parameters in the following table, and then enter **`back`** ↵.

Table 17-32 Primary main server parameters — redundancy, peer-server

Parameter	Description
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: —

Table 17-32 Primary main server parameters — redundancy, peer-server (continued)

Parameter	Description
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
ip-to-auxes	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: —
snmp-ipv4	The IPv4 address that the managed NEs must use to reach the standby main server
snmp-ipv6	The IPv6 address that the managed NEs must use to reach the standby main server
snmp-port	The TCP port on the standby main server station used for SNMP communication with the managed NEs Default: 162
traplog-id	The SNMP trap log ID associated with the standby main server Default: 98

35

Enter the following:

```
<main configure redundancy> back ↵
```

The prompt changes to `<main configure>`.

36

Configure the `nspos` parameters in the following table, and then enter **`back`** ↵.

Table 17-33 Standalone main server parameters — nspos

Parameter	Description
ip-list	The nspOS-server IP addresses, separated by a semicolon Specify only one IP address for a standalone NSP system. • If the NFM-P system is in a shared-mode NSP deployment specify the advertised address of each NSP cluster. • If the NSP system includes only the NFM-P, specify the main server private IP address. Default: —
address-to-nspos	The main server IP address that is reachable by the nspOS server Default: —
secure	Whether communication with the nspOS servers is secured using TLS It is strongly recommended to enable the parameter in an NFM-P-only deployment. Default: false
internal-certs	Whether internal certificates are used to secure nspOS communication between components; the parameter is configurable when the **secure** parameter is set to true. The parameter is deprecated, and must be set to the same value as the **secure** parameter. Default: false
dc-name	The nspOS DR data center name for aligning NSP components with the local NFM-P main server; must match the dcName value in the NSP configuration file The parameter is required only in a redundant deployment; however, in a shared-mode deployment, it is recommended that you configure the parameter, regardless of the NFM-P deployment type. Default: —

37

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 14.9 “NFM-P samconfig utility” (p. 432) 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>`.

38

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

39

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

40

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.

41

Close the console window.

Enable primary main server automatic startup

42

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

43

Log in as the root user on the standby main database station.

44

Perform one of the following.

Note: You must not download or install nsp-nfmp-nodeexporter unless the package is already installed on the existing standalone main server station or collocated station.

a. If the main server and database are to be collocated on one station, perform the following steps.

   1. Download the following installation files to an empty directory on the collocated 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
      - nsp-nfmp-nodeexporter-*R.r.p*-rel.*v*.rpm, if the NFM-P is in a shared-mode deployment and you want to forward NFM-P system metrics to the NSP
      - OracleSw_PreInstall.sh

      Note: In subsequent steps, the directory is called the NFM-P software directory.

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
   - nsp-nfmp-nodeexporter-*R.r.p*-rel.*v*.rpm, if the NFM-P is in a shared-mode deployment and you want to forward NFM-P system metrics to the NSP
   - OracleSw_PreInstall.sh

   Note: In subsequent steps, the directory is called the NFM-P software directory.

45

Open a console window.

46

Navigate to the directory that contains the OracleSw_PreInstall.sh file.

47

Enter the following:

```
# chmod +x OracleSw_PreInstall.sh ↵
```

48

⚠ **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 ↵
```

ℹ **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]:
```

49

Enter Yes. The following prompt is displayed:

```
Enter the Oracle dba group name [group]:
```

50

Enter a group name.

ℹ **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:
```

51

Enter a username.

ℹ **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/nsp/nfmp/oracle19].

Checking or Creating the Oracle user home directory
/opt/nsp/nfmp/oracle19...

Checking user username...

Adding username...

Changing ownership of the directory /opt/nsp/nfmp/oracle19 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:
```

52

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:
```

53

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]:
```

54

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
```

55

When the script execution is complete, enter the following to reboot the station:

```
# systemctl reboot ↵
```

The station reboots.

Install standby database

56

When the reboot is complete, log in as the root user on the standby main database station.

57

Open a console window.

58

Navigate to the NFM-P software directory.

Note: Ensure that the directory contains only the installation files.

59

Enter the following:

```
# chmod +x * ↵
```

60

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

61

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:
Running transaction check
```

```
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

62

Enter the following:

```
# samconfig -m db ↵
```

The following is displayed:

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

63

Enter the following:

```
<db> configure type standby ↵
```

The prompt changes to `<db configure>`.

64

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

65

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>`.

66

Enter the following, and then enter **`back`** ↵:

```
<db configure redundant> instance instance_name ↵
```

where *instance_name* is the primary database instance name

67

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 System Administrator Guide*.

Table 17-34 Standby database parameters — passwords

Parameter	Description
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

68

To enable IP validation, which restricts the server components that have access to the main database; configure the parameters in the following table, and then enter **`back`** ↵.

Note: For security reasons, it is strongly recommended that you enable IP validation.

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 17-35 Standby database parameters — ip-validation

Parameter	Description
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: —

69

To enable the forwarding of NFM-P system metrics to the NSP; configure the parameters in the following table, and then enter **`back`** ↵.

Note: The parameters are required only for a distributed main database, so are not shown or configurable if the main server and database are collocated.

Table 17-36 Standby database parameters — tls

Parameter	Description
keystore-pass	The TLS keystore password Default: available from technical support
pki-server	The PKI server IP address or hostname You must configure the parameter. Default: —
pki-server-port	The TCP port on which the PKI server listens for and services requests Default: 2391

70

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 14.9 “NFM-P samconfig utility” (p. 432) 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>`.

71

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.
```

72

When the database creation is complete, enter the following:

```
<db> exit ↵
```

The samconfig utility closes.

73

Enter the following to reboot the standby main database station:

```
# systemctl reboot ↵
```

The station reboots.

Install standby main server

74

Log in as the root user on the standby main server station.

75

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 collocated 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, download the following files to an empty directory on the main server station:

Note: You must not download or install nsp-nfmp-nodeexporter unless the package is already installed on the existing standalone main server station or collocated 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
- nsp-nfmp-nodeexporter-*R.r.p*-rel.*v*.rpm, if the NFM-P is in a shared-mode deployment and currently forwards NFM-P system metrics to the NSP

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.

76

You must remove the semvalidator package if it is installed; otherwise, the upgrade is blocked.

Perform the following steps.

1. Enter the following:

```
# rpm -q nsp-nfmp-semvalidator ↵
```

If the package is installed, the following is displayed:

```
nsp-nfmp-semvalidator-version
```

If the package is not installed, the following is displayed:

```
package nsp-nfmp-semvalidator is not installed
```

2. If the package is installed, enter the following:

```
# dnf remove nsp-nfmp-semvalidator ↵
```

The package is removed.

77

Open a console window.

78

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 OS documentation for information about closing user sessions.

79

Navigate to the NFM-P software directory.

Note: Ensure that the directory contains only the installation files.

80

Enter the following:

```
# chmod +x * ↵
```

81

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

82

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading Packages:
```

```
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

The package installation is complete when the following is displayed:

```
Complete!
```

83

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 or auxiliary server on the station, change the nsp password.

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.

84

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

85

Enter the following:

```
<main> configure ↵
```

The prompt changes to `<main configure>`.

86

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 the *NSP System Administrator Guide*.

```
<main configure> license license_file ↵
```

where *license_file* is the path and file name of the NSP license bundle

87

Enter the following:

```
<main configure> redundancy enabled ↵
```

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

88

Configure the general `redundancy` parameters in the following table.

Table 17-37 Standby main server parameters — redundancy

Parameter	Description
ip-to-peer	The standby main server IP address that the primary main server must use for general communication Default: IP address of primary network interface
rsync-ip	The standby main server IP address that the primary main server must use for data synchronization Default: IP address of primary network interface

89

Configure the `database` redundancy parameters in the following table, and then enter **back** ↵.

Table 17-38 Standby main server parameters — redundancy, database

Parameter	Description
ip	The IP address that the standby main server must use to reach the primary database Default: —
instance	Primary database instance name Default: —

Table 17-38 Standby main server parameters — redundancy, database (continued)

Parameter	Description
backup-sync	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 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
alignment	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 *NSP System Administrator Guide*. Default: false
preferred-instance	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: —
reinstantiation-delay	The delay, in minutes, between the completion of a database failover and the automatic reinstantiation of the standby database A value of 0 disables automatic database reinstantiation. Default: 60

90

Configure the `peer-server` redundancy parameters in the following table, and then enter **`back`** ↵.

Table 17-39 Standby main server parameters — redundancy, peer-server

Parameter	Description
ip	The primary main server IP address that the standby main server uses for general communication Default: —

Table 17-39 Standby main server parameters — redundancy, peer-server (continued)

Parameter	Description
hostname	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: —
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

91

Enter the following:

```
<main configure redundancy> back ↵
```

The prompt changes to `<main configure>`.

92

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 17-40 Standby main server parameters — mediation

Parameter	Description
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

93

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 94.

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.

94

Configure the `tls` parameters in the following table, and then enter **`back`** ↵.

Table 17-41 Standby main server parameters — tls

Parameter	Description
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
alias	The alias specified during keystore generation You must configure the parameter. Default: —
pki-server	The PKI server IP address or hostname Default: —
pki-server-port	The TCP port on which the PKI server listens for and services requests Default: 2391
regenerate-certs	Whether to regenerate the internal TLS certificates Certificate regeneration is required when the current certificates are about to expire, or a new internal root certificate is available. A new internal root certificate is available when the root certificate is reset, or when the PKI server is run on a station other than the station used for the previous certificate deployment. Default: false
hsts-enabled	Whether HSTS browser security is enabled Default: false

95

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 17-42 Standby main server parameters — oss

Parameter	Description
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
xml-output	The directory in which to store the output of XML API file export operations Default: /opt/nsp/nfmp/server/xml_output

96

If the NFM-P includes an auxiliary database, configure the `auxdb` parameters in the following table, and then enter **`back`** ↵.

Table 17-43 Standby main server parameters — auxdb

Parameter	Description
enabled	Whether the auxiliary database is enabled in the main server configuration
secure	Whether TLS is enabled on the auxiliary database If TLS is enabled on the main server, you must set the parameter to true, and enable TLS during the auxiliary database installation. Default: false
ip-list	A list of the auxiliary database station IP addresses that are accessible to the main server, in the following format: **Note:** For a geo-redundant auxiliary database, the order of the IP addresses must be the same on each main server in the geo-redundant system. ***`cluster_1_IP1,cluster_1_IP2,cluster_1_IPn;cluster_2_IP1,cluster_2_IP2,cluster_2_IPn`*** ↵ where *cluster_1_IP1*, *cluster_1_IP2*,*cluster_1_IPn* are the external IP addresses of the auxiliary database stations in one data center *cluster_2_IP1*, *cluster_2_IP2*,*cluster_2_IPn* are the external IP addresses of the stations in the other data center; required only for geo-redundant auxiliary database Default: —
oam-test-results	Whether the auxiliary database is to store OAM test results Default: false

Table 17-43 Standby main server parameters — auxdb (continued)

Parameter	Description
redundancy-level	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 apply the main server configuration, you cannot modify the `redundancy-level` parameter. Default: 1

97

As required, configure the `aa-stats` parameters in the following table, and then enter **`back`** ↵.

Table 17-44 Standby main server parameters — aa-stats

Parameter	Description
enabled	Whether the NFM-P is to collect AA accounting statistics Default: false
formats	AA accounting statistics file formats; the options are the following: • ipdr—IPDR format • ram—format for NSP Analytics reporting • ipdr,ram—both formats The parameter is configurable when the enabled parameter is set to true. Default: ram
aux-db storage	Whether the NFM-P is to store the statistics in an auxiliary database The parameter is configurable when the enabled parameter is set to true. Default: false

98

Configure the `nspos` parameters in the following table, and then enter **`back`** ↵.

Table 17-45 Standby main server parameters — nspos

Parameter	Description
ip-list	The nspOS-server IP addresses, separated by a semicolon Specify only one IP address for a standalone NSP system. • If the NFM-P system is in a shared-mode NSP deployment specify the advertised address of each NSP cluster. • If the NSP system includes only the NFM-P, specify the main server private IP address. Default: —
address-to-nspos	The main server IP address that is reachable by the nspOS server Default: —
secure	Whether communication with the nspOS servers is secured using TLS It is strongly recommended to enable the parameter in an NFM-P-only deployment. Default: false
internal-certs	Whether internal certificates are used to secure nspOS communication between components; the parameter is configurable when the **secure** parameter is set to true. The parameter is deprecated, and must be set to the same value as the **secure** parameter. Default: false
dc-name	The nspOS DR data center name for aligning NSP components with the local NFM-P main server; must match the dcName value in the NSP configuration file The parameter is required only in a redundant deployment; however, in a shared-mode deployment, it is recommended that you configure the parameter, regardless of the NFM-P deployment type. Default: —
mtls-kafka-enabled	Specifies whether mTLS is enabled for Kafka communication with the NSP The parameter is displayed only: • if the ip-list parameter is set to a remote address • after the configuration is initially applied in a subsequent step **Note:** The parameter is configurable only if the **secure** and **internal-certs** parameters are set to true. **Note:** The function is supported only in an NSP system that uses separate interfaces for internal and client communication. Default: false

Table 17-45 Standby main server parameters — nspos (continued)

Parameter	Description
authMode	NSP authentication mode, which is one of the following: • oauth2—OAUTH2 user authentication • cas—CAS user authentication (deprecated) The parameter is configurable only in a shared-mode NSP deployment. The parameter setting must match the authMode setting in the NSP cluster configuration. Default: oauth2

99

Configure the `remote-syslog` parameters in the following table, and then enter **`back`** ↵.

Table 17-46 Standby main server parameters — remote-syslog

Parameter	Description
enabled	Enable the forwarding of the NFM-P User Activity logs in syslog format to a remote server Default: disabled
syslog-host	Remote syslog server hostname or IP address Default: —
syslog-port	Remote server TCP port Default: —
ca-cert-path	Absolute local path of public CA TLS certificate copied from remote server

100

Configure the `server-logs-to-remote-syslog` parameters in the following table, and then enter **`back`** ↵.

Table 17-47 Standby main server parameters — server-logs-to-remote-syslog

Parameter	Description
enabled	Enable the forwarding of the NFM-P server logs in syslog format to a remote server Default: disabled
secured	Whether the communication with the remote server is TLS-secured Default: disabled

Table 17-47 Standby main server parameters — server-logs-to-remote-syslog (continued)

Parameter	Description
syslog-host	Remote syslog server hostname or IP address Default: —
syslog-port	Remote server TCP port Default: —
ca-cert-path	Absolute local path of public CA TLS certificate copied from remote server

101

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 14.9 “NFM-P samconfig utility” (p. 432) 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>`.

102

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

103

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

104

If the NFM-P is part of a shared-mode NSP system and you want to enable mTLS for internal Kafka authentication using two-way TLS, perform the following steps.

Note: Enabling mTLS for internal Kafka authentication is supported only in an NSP deployment that uses separate interfaces for internal and client communication.

Note: The parameter you must configure is displayed only if the ip-list parameter is set to a remote address.

Note: The parameter is configurable only if the **secure** and **internal-certs** parameters in the **nspos** section are set to true.

1. Enter the following:

   ```
   # samconfig -m main ↵
   ```

   The following is displayed:

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

2. Enter the following:

   ```
   # configure nspos mtls-kafka-enabled back ↵
   ```

3. Enter the following:

   ```
   <main> apply ↵
   ```

   The configuration is applied.

4. Enter the following:

   ```
   <main> exit ↵
   ```

   The samconfig utility closes.

Enable Windows Active Directory access

105

If you intend to use Windows Active Directory, or AD, for single-sign-on client access, you must configure LDAP remote authentication for AD; otherwise, go to Step 124.

Open the following file as a reference for use in subsequent steps:

/opt/nsp/os/install/examples/config.yml

Note: Consider the following.

- The NFM-P does not assign a default user group to users of a remote authentication source that you define for Windows AD; the authentication source must provide the user group attributes.
- Windows AD supports the following LDAP server types for remote authentication:

  AD—The user group of an AD user is derived from the group_base_dn attribute in the server configuration; group search filters are not supported.

  AUTHENTICATED—The server configuration must include bind credentials; group search filters are supported. After NFM-P initialization, you add the AD server bind credentials to the NSP password vault using the NSP Session Manager REST API.

106

Locate the section that begins with the following lines:

```
#   ldap:
#     enabled: true
#     servers:
```

```
#       - type: AUTHENTICATED/AD/ANONYMOUS
#         url: ldaps://ldap.example.com:636
#         security: SSL/STARTTLS/NONE
```

107

Open the following file using a plain-text editor such as vi:

/opt/nsp/os/install/config.json

108

Locate the section that begins with the following line:

```
"sso": {
```

The section has one subsection for each type of SSO access.

Note: You can enable multiple remote authentication methods such as LDAP and RADIUS in the config.json file, or by using the NFM-P GUI. Using the GUI also allows you to specify the order in which the methods are tried during login attempts; however, no ordering is applied to multiple methods enabled in the config.json file.

109

In the **sso** section, create an **ldap** subsection as shown below using the parameter names from the **ldap** section of config.yml and the required values for your configuration.

The following example shows the LDAP configuration for two AD servers:

```
"ldap": {
"enabled": true,
"servers": [
{
"type": "auth_type",
"url": "ldaps://server1:port",
"server1_parameter_1": "value",
"server1_parameter_2": "value",
.
.
"server1_parameter_n": "value",
},
{
"type": "auth_type",
"url": "ldaps://server2:port",
"server2_parameter_1": "value",
"server2_parameter_2": "value",
.
.
"server2_parameter_n": "value",
},
}]
```

```
}
```

where *auth_type* is AD or AUTHENTICATED

110

Save and close the files.

111

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

112

Enter the following:

```
<main> apply ↵
```

The AD LDAP configuration is applied.

113

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Enable CAC access

114

If you do not intend to enable Common Access Card, or CAC, technology for NFM-P client access, go to Step 124.

115

Download the federationmetadata.xml from the following ADFS link:

https://*ADFS_server_name*/FederationMetadata/2007-06/federationmetadata.xml

where *ADFS_server_name* is the ADFS server FQDN

116

Add an ADFS server entry to the /etc/hosts file on the main server.

1. Open the /etc/hosts file using a plain-text editor such as vi.
2. Add the following line below the line that contains the main server IP address:

   ```
   IP_address FQDN
   ```

   where

IP_address is the IP address of the ADFS server

FQDN is the FQDN of the ADFS server

3. Save and close the file.

117

In order to enable CAC for client access, you must configure Active Directory Federation Services, or ADFS.

Open the following file using a plain-text editor such as vi:

/opt/nsp/os/install/config.json

118

In the **sso** section, create an **saml2** subsection as shown below using the parameter names from the **saml2** section of config.yml and the required values for your configuration.

The following example shows the ADFS configuration.

Note: You must preserve the lead spacing of each line.

```
  "sso" : {
    "saml2": {
       "enabled": true,
       "service_provider_entity_id": "NFM-P_identifier",
       "service_provider_metadata_filename": "casmetadata.xml",
       "maximum_authentication_lifetime": 3600,
       "accepted_skew": 300,
       "destination_binding": "urn:oasis:names:tc:SAML:2.0:bindings:
HTTP-Redirect",
       "identity_provider_metadata_path": "ADFS_metadata_file",
       "authn_context_class_ref": "urn:oasis:names:tc:SAML:2.0:ac:
classes:TLSClient",
       "authn_context_comparison_type": "minimum",
       "name_id_policy_format": "urn:oasis:names:tc:SAML:1.1:
nameid-format:unspecified",
       "force_auth": true,
       "passive": false,
       "wants_assertions_signed": false,
       "wants_responses_signed": false,
       "all_signature_validation_disabled": false,
       "sign_service_provider_metadata": false,
       "principal_id_attribute": "UPN",
       "use_name_qualifier": false,
       "provider_name": "ADFS_server_URI",
       "requested_attributes": [{
         "name": "http://schemas.xmlsoap.
org/ws/2005/05/identity/claims/emailaddress",
          "friendly_name": "E-Mail Address",
          "name_format": "urn:oasis:names:tc:SAML:2.0:attrname-format:
uri",
          "required": false
      } ],
       "mapped_attributes": [{
           "name": "http://schemas.xmlsoap.org/claims/Group",
           "mapped_to": "authorizationProfile"
      }, {
           "name": "http://schemas.xmlsoap.
org/ws/2005/05/identity/claims/upn",
           "mapped_to": "upn"
      } ]
    },
```

119

Configure the following parameters; leave all other parameters at the default:

- "service_provider_entity_id": "*NFM-P_identifier*"
- "identity_provider_metadata_path": "*ADFS_metadata_file*"
- "provider_name": "*ADFS_server_name*"

NFM-P_identifier is the unique ADFS Relying Trust Party identifier

*ADFS_metadata_fil*e is the absolute path of the ADFS metadata XML file, for example, /opt/federationmetadata.xml

ADFS_server_name is the ADFS server FQDN

120

Save and close the files.

121

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

122

Enter the following:

```
<main> apply ↵
```

The ADFS configuration is applied.

123

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Configure WS-NOC integration

124

If the NFM-P is integrated with a WS-NOC system, open the following file with a plain-text editor such as vi:

/opt/nsp/os/install/examples/config.json

Otherwise, go to Step 134.

125

Copy the following section:

```
  "nfmt": {
    "primary_ip": "",
    "standby_ip": "",
    "username": "",
    "password": "",
    "cert_provided": false
  },
```

126

Close the file.

127

Open the following file with a plain-text editor such as vi:

/opt/nsp/os/install/config.json

128

Paste in the copied section.

129

Configure the required parameters to enable the WS-NOC integration:

- primary_ip—the primary WS-NOC server IP address
- standby_ip—the standby WS-NOC server IP address
- username—the username required for WS-NOC access
- password—the password required for WS-NOC access
- cert_provided—whether a TLS certificate is used

130

Save and close the file.

131

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

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

132

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

133

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

Start standby main server

134

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 the *NSP 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.

135

Define the memory requirement for GUI clients based on the type of network that the NFM-P is to manage.

1. Enter the following:

   ```
   bash$ ./nmsdeploytool.bash clientmem -option ↵
   ```

   where *option* is one of the following:
   - m—medium, for management of limited-scale network
   - l—large, for a network of 15 000 or more NEs
2. Enter the following to commit the configuration change:

   ```
   bash$ ./nmsdeploytool.bash deploy ↵
   ```

136

If you have enabled CAC for NFM-P client access, download the casmetadata.xml file from the following URL, and then import the file into the ADFS server relying-trust-party:

https://*server*/cas/sp/metadata

where *server* is the main server IP address or hostname

After the download, the casmetadata.xml file is available in the following directory on the main server:

/opt/nsp/os/tomcat/conf/cas/saml

137

If you have enabled Windows Active Directory access using the AUTHENTICATED type of LDAP server, perform the following steps.

1. Use the NSP Session Manager REST API to add the LDAP server bind credentials; see the Network Developer Portal for information.
2. If the NFM-P is not part of a shared-mode NSP deployment, enter the following to restart the local nspos-tomcat service:

   Note: The service restart may take a few minutes, during which NFM-P GUI and REST client access is degraded. General NFM-P operation is unaffected.

   ```
   # systemctl restart nspos-tomcat ↵
   ```

138

If the NFM-P system includes one or more NSP Flow Collectors, configure the standby main server parameters and other redundancy parameters, as required; see the NSP documentation for information.

139

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

140

Open an NFM-P GUI client as the admin user.

141

Choose Administration→System Information from the main menu. The System Information form opens.

142

Click Re-Instantiate Standby.

143

Click Yes to confirm the action. The reinstantiation begins, and the GUI status bar displays reinstantiation information.

> **Note:** Database reinstantiation 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.

144

When the reinstantiation is complete, close the System Information form.

145

Use an NFM-P GUI client to perform sanity testing of the newly redundant system.

Configure and enable firewalls

146

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 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 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

18 NSP component integration

18.1 Integrating NSP components

18.1.1 Component integration support

This chapter describes the integration of NSP components deployed outside an NSP cluster . See the NSP compatibility matrix in the *NSP Release Notice* to ensure that the proposed integration results in a supported configuration.

18.2 To integrate IP-optical coordination and path simulation

18.2.1 Purpose

You can enable cross-launch between NSP's IP-optical coordination function and NSP's path simulation function. See the *NSP IP-Optical Coordination Guide* for information.

18.3 To add a WS-RC controller to IP-optical coordination

Note: *release-ID* in a file path has the following format:
R.r.p-rel.*version*
where
R.r.p is the NSP release, in the form *MAJOR.minor.patch*
version is a numeric value

18.3.1 Steps

1

Extract md-adaptor-suite-x.x.x-rel.x.zip.

2

Extract tapi-x.x.x-rel.x.zip.

3

Enter the following:

```
#
/opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/mdm/bin/adaptor-suite.bas
--install tapi-x.x.x-rel.x.zip ↲
```

The T-API adaptor is installed.

4

When the package is installed, log in to the Karaf console as the nsp user.

5

Enter the following to verify that the adaptor is started:

```
# /opt/nsp/mediation/bin/mdmserver.bash console ↵
```

6

Add the WS-RC controller to the NSP cluster from the NSP's IP-optical coordination views. See the *NSP IP-Optical Coordination Guide* for information.

END OF STEPS

19 NSP component uninstallation

19.1 Overview

19.1.1 Purpose

This chapter describes how to uninstall the NSP software from system components that are hosted outside the NSP cluster.

19.1.2 Contents

Uninstalling supplementary system components

19.2 To uninstall an NSP analytics server

19.2.1 Purpose

Perform this procedure to remove the NSP analytics server software from a station.

Note: You require root and nsp user privileges on the 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

19.2.2 Steps

1

Log in to the analytics server station as the nsp user.

2

Open a console window.

3

Enter the following:

```
bash$ /opt/nsp/analytics/bin/AnalyticsAdmin.sh uninstall ↵
```

The script displays the following message and prompt:

```
THIS ACTION WILL ERASE Analytics Application INSTALLATION
Please type 'YES' to continue
```

4

Enter YES.

The analytics server software uninstallation begins, and messages like the following are displayed:

```
Stopping Analytics Application
Dropping Existing Analytics Schema
```

The uninstallation is complete when the following is displayed:

```
Analytics Application has been uninstalled
```

5

Enter the following to switch to the root user:

```
bash$ su - ↵
```

6

Enter the following:

```
# dnf erase nsp-analytics-server nspos-tomcat nspos-jre ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Remove 3 Packages
Installed size: n.n G
Is this ok [y/N]:
```

7

Enter y ↵. The following and other progress messages are displayed:

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
```

When the removal of all packages is complete, the following is displayed:

```
Complete!
```

8

When all packages are removed, enter the following to reboot the station:

```
# systemctl reboot ↵
```

The station reboots.

9

Remove the /opt/nsp/analytics directory and contents.

10

Close the console window.

END OF STEPS

19.3 To uninstall NSP Flow Collectors

19.3.1 Purpose

Perform this procedure to remove the NSP Flow Collector software from one or more stations.

An NSP Flow Collector uninstallation backs up the component configuration files in the /opt/nsp/backup_flow directory on the station. A subsequent NSP Flow Collector installation on the station automatically reloads the saved configuration files. If you do not want the previous configuration restored during a subsequent installation, you must delete the /opt/nsp/backup_flow directory before the installation.

Note: You require the following user privileges:

- on the station that hosts the NSP installer software—root
- on each NSP Flow Collector 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

CAUTION

System degradation

On a station that has a collocated NSP Flow Collector and Flow Collector Controller, uninstalling the Flow Collector also uninstalls the Flow Collector Controller, which affects all Flow Collectors that it controls.

Before you attempt to uninstall an NSP Flow Collector that is collocated with a Flow Collector Controller, ensure that you fully understand the consequences.

19.3.2 Steps

1

Perform Step 3 and Step 4 on each NSP Flow Collector station.

2

Go to Step 5.

3

Log in as the nsp user.

4

Perform one of the following to stop the NSP Flow Collector.

Note: If an NSP Flow Collector Controller is also installed on the station, the Flow Collector Controller stops automatically.

a. If the NSP Flow Collector is collocated on a station with an NSP Flow Collector Controller, enter the following:

```
bash$ /opt/nsp/flow/fcc/bin/flowCollectorController.bash stop ↵
```

The command displays a series of status messages as the NSP Flow Collector and Flow Collector Controller stop.

b. If the NSP Flow Collector is on a dedicated station, enter the following:

```
bash$ /opt/nsp/flow/fc/bin/flowCollector.bash stop ↵
```

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

5

Log in as the root user on a station that has the downloaded and extracted NSP component installer package (NSP_NSD_NRC_*R_r*.tar.gz).

6

Open a console window.

7

Enter the following:

```
# cd path/NSD_NRC_R_r/bin ↵
```

where

path is the directory path of the NSP component installer package

R_r is the NSP software release, in the form *MAJOR_minor*

8

Enter the following:

```
# ./uninstall.sh --ask-pass --target address_1,address_2,...address_n
↵
```

where *address_1, address_2,...address_n* is a comma-separated list of the NSP Flow Collector station IP addresses

You are prompted for the common root password of the stations.

9

Enter the password.

The NSP Flow Collector software is removed from each station.

10

Remove the /opt/nsp/flow directory and contents from each station.

11

Close the console window.

END OF STEPS

19.4 To uninstall NSP Flow Collector Controllers

19.4.1 Purpose

Perform this procedure to remove the NSP Flow Collector Controller software from one or more stations.

An NSP Flow Collector Controller uninstallation backs up the component configuration files in the /opt/nsp/backup_flow directory on the station. A subsequent NSP Flow Collector Controller installation on the station automatically reloads the saved configuration files. If you do not want the previous configuration restored during a subsequent installation, you must delete the /opt/nsp/backup_flow directory before the installation.

Note: If an NSP Flow Collector Controller is collocated on a station with an NSP Flow Collector, uninstalling the Flow Collector Controller also uninstalls the Flow Collector.

Note: You require the following user privileges:

- on the station that hosts the NSP installer software—root
- on each NSP Flow Collector Controller 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

CAUTION

System degradation

Uninstalling an NSP Flow Collector Controller affects all NSP Flow Collectors associated with the Controller.

Before you attempt to uninstall an NSP Flow Collector Controller, ensure that you fully understand the consequences.

19.4.2 Steps

1

Perform Step 3 and Step 4 on each NSP Flow Collector Controller station.

2

Go to Step 5.

3

Log in as the nsp user on the NSP Flow Collector Controller station.

4

Enter the following to stop the NSP Flow Collector Controller:

> **Note:** If an NSP Flow Collector is also installed on the station, the Flow Collector stops automatically.

```
bash$ /opt/nsp/flow/fcc/bin/flowCollectorController.bash stop ↵
```

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

5

Log in as the root user on a station that has the downloaded and extracted NSP component installer package.

6

Open a console window.

7

Enter the following:

```
# cd path/NSD_NRC_R_r/bin ↵
```

where

path is the directory path of the NSP component installer package

R_r is the NSP software release, in the form *MAJOR_minor*

8

Enter the following:

```
# ./uninstall.sh --ask-pass --target address_1,address_2,...address_n
↵
```

where *address_1, address_2,...address_n* is a comma-separated list of the NSP Flow Collector Controller station IP addresses

You are prompted for the common root password of the stations.

9

Enter the password.

The NSP Flow Collector Controller software is removed from each station.

10

Remove the /opt/nsp/flow directory and contents from each station.

11

Close the console window.

END OF STEPS

Uninstalling the NFM-P

19.5 NFM-P system uninstallation workflow

19.5.1 Description

The following is the sequence of high-level actions required to completely uninstall a standalone or redundant NFM-P system.

As required for maintenance, you can also install one or more components individually, under the guidance of technical support.

19.5.2 Stages

1

Uninstall the single-user GUI clients; see 19.6 “To uninstall a single-user GUI client” (p. 1082).

2

Uninstall the client delegate servers; see 19.7 “To uninstall a client delegate server” (p. 1083).

3

If the system includes one or more auxiliary servers, perform 19.8 “To uninstall an auxiliary server” (p. 1084) for each auxiliary server.

4

If the system includes an auxiliary database, perform 19.9 “To uninstall an auxiliary database” (p. 1086).

5

Perform one of the following to uninstall each main server and main database:

a. If the main server and database are collocated, perform 19.10 “To uninstall a collocated main server and database” (p. 1088) on each collocated main server and database station.

b. If the main server and database are distributed on separate stations, perform 19.11 “To uninstall a distributed main server or main database” (p. 1090) on each main server station, and on each main database station.

19.6 To uninstall a single-user GUI client

19.6.1 Purpose

The following steps describe how to remove the single-user GUI client software from a station.

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

19.6.2 Steps

1

Log in to the client station.

2

Close the client GUI, if it is open.

3

For a Windows client, open the Windows Control Panel or Settings applet, select the NFM-P Client version *R.r* and click Uninstall. Click Yes or OK, as required, to acknowledge any confirmation or security prompts that are displayed.

The client software is uninstalled.

4

For a RHEL client, delete the client installation directory.

Note: The client installation does not create or modify any files other than the files in the installation directory.

5

For a Mac OS client, drag the package icon to the trash.

6

Remove any files that remain in the client installation directory of a Windows or Mac OS client.

END OF STEPS

19.7 To uninstall a client delegate server

19.7.1 Purpose

The following steps describe how to remove the client delegate server software.

Note: If you are not the original installer of the client delegate server, you require the following user privileges on the client delegate server station:

- Microsoft Windows—local Administrator
- RHEL—root

19.7.2 Steps

1

Log in to the client delegate server station.

2

Close the local client GUI, if it is open.

3

To uninstall a Windows client delegate server:

1. Open the Windows Control Panel or Settings applet.
2. Select NFM-P Client Delegate version *R.r*.
3. Click Uninstall.
4. Click Yes or OK, as required, to acknowledge any confirmation or security prompts that are displayed.

   The client software is uninstalled.

4

To uninstall a RHEL client delegate server, delete the client delegate server installation directory.

Note: The client delegate server installation does not create or modify any files other than the files in the installation directory.

5

Remove any files that remain in the installation directory of a Windows client delegate server.

End of steps

19.8 To uninstall an auxiliary server

19.8.1 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
- 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

19.8.2 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:

```
# dnf remove nsp-nfmp-aux-server ↵
# dnf remove nsp-nfmp-config ↵
# dnf remove nsp-nfmp-jre ↵
# dnf remove nsp-nfmp-semvalidator
```

After you enter a command, the dnf utility resolves any 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
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction check
Uninstalling the NFM-P package...
```

As each package removal completes, the following is displayed:

```
Complete!
```

5

Return to Step 4 as required to remove the next package in the sequence.

6

When all packages are removed, enter the following to reboot the auxiliary server station:

```
# systemctl reboot ↵
```

The station reboots.

7

Remove the /opt/nsp/nfmp/auxserver directory and contents.

END OF STEPS

19.9 To uninstall an auxiliary database

19.9.1 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.

19.9.2 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:

   ```
   # dnf erase nspos-auxdb nspos-jre ↵
   ```

   The dnf utility resolves any package dependencies and displays the following prompt:

   ```
   Remove 2 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.

END OF STEPS

19.10 To uninstall a collocated main server and database

19.10.1 Description

CAUTION

Service Disruption

The procedure requires that you stop the NFM-P main server and database software, which is service-affecting.

Perform the procedure only during a scheduled maintenance period.

The following steps describe how to remove the NFM-P main server and database software from the station on which they are collocated.

Note: You require root user privileges on the station.

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

Collocated component uninstallation in a redundant deployment

Before you attempt to uninstall a collocated main server and database in a redundant NFM-P deployment, you must ensure that the collocated main server and database roles, whether primary or standby, are aligned.

To avoid a server activity switch in a redundant deployment, you must perform the procedure on the standby cluster first.

If you need to uninstall only the primary main server and database, for example, to address a hardware problem, the components in the primary cluster must first assume the standby role. A role change may involve one or more server activity switch or database switchover operations, depending on whether automatic database realignment is enabled.

See “NSP component redundancy” in the *NSP System Administrator Guide* for information about the following:

- determining a component role
- automatic database realignment
- main server activity switches
- database switchovers

19.10.2 Steps

1

Log in to the collocated main server and database station as the root user.

2

Open a console window.

3

Back up any custom configuration files in the /opt/nsp/nfmp/server file path that you want to keep.

4

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]:
```

5

Enter Yes ↵.

The following, and uninstallation task messages, are displayed as the uninstaller stops the components and the uninstallation begins.

```
Stopping NFM-P Main Server...

Stopping NFM-P Main Database Proxy...

Stopping NFM-P Main Database...

Welcome to the NSP uninstaller

Verifying prerequisites...

Starting uninstall ...
```

When the uninstallation is complete, a line similar to the following is displayed:

```
PLAY RECAP
***************************************************************

*******

n.n.n.n                  : ok=nn   changed=n    unreachable=n
failed

=n    skipped=n    rescued=n    ignored=n
```

6

If the `failed=` value is not zero, one or more package removal operations has failed. Contact technical support for assistance, and provide any error messages that the uninstallation displays; do not proceed to the next step until recommended by technical support.

7

Enter the following to reboot the station:

```
# systemctl reboot ↵
```

The station reboots.

8

Remove the /opt/nsp/nfmp/server directory.

9

Remove the /opt/nsp/nfmp/oracle19 and database directories.

END OF STEPS

19.11 To uninstall a distributed main server or main database

19.11.1 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 main server or main database software that is installed on a station in a standalone or redundant NFM-P deployment.

Note: You require root user privileges on the station.

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

Distributed component uninstallation in a redundant deployment

To avoid a server activity switch in a redundant deployment, you must perform the procedure on the standby components first.

If you need to uninstall only the primary main server or database, for example, to address a hardware problem, the server or database must first assume the standby role. A role change may involve one or more server activity switch or database switchover operations, depending on whether automatic database realignment is enabled.

See “NSP component redundancy” in the *NSP System Administrator Guide* for information about the following:

- determining a component role
- automatic database realignment
- main server activity switches
- database switchovers

19.11.2 Steps

1

Log in to the station as the root user.

2

Open a console window.

3

If you are uninstalling a main server, perform the following steps.

1. Back up any custom configuration files in the /opt/nsp/nfmp/server file path that you want to keep.
2. Enter the following:

   ```
   # /opt/nsp/Uninstaller/uninstall.sh ↵
   ```

   The following is displayed:

   ```
   WARNING: This will remove all the nsp software from the system. The
   nsp user will NOT be removed.
   ```

   The following prompt is displayed:

   ```
   Do you want to continue? [Yes/No]:
   ```

3. Enter Yes ↵.

   The following, and uninstallation task messages, are displayed as the uninstallation begins.

   ```
   Stopping NFM-P Main Server...

   Welcome to the NSP uninstaller

   Verifying prerequisites...

   Starting uninstall ...
   ```

   When the uninstallation is complete, a line similar to the following is displayed:

   ```
   PLAY RECAP
   **************************************************************

   *******

   n.n.n.n                  : ok=nn   changed=n    unreachable=n
   failed

   =n    skipped=n    rescued=n    ignored=n
   ```

4. If the `failed=` value is not zero, one or more package removal operations has failed.

Contact technical support for assistance, and provide any error messages that the uninstallation displays; do not proceed to the next step until recommended by technical support.

4

If you are uninstalling a main database, perform the following steps.

1. Copy and paste, or enter the following commands in sequence:

   ```
   dnf remove nsp-nfmp-main-db
   dnf remove nsp-nfmp-oracle
   dnf remove nsp-nfmp-config
   dnf remove nsp-nfmp-jre
   dnf remove nsp-nfmp-semvalidator
   ```

   The following prompt is displayed for each package:

   ```
   Do you want to continue? [Yes/No]:
   ```

2. Enter y. The following is displayed:

   ```
   Downloading Packages:
   Running transaction check
   Transaction check succeeded.
   Running transaction test
   Transaction test succeeded.
   Running transaction check
   Uninstalling the NFM-P package...
   ```

   As each package removal completes, the following is displayed:

   ```
   Complete!
   ```

3. Repeat substep 2 as required to remove the next package in the sequence.

5

Enter the following to reboot the station:

```
# systemctl reboot ↵
```

The station reboots.

6

If you are uninstalling a main server, remove the /opt/nsp/nfmp/server directory.

7

If you are uninstalling a main database, remove the /opt/nsp/nfmp/oracle19 and database directories.

End of steps

A Removing world permissions from compiler executables

A.1 Resetting GCC-compiler file permissions

A.1.1 Description

This appendix describes the post-deployment configuration of specific file permissions for additional NSP system security.

Read and execute privileges for the “other” user type may be enabled on specific RPM files during RHEL OS installation, upgrade, or update.

As a security-hardening measure after such a RHEL OS operation, you can revoke the privileges, as described in A.2 “To remove world permissions from compiler executables” (p. 1093).

In the event that you need to roll back the security hardening, see A.3 “To restore compiler world permissions” (p. 1094).

A.2 To remove world permissions from compiler executables

A.2.1 Purpose

Perform this procedure to clear the “other” user permissions on specific GCC-compiler files on an NSP component station.

Note: It is recommended that you perform the procedure only during a scheduled maintenance period.

Note: You require root user privileges on the station.

A.2.2 Steps

1

Log in to the NSP component station as the root user.

2

Open a console window.

3

Paste the following command block into the console window:

```
chmod 750 /usr/bin/c89
chmod 750 /usr/bin/c99
chmod 750 /usr/bin/cc
chmod 750 /usr/bin/f95
chmod 750 /usr/bin/gcc
chmod 750 /usr/bin/gcc-ar
chmod 750 /usr/bin/gcc-nm
chmod 750 /usr/bin/gcc-ranlib
chmod 750 /usr/bin/gcov
chmod 750 /usr/bin/x86_64-redhat-linux-gcc
chmod 750 /usr/bin/c++
chmod 750 /usr/bin/g++
chmod 750 /usr/bin/x86_64-redhat-linux-c++
chmod 750 /usr/bin/x86_64-redhat-linux-g++
chmod 750 /usr/bin/gfortran
```

The file permissions are reset.

4

Close the console window.

END OF STEPS

A.3 To restore compiler world permissions

A.3.1 Purpose

Perform this procedure to restore the original file permissions reset by performing A.2 “To remove world permissions from compiler executables” (p. 1093) on an NSP component station.

Note: It is recommended that you perform the procedure only during a scheduled maintenance period.

Note: You require root user privileges on the station.

A.3.2 Steps

1

Log in to the station as the root user.

2

Open a console window.

3

Paste the following command block into the console window:

```
chmod 755 /usr/bin/c89
chmod 755 /usr/bin/c99
chmod 755 /usr/bin/cc
chmod 755 /usr/bin/f95
chmod 755 /usr/bin/gcc
chmod 755 /usr/bin/gcc-ar
chmod 755 /usr/bin/gcc-nm
chmod 755 /usr/bin/gcc-ranlib
chmod 755 /usr/bin/gcov
chmod 755 /usr/bin/x86_64-redhat-linux-gcc
chmod 755 /usr/bin/c++
chmod 755 /usr/bin/g++
chmod 755 /usr/bin/x86_64-redhat-linux-c++
chmod 755 /usr/bin/x86_64-redhat-linux-g++
chmod 755 /usr/bin/gfortran
```

The original file permissions are restored.

4

Close the console window.

END OF STEPS

B NSP Single Sign-On configuration examples

LDAPS configuration examples

B.1 Configuring LDAPS or secure AD

B.1.1 Introduction

The NSP configuration examples in the following topics show typical parameter settings for enabling secure LDAP (LDAPS) and secure AD, which uses LDAP lookup criteria, for user authentication. Examples for NSP OAUTH2 and CAS user authentication modes are provided.

Note: Each configuration is an example only; you must customize the parameters in an example using the values specific to your LDAP server deployment.

B.2 LDAPS configuration for OAUTH2 mode

B.2.1 Description

Example LDAPS parameters for NSP OAUTH2 mode are shown below.

```
ldap:
  enabled: true
  servers:
    - type: "AUTHENTICATED"
      name: "Ldap Server 1"
      url: "ldaps://ldap.company.com:636"
      priority: 0
      usernameLdapAttribute: "uid"
      rdnLdapAttribute: "cn"
      uuidLdapAttribue: "uid"
      userObjectClasses: "person,organizationalPerson,user"
      customUserLdapFilter: ""
      searchScope: 2
      security: "SSL"
      timeout: 5000
      userDn: "ou=People,dc=company,dc=com"
      userFilter: ""
      groupDn: "ou=Group,dc=company,dc=com"
      groupNameLdapAttribute: "cn"
      groupsLdapFilter: ""
      groupObjectClasses: "posixGroup"
      groupMembershipLdapAttribute: "memberUid"
      groupMembershipUserLdapAttribute: "cn"
      groupMemberOfLdapAttribute: "memberOf"
      bind:
        dn: "cn=Manager,dc=company,dc=com"
        credential: "password"
      minPoolSize: 0
      maxPoolSize: 10
```

B.3 Secure AD configuration for OAUTH2 mode

B.3.1 Description

Example secure AD parameters for NSP OAUTH2 mode are shown below.

```
ldap:
  enabled: true
  servers:
    - type: "AD"
      name: "Ldap Server 2"
      url: "ldaps://our-AD-servername:636"
      priority: 5
      usernameLdapAttribute: "cn"
      rdnLdapAttribute: "cn"
      uuidLdapAttribute: "cn"
      userObjectClasses: "person,organizationalPerson,user"
      customUserLdapFilter: ""
      searchScope: 2
      security: "SSL"
      timeout: 5000
      userDn: "cn=myserver,dc=mycompany,dc=com"
      userFilter: ""
      groupDn: "cn=groups,cn=myserver,dc=mycompany,dc=com"
      groupNameLdapAttribute: "cn"
      groupObjectClasses: "group"
      groupObjectClasses: "group"
      groupMembershipLdapAttribute: "member"
      groupMembershipUserLdapAttribute: "cn"
      groupMemberOfLdapAttribute: "memberOf"
      bind:
        dn: "cn=manager,cn=myserver,dc=mycompany,dc=com"
        credential: "password"
      minPoolSize: 0
      maxPoolSize: 10
```

B.4 LDAPS configuration for CAS mode

B.4.1 Description

Example LDAPS parameters for NSP CAS mode are shown below.

```
sso:
  ldap:
    enabled: true
    servers:
      - type: AUTHENTICATED
        url: ldaps://ldap.company.com:636
        security: SSL
        timeout: 5
        userBaseDn: ou=People,dc=company,dc=com
        userFilter: uid={user}
        groupBaseDn: ou=Group,dc=company,dc=com
        groupSearch:
          filter: (memberUid={1})
          attributeId: cn
        bind:
          dn: cn=Manager,dc=company,dc=com
          credential: "password"
        minPoolSize: 0
```

```
maxPoolSize: 10
useEntryResolver: true
```

B.5 Secure AD configuration for CAS mode

B.5.1 Description

Example secure AD parameters for NSP CAS mode are shown below.

```
sso:
ldap:
   enabled: true
   servers:
     - type: "AD"
       url: "ldaps://AD-servername:636"
       security: "SSL"
       timeout: 7
       userBaseDn: "cn=myserver,dc=mycompany,dc=com"
       userFilter: "cn={user}"
       dnFormat: "cn=%s,cn=myserver,dc=mycompany,dc=com"
       groupBaseDn: "cn=groups,cn=myserver,dc=mycompany,dc=com"
       useEntryResolver: true
```

RADIUS configuration examples

B.6 Configuring RADIUS authentication

B.6.1 Introduction

The NSP configuration examples in the following topics show typical parameter settings for enabling RADIUS user authentication. Examples for NSP OAUTH2 and CAS user authentication modes are provided.

Note: Each configuration is an example only; you must customize the parameters in an example using the values specific to your RADIUS server deployment.

B.7 RADIUS configuration for OAUTH2 mode

B.7.1 Description

Example RADIUS parameters for NSP OAUTH2 mode are shown below.

```
radius:
  enabled: true
  address: "203.0.113.34:1812"
  secret: "secret"
  protocol: "PAP"
  retries: 2
  timeout: 5000
  vendorId: "vendor_ID"
  roleVsaId: "VSA_ID"
  nasId: ""
  nasIp: ""
  nasIpv6: ""
```

B.8 RADIUS configuration for CAS mode

B.8.1 Description

Example RADIUS parameters for NSP CAS mode are shown below.

```
radius:
  enabled: true
  address: "203.0.113.37,radius.example.com”
  secret: "secret1,secret2"
```

```
protocol: "PAP"
retries: 2
timeout: 3
failoverOnException: true
failoverOnRejection: true
authenticationPort: 1812
vendorId: "vendor_ID"
roleVSAId: "VSA_ID"
mfa: false
```

TACACS+ configuration examples

B.9 Configuring TACACS+ authentication

B.9.1 Introduction

The NSP configuration examples in the following topics show typical parameter settings for enabling TACACS+ user authentication. Examples for NSP OAUTH2 and CAS user authentication modes are provided.

Note: Each configuration is an example only; you must customize the parameters in an example using the values specific to your TACACS+ server deployment.

B.10 TACACS+ configuration for OAUTH2 mode

B.10.1 Description

Example TACACS+ parameters for NSP OAUTH2 mode are shown below.

```
tacacs:
  enabled: true
  address: "tacacs1.example.com,203.0.113.37:49"
  secret: "secret"
  protocol: "PAP"
  timeout: 7000
  defaultGroup: ""
  vsaEnabled: true
  roleVsaId: "VSA_search_role"
  vsaServiceId: "VSA_search_service"
```

B.11 TACACS+ configuration for CAS mode

B.11.1 Description

Example TACACS+ parameters for NSP CAS mode are shown below.

```
tacacs:
  enabled: true
  address: "tacacs1.example.com,135.121.2.99"
  secret: "secret1,secret2"
  protocol: "PAP"
  timeout: 5
```

```
failoverOnException: true

failoverOnRejection: true

authenticationPort: 49

defaultGroup: "default_user_group"

vsaEnabled: true

roleVsaId: "VSA_search_role"

vsaServiceId: "VSA_search_service"
```