NOKIA

NSP
Network Services Platform

Release 19.6

Deployment and Installation Guide

3HE-15135-AAAB-TQZZA

Issue 3

October 2019

Legal notice

Contents

About this document

Purpose

The *NSP Deployment and Installation Guide* describes the options and methods for deploying the Network Services Platform, or NSP.

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

Documentation feedback

Part I: Getting started

Overview

Purpose

This part of the *NSP Deployment and Installation Guide* defines essential NSP terms and concepts, provides a product description, and describes scaling guidelines and redundancy support.

Contents

1 NSP deployment overview

1.1 NSP terms and concepts

1.1.1 Module

NSP product software is licensed, versioned, and delivered in modules. The modules are the orderable commercial units that comprise the NSP product. An NSP system operator interacts with the NSP applications that are licensed for the purchased modules. See 1.2.2 “NSP modules” (p. 12) for a list of the available NSP modules.

1.1.2 Application

The NSP provides a suite of browser-based and traditional network management applications for network operators. Some applications are specific to modules, and are enabled in the module license. Other applications are common to multiple modules. All licensed browser-based applications are accessible from the NSP Launchpad.

Note: Some applications require the purchase of a premium license.

Localization

By default, the NSP applications are ONLY available in English.

The translation process of i18n properties will be handled by the region. Deployment of the i18n resources can be done at install time or as part of a re-configuration of the NSP modules. The region is responsible for keeping a copy of the localization files as they will not survive an upgrade.

Note: If there are existing localization files, they will NOT automatically be backed up during the NSP upgrade. Localization file must be backed up prior to NSP upgrade and should be redeployed after the upgrade.

1.1.3 Component

The components of an NSP system are the NSP modules, separate products, and ancillary devices or appliances that comprise an NSP deployment.

1.1.4 Shared-mode deployment

You can deploy an NSP module as an independent system, or in combination with other components to create a shared-mode deployment that expands the NSP network management capabilities.

1.1.5 Package

A package is a set of one or more installation files that you download and use to deploy a component. The purchase of a component grants the right to download the component package, install the package, and use the deployed applications that the component provides.

1.1.6 Station

A station is a processing entity that hosts one instance of an operating system. A station may be a discrete physical entity, or a hardware abstraction such as a virtual machine, or VM.

1.1.7 NSP server

An NSP server is a station that typically hosts one NSP module. An NSP deployment may require multiple NSP servers. For example, a redundant NSP system requires two NSP servers.

1.2 NSP system components

1.2.1 Common nspOS resource base

The nspOS is a set of platform services that is used and required by each NSP component. The nspOS provides system-wide functions such as single sign-on, or SSO, application cross-launch, and operator access via the NSP Launchpad.

Each NSP module includes the nspOS, as does the NFM-T product. In a shared-mode NSP deployment, the nspOS runs on an NSD and NRC host station. In an NSP deployment that does not include the NSD and NRC, a server in a component system such as the NFM-P or NFM-T hosts the nspOS.

Only one nspOS instance is active at any time. For example, in a redundant NSP deployment that includes the NSD and NRC, the active nspOS instance runs on the primary NSD and NRC server.

When an independent system is converted to a shared-mode deployment, the nspOS instance in the independent system remains, but is no longer active; instead, the active nspOS instance runs on the standalone or primary NSD and NRC server.

The nspOS services and functions include the following:

- **Login**—grants SSO access to all NSP applications, GUI clients, and other resources on the NSP Launchpad
- **NSP Launchpad**—entry point for all NSP applications
- **Central Authentication Server, or CAS**—authenticates user login attempts
- **Session Manager**—tracks and manages SSO sessions
- **REST API Gateway**—acquires NSP REST API tokens and locates specific NSP APIs
- **NSP PKI Server**—generates TLS certificates for system-wide NSP deployment

The nspOS also contains a service registry, distributed streaming platform, and graph database.

1.2.2 NSP modules

The following table lists and describes each NSP module.

Table 1-1 NSP modules

Module	Expanded name	Functional domains
NFM-P	Network Functions Manager - Packet	• IP/MPLS network infrastructure management • IP/MPLS network and service assurance • Traditional L2 and L3 service management
NSD	Network Services Director	• SDN L2 and L3 service fulfilment • Assurance using service supervision • Model-driven mediation of Nokia and multi-vendor devices
NRC-P	Network Resource Controller - Packet	• IP/MPLS network optimization • IP/MPLS path computation • Flow steering based on statistics, analytics, and operator action
NRC-X	Network Resource Controller - Cross-domain	• IP/optical traffic correlation • Cross-domain link creation and discovery

1.2.3 Other NSP system components

An NSP system can include the following.

NFM-T

An NSP deployment that requires optical management functions must include the NFM-T product, which is an evolution of the former 1350 OMS product. The NFM-T provides end-to-end optical management functions that include service provisioning over multi-technology optical transport networks such as SDH/SONET, carrier Ethernet, WDM, ROADM, OTN, and packet. Browser-based fault management applications reduce the time and cost of network and service assurance operations, and an API enables OSS integration.

For more information about the NFM-T, see the *NFM-T Getting Started Guide*.

VSR-NRC

The Nokia Virtual Service Router - Network Resources Controller (VSR-NRC) is a Virtualized Network Function (VNF) that is based on the SROS software and which implements the southbound protocols of the NRC-P. These consist of the Path Computation Element (PCE) function, with PCEP, BGP-LS and IGP protocols, and the OpenFlow Controller (OFC).

The VSR-NRC is a virtual SR OS instance that uses the same software image as the vSIM of the same SROS release number; the VSR-NRC license enables additional code to interact with the NSP; this software can only run on a Linux KVM environment.

The VSR-NRC instance has a physical interface to the network and collects topology information and signaled path computation requests from head-end routers. The VSR-NRC is connected to the network by way of a PE router.

For platform requirements and installation instructions, see the *Virtualized 7750 SR and 7950 XRS Simulator (vSIM) Installation and Setup Guide*.

NSP Flow Collectors and Flow Collector Controllers

An NSP Flow Collector is an optional, scalable component that collects AA Cflowd or System Cflowd statistics directly from NEs and forwards the statistics records to a remote target server or an NFM-P database, after which they are available for processing by third-party tools or by applications such as NSP Analytics.

An NSP Flow Collector Controller is required in any deployment that includes one or more NSP Flow Collectors. The Flow Collector Controller extracts the network data model from the NFM-P, and distributes the data model to each Flow Collector, which uses the data model as a statistics-collection framework. The controller receives NFM-P JMS notifications about updates to the objects in the data model, and directs Flow Collector activity by distributing the messages to the appropriate Flow Collectors.

Like other NSP components, NSP Flow Collectors and NSP Flow Collector Controllers support redundant deployment. You can deploy two NSP Flow Collector Controllers that each manage a set of NSP Flow Collectors. In such a scenario, when the active NSP Flow Collector Controller cannot reach the primary NFM-P main server, the NSP Flow Collector Controller tries to reach the standby main server.

Note: The NSP Flow Collector Controller that initializes first assumes the active role.

You can also configure NSP Flow Collectors to transfer the collected statistics files to redundant remote destinations, as described in the *NSP NSM-P User Guide*, and employ other fault-tolerance mechanisms.

See the *NSP System Administrator Guide* for more information about redundancy and other fault-tolerance mechanisms.

NSP analytics servers

An NSP analytics server creates on-demand and scheduled reports about various network conditions and trends for display in the NSP Analytics application. An analytics server generates the reports using business intelligence software to analyze raw and aggregated NE statistics data collected by the NFM-P.

Like other NSP components, NSP analytics servers support redundant deployment. You can deploy multiple redundant analytics servers in an active/active configuration that eliminates a single point of failure in the event that an analytics server fails. Deploying multiple analytics servers also allows load balancing of client requests among the servers, and other fault-tolerance mechanisms.

See the *NSP System Administrator Guide* for more information about redundancy and other fault-tolerance mechanisms.

1.3 Scaling information

1.3.1 Independent deployments

The following describe where to find scaling guidelines for independent component deployments.

NSD and NRC

The *NSP Planning Guide* must be used as a reference when you plan an NSD and NRC deployment.

NFM-P

The *NSP NFM-P Planning Guide* provides scaling guidelines for NFM-P functional areas such as OSS client capacity, scheduled network tests, and statistics collection, and must be used as a reference when you plan an NFM-P deployment.

NFM-T

The *NFM-T Dimensioning and System Configuration Guideline* provides scaling guidelines for the NFM-T, and must be used as a reference when you plan an NFM-T deployment.

1.3.2 Shared-mode deployments

The scale limits of each component in a shared-mode NSP deployment must be considered before you deploy any component; support is limited to the lowest scale limit of the combined components.

See the documents described in 1.3.1 “Independent deployments” (p. 14) for the scale guidelines of each component in your NSP deployment.

1.4 NSP system redundancy and fault tolerance

1.4.1 Description

All NSP modules support a 1+1, or warm standby, redundancy model. In this scenario, each module has a group of active components, and a group of warm standby components; each component is a separate OS instance that hosts a module function. For example, the NFM-P has main server, main database, and optional auxiliary components that perform additional functions. Each main or auxiliary component supports redundancy. All active components of a module require low network latency, so ideally are geographically collocated.

For NSP disaster recovery, you can use the NSP 1+1 redundancy model in two geographically separate locations. Only one system is active at a time; the active system hosts all NSP applications and processes all client requests. The system at the other location runs in a warm standby mode. When redundant NSP systems are in geographically separate facilities, for best performance, it is strongly recommended that the active NSP modules are at the same location. An NSP administrator can allign the active NSP modules in a shared-mode deployment.

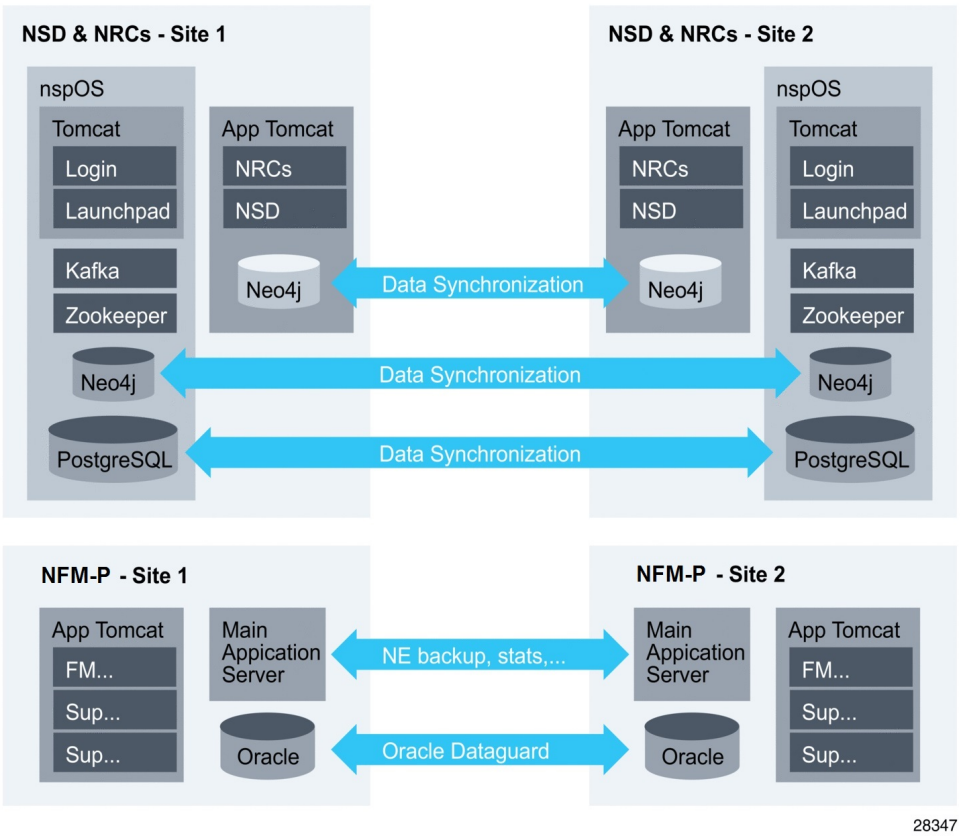
To deploy the NSP as a redundant shared-mode system, each module in the system must be a redundant deployment. If a redundant NSP deployment includes the NFM-T product, the NFM-T must be deployed as a 1+1 redundant system. For the NSD and NRC modules, the redundancy model can be 1+1 or 3+3, which is known as high-availability, or HA, with disaster recovery.

NSP components such as NSP analytics servers, NSP Flow Collector Controllers, and NSP Flow Collectors, also support redundant deployment and other fault-tolerance mechanisms.

See the *NSP System Administrator Guide* for comprehensive descriptions of various NSP system redundancy failure and recovery scenarios, and for information about other NSP fault-tolerance mechanisms.

The following figure shows the NSP modules deployed using 1+1 redundancy.

Figure 1-1 NSP modules, 1+1 redundancy



2 IP-only deployment

2.1 Overview

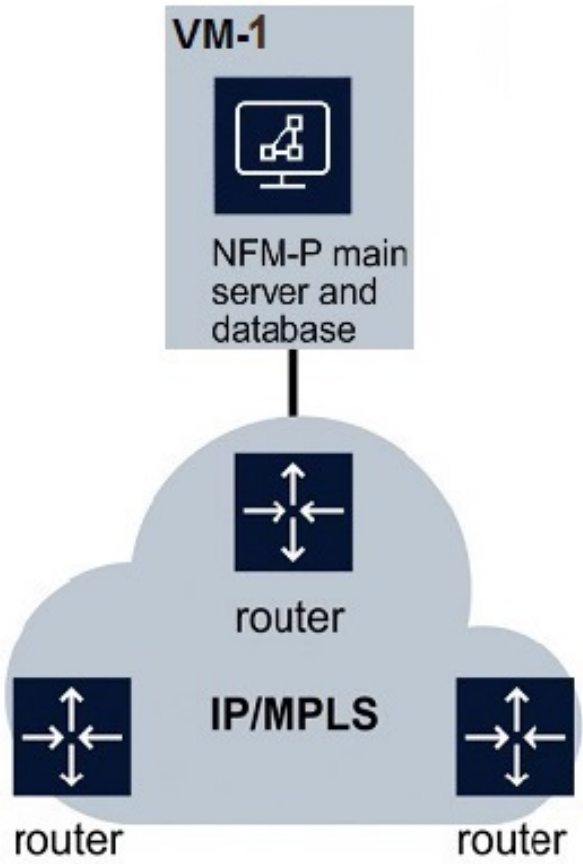
2.1.1 Functionality

An IP-only deployment consists solely of the NFM-P module. When deployed in this role, the NFM-P can perform IP/MPLS network management functions, including SNMP management of NEs.

2.1.2 Sample deployment diagram

The following figure shows an example of an IP-only deployment on virtual machines.

Figure 2-1 IP-only deployment sample diagram



2.1.3 Component summary

The components in the following table, and their corresponding applications, are used in this deployment type.

Table 2-1 IP-only deployment components

Component	Corresponding applications
Common to NSP	Fault Management
	Network Supervision
	Service Supervision
	Supervision Manager
	Telemetry
NFM-P	Analytics
	Inventory Manager
	Link Utilization
	Network Functions Manager - Packet
	Subscriber Manager
	VNF Manager
	Wireless NE View
	Wireless Supervision

Note: In addition to the purchase of the corresponding component, the availability of certain applications may be further dependent on the purchase of specific license types.

2.1.4 Redundancy

IP-only deployments can be installed in either standalone or 1+1 (warm standby) configurations.

2.1.5 Security/authentication

The NFM-P server component interfaces are TLS-secured using the NSP PKI server or custom certificates. The use of a firewall is supported between specific components. For detailed information about securing the NFM-P, including firewall port restrictions, see the *NSP NFM-P Planning Guide*.

User authentication for IP-only deployments is achieved using the local Oracle solution for the NFM-P.

2.2 IP-only installation workflow

2.2.1 Installation

Note: Before you attempt to install any NSP component, you must review and comply with the deployment requirements in the planning guide for that component.

To install an IP-only deployment, install the NFM-P and discover IP nodes as described in the *NSP NFM-P Installation and Upgrade Guide*.

3 Control plane-only deployment

3.1 Overview

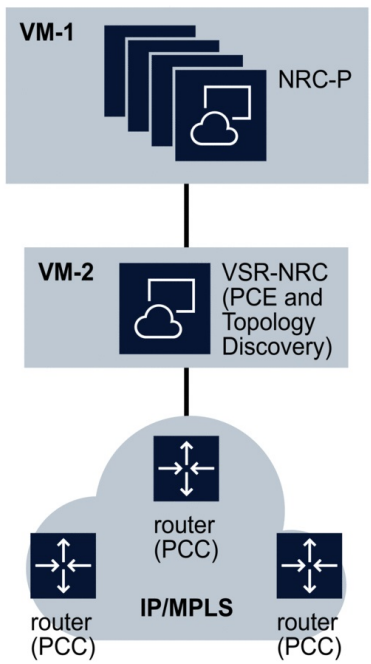
3.1.1 Functionality

A control plane-only deployment consists of the NRC-P module and a VSR-NRC. When deployed in this role, the NRC-P can perform IGP link-state topology optimization functions.

3.1.2 Sample deployment diagram

The following figure shows an example of a control plane-only deployment on virtual machines.

Figure 3-1 Control plane-only deployment sample diagram



3.1.3 Component summary

The components in the following table, and their corresponding applications, are used in this deployment type.

Table 3-1 Control plane-only deployment components

Component	Corresponding applications
Common to NSP	Fault Management
	Network Supervision
	Supervision Manager
	Telemetry
NRC-P	IP/MPLS Optimization

Note: In addition to the purchase of the corresponding component, the availability of certain applications may be further dependent on the purchase of specific license types.

Note: Additional NSD and NRC-P applications are installed with this deployment but are not usable.

3.1.4 Redundancy

Control plane-only deployments can be installed in either a standalone configuration or a redundant configuration.

Table 3-2, “Control plane-only deployment redundancy options” (p. 22) provides information about redundancy options for different components of the deployment.

Table 3-2 Control plane-only deployment redundancy options

Component or VM	Redundancy options	Notes
NRC-P/NSD	• 1+1 (warm standby) • 3+3 (high availability with disaster recovery)	If the redundant deployment includes a VSR-NRC, the VSR-NRC must also be in a redundant configuration.
VSR-NRC	1+1 (warm standby)	—

See the *NSP System Administrator Guide* for information about the redundancy failure and recovery scenarios.

Note: VSR-NRC failover/switchover is controlled by NRC-P, not the VSR-NRC

3.1.5 Security/authentication

The NRC-P module is TLS-secured using the NSP PKI server or custom certificates. See 12.2 “NSP user accounts” (p. 86) for more information. The use of a firewall is supported between the module components. For detailed information about securing the NRC-P, including firewall port restrictions, see the *NSP Planning Guide*.

User authentication for control plane-only deployments is achieved using the NSP CAS.

3.2 Control plane-only installation workflow

3.2.1 Description

Follow this workflow to install the components that make up a control plane-only deployment.

Note: Before you attempt to install any NSP component, you must review and comply with the deployment requirements in the planning guide for that component.

3.2.2 Stages

1

Install an NSP server to host the NSD and NRC modules. Perform one of the following procedures:

a. 14.2 “To install a standalone NSP server” (p. 121)

b. 14.3 “To install a redundant NSP server” (p. 124)

c. 14.4 “To install NSP servers in HA mode with redundancy” (p. 127)

Note: The NSD module is installed in this deployment but is not licensed or used.

2

Install the VSR-NRC. See 14.12 “VSR-NRC installation” (p. 153) for more information.

4 NRC-P Sim deployment

4.1 Overview

4.1.1 Functionality

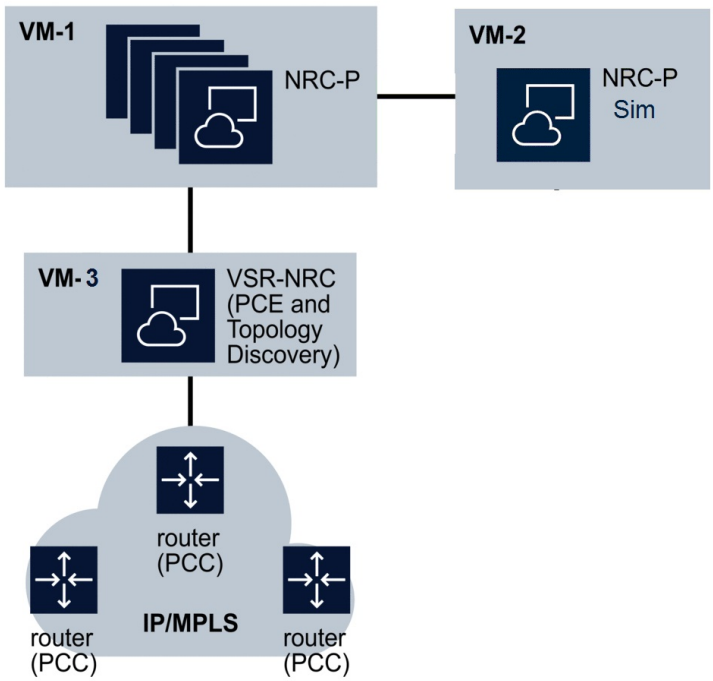
An NRC-P Sim deployment consists of the NRC-P module, a VSR-NRC, and the NRC-P Sim traffic engineering tool. When deployed in this configuration, the NRC-P Sim is used to simulate the impact of actions typically performed by the NRC-P on IGP topologies imported from VSR-NRC.

4.1.2 Sample deployment diagram

The following figure shows an example of an NRC-P Sim deployment on virtual machines.

Note: This sample deployment displays only those components that are essential to the NRC-P Sim tool. NRC-P Sim can be included in any other deployment type that includes the NRC-P module.

Figure 4-1 NRC-P Sim deployment sample diagram



4.1.3 Component summary

The components in the following table, and their corresponding applications, are used in this deployment type.

Table 4-1 NRC-P Sim deployment components

Component	Corresponding applications
Common to NSP	Fault Management
	Network Supervision
	Supervision Manager
	Telemetry
NRC-P	IP/MPLS Optimization
NRC-P Sim	IP/MPLS Simulation

Note: In addition to the purchase of the corresponding component, the availability of certain applications may be further dependent on the purchase of specific license types.

Note: Additional NSD and NRC-P applications are installed with this deployment but are not usable.

4.1.4 Redundancy

NRC-P Sim deployments can only be installed in a standalone configuration.

4.1.5 Security/authentication

The NRC-P Sim is TLS-secured using the NSP PKI server or custom certificates. See 12.2 “NSP user accounts” (p. 86) for more information. The use of a firewall is supported between the module components. For detailed information about securing the NRC-P Sim, including firewall port restrictions, see the *NSP Planning Guide*.

User authentication for control plane-only deployments is achieved using the NSP CAS.

The NRC-P Sim is deployed with its own instance of nspOS, and selects its own user authentication sources independent of those selected by the NSP server hosting the NSD and NRC-P modules. Either local users or external authentication sources will be selected during installation.

4.2 NRC-P Sim installation workflow

4.2.1 Description

Follow this workflow to install the components that make up an NRC-P Sim deployment.

Note: Before you attempt to install any NSP component, you must review and comply with the deployment requirements in the planning guide for that component.

4.2.2 Stages

1

Install an NSP server to host the NSD and NRC-P modules. Perform one of the following procedures:

a. 14.2 “To install a standalone NSP server” (p. 121)

b. 14.3 “To install a redundant NSP server” (p. 124)

c. 14.4 “To install NSP servers in HA mode with redundancy” (p. 127)

Note: The NSD module is installed in this deployment but is not licensed or used.

2

Perform 14.2 “To install a standalone NSP server” (p. 121) to install an NSP server to host the NRC-P Sim tool.

3

Install the VSR-NRC. See 14.12 “VSR-NRC installation” (p. 153) for more information.

5 WAN SDN + IP deployment with MDM

5.1 Overview

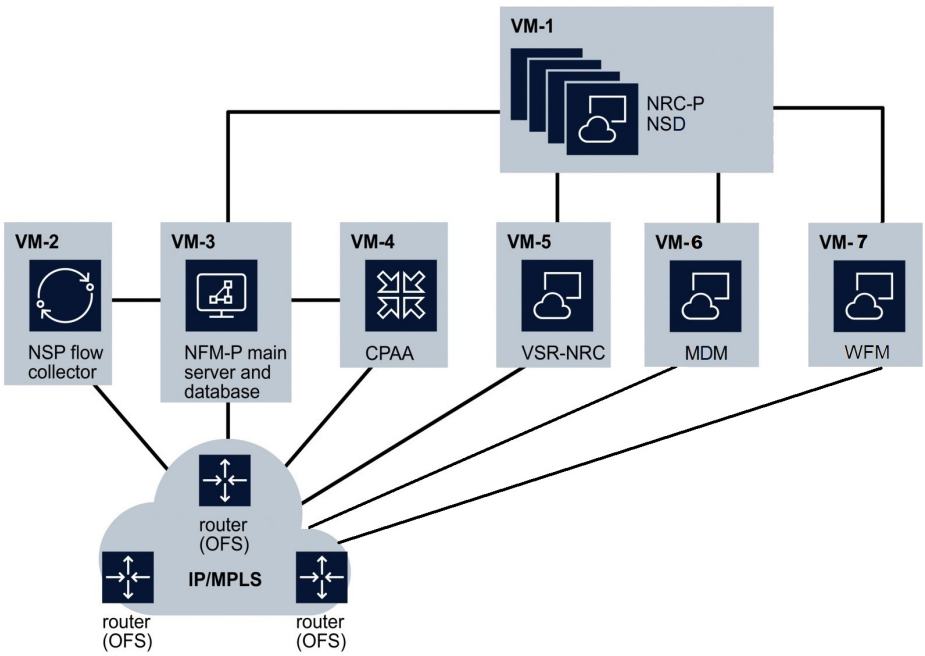
5.1.1 Functionality

A WAN SDN + IP deployment consists of the NFM-P module and the NSD and NRC modules, as well as ancillary components such as the CPAA and VSR-NRC. WAN SDN + IP NSP deployments allow for IP/MPLS network management functions while also providing SDN service provisioning and resource control. In the example shown in this chapter, MDM is in use.

5.1.2 Sample deployment diagram

The following figure shows an example of a WAN SDN + IP deployment on virtual machines.

Figure 5-1 WAN SDN + IP only deployment sample diagram



5.1.3 Component summary

The components in the following table, and their corresponding applications, are used in this deployment type.

Table 5-1 WAN SDN + IP deployment components

Component	Corresponding applications
Common to NSP	Fault Management
	Network Supervision
	Service Supervision
	Supervision Manager
	Telemetry
NFM-P	Analytics
	Inventory Manager
	Link Utilization
	Network Functions Manager - Packet
	Subscriber Manager
	VNF Manager
	Wireless NE View
	Wireless Supervision
NRC-P	Autonomous System Optimizer
	IP/MPLS Optimization
	Latency Steering Optimizer
	Traffic Steering Controller
NSD	Policy Management
	Service Fulfillment
	Task Scheduler
MDM	Modeled Device Configurator
	Device Administrator
Workflow Manager	

Note: In addition to the purchase of the corresponding component, the availability of certain applications may be further dependent on the purchase of specific license types.

5.1.4 Redundancy

WAN SDN + IP deployments can be installed in either a standalone configuration or a redundant configuration.

Table 5-2, “WAN SDN + IP deployment redundancy options” (p. 31) provides information about redundancy options for different components of the deployment.

Redundancy of components is configured in the hosts file; see 13.2 “NSP hosts file” (p. 101).

Table 5-2 WAN SDN + IP deployment redundancy options

Component or VM	Redundancy options	Notes
NRC-P/NSD	• 1+1 (disaster recovery) • 3+3 (high availability with disaster recovery)	If the redundant deployment includes a VSR-NRC, the VSR-NRC must also be in a redundant configuration.
NFM-P	1+1 (warm standby)	—
MDM server	• 1+1 (disaster recovery) • MDM server cluster with high availability (HA) • MDM HA in a disaster recovery configuration (HA/DR) MDM HA redundancy is non-revertive: if an active server goes down, it will become a standby server after it is brought back online.	An MDM cluster can be used with either a standalone or redundant NRC-P/NSD system. If the NRC-P/NSD system is redundant, both the total number of MDM servers and the number of standby MDM servers must be the same at both sites.
VSR-NRC	1+1 (disaster recovery)	—
Workflow Manager	The Workflow Manager is installed on its own VM (distributed) in production deployments. Collocated WFM installations, where WFM is installed on the same VM as the NSD/NRC, are supported in lab or trial deployments. Redundancy options are: • 1+1 distributed • 1+1 collocated (lab/trial only)	In a redundant distributed configuration, the NRC-P/NSD and the WFM must be manually aligned.

See the *NSP System Administrator Guide* for comprehensive descriptions of various redundancy failure and recovery scenarios.

Note: VSR-NRC failover/switchover and MDM failover/switchover is controlled by NSD and NRC-P

You can convert a standalone NRC-P/NSD system to a redundant deployment, or convert a standalone MDM server to a cluster, with a standalone or redundant NRC-P/NSD. See 17.2 “To convert a standalone NSD and NRC system to a redundant NSD and NRC system” (p. 237).

5.1.5 Security/authentication

The NFM-P server component interfaces are TLS-secured using the NSP PKI server or custom certificates. The use of a firewall is supported between specific components. For detailed information about securing the NFM-P, including firewall port restrictions, see the *NSP NFM-P Planning Guide*.

The NSD and NRC modules are TLS-secured using the NSP PKI server or custom certificates. See 12.2 “NSP user accounts” (p. 86) for more information. The use of a firewall is supported between the module components. For detailed information about securing the NSD and NRC modules, including firewall port restrictions, see the *NSP Planning Guide*.

User authentication for shared-mode deployments is achieved using the NSP CAS.

5.2 WAN SDN + IP installation workflow

5.2.1 Description

Follow this workflow to install the components that make up a WAN SDN + IP deployment.

Note: The components of an NSP shared-mode deployment can be installed together, or added over time. Component release compatibility is described in the *NSP Release Notice*.

Note: User group properties are module-specific. This means that, when a user of a specific NSP module requires authorization to access an additional module, that user's group property must be re-created within the new module in order for them to access those module applications. Instructions for creating a user group property within a module are in the required module documentation.

Note: Before you attempt to install any NSP component, you must review and comply with the deployment requirements in the planning guide for that component.

5.2.2 Stages

1

Install an NSP server to host the nspOS + common applications + NSD and NRC modules; perform one of the following procedures, based on the NFM-P deployment type:

a. 14.2 “To install a standalone NSP server” (p. 121)

b. 14.3 “To install a redundant NSP server” (p. 124)

c. 14.4 “To install NSP servers in HA mode with redundancy” (p. 127)

2

Install the NFM-P, as described in the *NSP NFM-P Installation and Upgrade Guide*; configure the NFM-P to use the NSP PKI server for TLS.

3

If you are adding the NSD and NRC to an existing NFM-P system, add the NSP servers to the NFM-P system; perform 16.2 “To integrate NSP servers with an NFM-P system” (p. 205).

4

Perform 14.10 “To install the NSP templates on the NFM-P” (p. 151) to install the NSP templates on the NFM-P.

5

Install the VSR-NRC, if required. See 14.12 “VSR-NRC installation” (p. 153) for more information.

6

Install adaptors on the MDM server; see 14.5 “To install MDM adaptors” (p. 130).

6 WAN SDN with MDM deployment

6.1 Overview

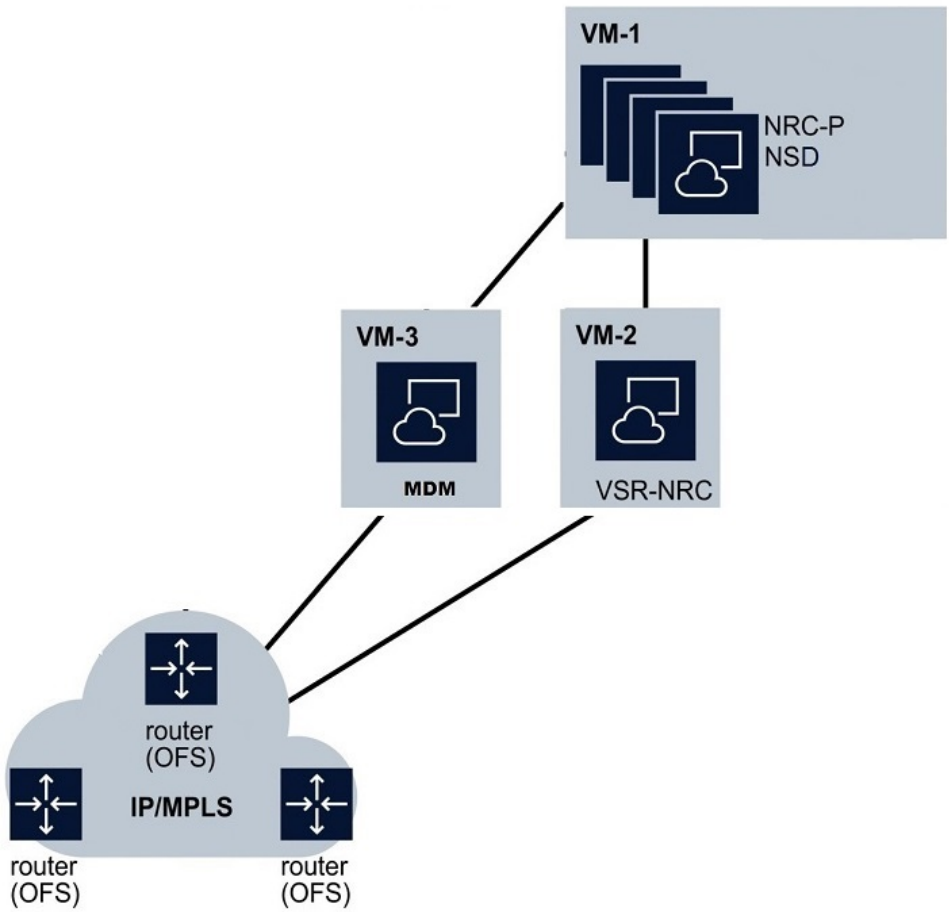
6.1.1 Functionality

A WAN SDN deployment consists of the NSD and NRC modules with MDM, as well as ancillary components such as the VSR-NRC. WAN SDN NSP deployments with MDM allow for NE management while also providing SDN service provisioning and resource control.

6.1.2 Sample deployment

The following figure shows an example of a WAN SDN with MDM deployment on virtual machines.

Figure 6-1 WAN SDN with MDM deployment sample diagram



6.1.3 Component summary

The components in the following table, and their corresponding applications, are available in this deployment type.

Table 6-1 WAN SDN with MDM deployment components

Component	Corresponding applications
Common to NSP	Fault Management
	Network Supervision
	Supervision Manager
	Telemetry
NRC-P	Autonomous System Optimizer
	IP/MPLS Optimization
	Latency Steering Optimizer
	Traffic Steering Controller
NSD	Policy Management
	Service Fulfillment
	Task Scheduler
MDM	Modeled Device Configurator
	Device Administrator

6.1.4 Redundancy

WAN SDN with MDM deployments can be installed in either a standalone configuration or a redundant configuration.

Table 6-2, “WAN SDN with MDM deployment redundancy options” (p. 36) provides information about redundancy options for different components of the deployment.

Table 6-2 WAN SDN with MDM deployment redundancy options

Component or VM	Redundancy options	Notes
NRC-P/NSD	• 1+1 (disaster recovery) • 3+3 (high availability with disaster recovery)	If the redundant deployment includes a VSR-NRC, the VSR-NRC must also be in a redundant configuration.

Table 6-2 WAN SDN with MDM deployment redundancy options (continued)

Component or VM	Redundancy options	Notes
MDM server	• 1+1 (disaster recovery) • MDM server cluster with high availability (HA) • MDM HA in a disaster recovery configuration (HA/DR) MDM HA redundancy is non-revertive: if an active server goes down, it will become a standby server after it is brought back online.	An MDM cluster can be used with either a standalone or redundant NRC-P/NSD system. If the NRC-P/NSD system is redundant, both the total number of MDM servers and the number of standby MDM servers must be the same at both sites.
VSR-NRC	1+1 (disaster recovery)	—

See the *NSP System Administrator Guide* for comprehensive descriptions of various redundancy failure and recovery scenarios.

Note: VSR-NRC failover/switchover and MDM failover/switchover is controlled by NSD and NRC-P

You can convert a standalone NRC-P/NSD system to a redundant deployment, or convert a standalone MDM server to a cluster, with a standalone or redundant NRC-P/NSD. See 17.2 “To convert a standalone NSD and NRC system to a redundant NSD and NRC system” (p. 237).

6.2 WAN SDN with MDM installation workflow

6.2.1 Description

Follow this workflow to install the components that make up a WAN SDN + MDM deployment.

Note: The components of an NSP deployment can be installed together, or added over time. Component release compatibility is described in the *NSP Release Notice*.

Note: User group properties are module-specific. This means that, when a user of a specific NSP module requires authorization to access an additional module, that user's group property must be re-created within the new module in order for them to access those module applications. Instructions for creating a user group property within a module are in the required module documentation.

6.2.2 Stages

1

Install an NSP server to host the nspOS + common applications. Perform one of the following procedures:

a. 14.2 “To install a standalone NSP server” (p. 121)

b. 14.3 “To install a redundant NSP server” (p. 124)

c. 14.4 “To install NSP servers in HA mode with redundancy” (p. 127)

2

Install the VSR-NRC. See 14.12 “VSR-NRC installation” (p. 153) for information.

3

Install adaptors on the MDM server; see 14.5 “To install MDM adaptors” (p. 130).

7 WAN SDN + IP + Optical deployment

7.1 Overview

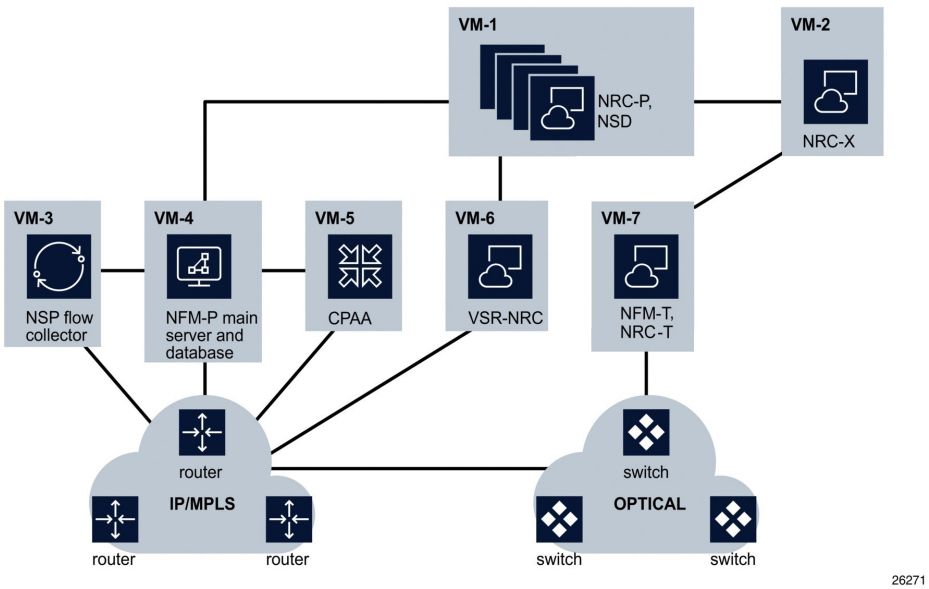
7.1.1 Functionality

A WAN SDN + IP + Optical deployment consists of the NFM-P module, the NFM-T product, and the NSD and NRC modules, as well as ancillary components such as the CPAA and VSR-NRC. WAN SDN + IP + Optical NSP deployments allow for IP/MPLS network management functions and transport network management functions while also providing SDN service provisioning and resource control.

7.1.2 Sample deployment diagram

The following figure shows an example of a WAN SDN + IP + Optical deployment on virtual machines.

Figure 7-1 WAN SDN + IP + Optical deployment sample diagram



7.1.3 Component summary

The components in the following table, and their corresponding applications, are used in this deployment type.

Table 7-1 WAN SDN + IP + Optical deployment components

Component	Corresponding applications
Common to NSP	Fault Management
	Network Supervision
	Service Supervision
	Supervision Manager
	Telemetry
NFM-P	Analytics
	Inventory Manager
	Link Utilization
	Network Functions Manager - Packet
	Subscriber Manager
	VNF Manager
	Wireless NE View
	Wireless Supervision
NFM-T	Network Functions Manager - Transport
NRC-P	Autonomous System Optimizer
	IP/MPLS Optimization
	Latency Steering Optimizer
	Traffic Steering Controller
NRC-T	Optical Service Fulfillment
NRC-X	Cross Domain Correlation
NSD	Policy Management
	Service Fulfillment
	Task Scheduler

Note: In addition to the purchase of the corresponding component, the availability of certain applications may be further dependent on the purchase of specific license types.

7.1.4 Redundancy

WAN SDN + IP + Optical deployments can be installed in either a standalone configuration or a redundant configuration.

Table 7-2, “WAN SDN + IP + Optical deployment redundancy options” (p. 41) provides information about redundancy options for different components of the deployment.

Table 7-2 WAN SDN + IP + Optical deployment redundancy options

Component or VM	Redundancy options	Notes
NRC-P/NSD NRC-X	• 1+1 (warm standby) • 3+3 (high availability with disaster recovery)	If the redundant deployment includes a VSR-NRC, the VSR-NRC must also be in a redundant configuration.
NFM-T NRC-T	1+1 (classic HA)	—
NFM-P	1+1 (warm standby)	—
VSR-NRC	1+1 (warm standby)	—

See the *NSP System Administrator Guide* for comprehensive descriptions of various redundancy failure and recovery scenarios.

Note: VSR-NRC failover/switchover is controlled by NSD and NRC-P, not the VSR-NRC.

7.1.5 Security/authentication

The NFM-P server component interfaces are TLS-secured using the NSP PKI server or custom certificates. The use of a firewall is supported between specific components. For detailed information about securing the NFM-P, including firewall port restrictions, see the *NSP NFM-P Planning Guide*.

For detailed information about securing the NFM-T, including firewall port restrictions, see the *NFM-T Firewall Configuration Guide*.

The NSD and NRC modules are TLS-secured using the NSP PKI server or custom certificates. See 12.2 “NSP user accounts” (p. 86) for more information. The use of a firewall is supported between the module components. For detailed information about securing the NSD and NRC modules, including firewall port restrictions, see the *NSP Planning Guide*.

User authentication for shared-mode deployments is achieved using the NSP CAS.

Note: Only unsecured connections are supported between NFM-T and ZooKeeper/Kafka.

7.2 WAN SDN + IP + Optical installation workflow

7.2.1 Description

Follow this workflow to install the components that make up a WAN SDN + IP + Optical deployment.

Note: The components of an NSP shared-mode deployment can be installed together, or added over time. Component release compatibility is described in the *NSP Release Notice*.

Note: User group properties are module-specific. This means that, when a user of a specific NSP module requires authorization to access an additional module, that user's group property

must be re-created within the new module in order for them to access those module applications. Instructions for creating a user group property within a module are in the required module documentation.

Note: Before you attempt to install an NSP component, you must review and comply with the deployment requirements in the planning guide for that component.

7.2.2 Stages

1

Install an NSP server to host the nspOS + common applications + NSD and NRC modules. Perform one of the following procedures based on the NFM-P and NFM-T deployment types installed in Stage 2 and Stage 5.

a. 14.2 "To install a standalone NSP server" (p. 121)

b. 14.3 "To install a redundant NSP server" (p. 124)

c. 14.4 "To install NSP servers in HA mode with redundancy" (p. 127)

2

Install the NFM-P, as described in the *NSP NFM-P Installation and Upgrade Guide*; configure the NFM-P to use the NSP PKI server for TLS.

3

If you are adding the NSD and NRC to an existing NFM-P system, add the NSP servers to the NFM-P system; perform 16.2 "To integrate NSP servers with an NFM-P system" (p. 205).

4

Perform 14.10 "To install the NSP templates on the NFM-P" (p. 151) to install the NSP templates on the NFM-P.

5

Install the NFM-T, as described in the *NFM-T HW and OS Installation Guide* and the *NFM-T Installation Guide*.

6

If you are adding the NSD and NRC to an existing NFM-T system, add the NSP servers to the NFM-T system; perform 16.3 "To integrate NSP servers with an NFM-T system" (p. 211).

Note: NFM-T information must be added to the NSD and NRC module config.yml file, then the install.sh script must be run in order to capture the changes.

7

Perform 14.11 "To map external user groups to predefined NFM-T roles" (p. 151).

8

Install the VSR-NRC, if required. See 14.12 “VSR-NRC installation” (p. 153) for more information.

8 IP + Optical (small scale) deployment

8.1 Overview

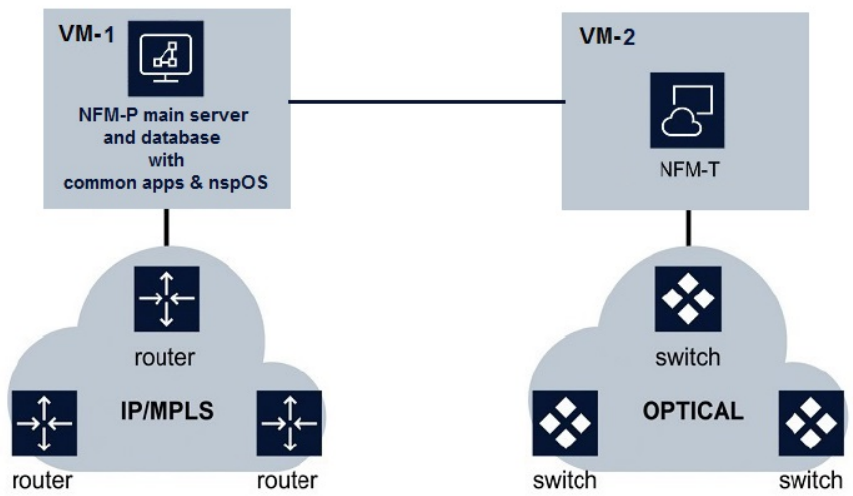
8.1.1 Functionality

An IP + Optical (small scale) deployment consists of the NFM-P module and the NFM-T product. IP + Optical (small scale) NSP deployments allow for IP/MPLS network management functions and transport network management functions. In this configuration, the NSP common applications and nspOS instance are hosted alongside the NFM-P module. Deployments of this type should only be used when the IP and Optical networks consist of fewer than fifty (50) network elements combined. Larger networks should use the traditional IP + Optical deployment described in Chapter 9, “IP + Optical deployment”.

8.1.2 Sample deployment diagram

The following figure shows an example of an IP + Optical (small scale) deployment on virtual machines.

Figure 8-1 IP + Optical (small scale) deployment sample diagram



8.1.3 Component summary

The components in the following table, and their corresponding applications, are available in this deployment type.

Table 8-1 IP + Optical (small scale) deployment components

Component	Corresponding applications
Common to NSP	Fault Management
	Network Supervision
	Service Supervision
	Supervision Manager
NFM-P	Network Functions Manager - Packet
NFM-T	Network Functions Manager - Transport

Note: In addition to the purchase of the corresponding component, the availability of certain applications may be further dependent on the purchase of specific license types.

8.1.4 Redundancy

IP + Optical (small scale) deployments can be installed in either a standalone configuration or a redundant configuration.

Table 8-2, “IP + Optical deployment redundancy options” (p. 46) provides information about redundancy options for different components of the deployment.

Table 8-2 IP + Optical deployment redundancy options

Component or VM	Redundancy options	Notes
NFM-P	1+1 (warm standby)	—
NFM-T	1+1 (classic HA)	—

See the *NSP System Administrator Guide* for comprehensive descriptions of various redundancy failure and recovery scenarios.

8.1.5 Security/authentication

The NFM-P server component interfaces are TLS-secured using the NSP PKI server or custom certificates. The use of a firewall is supported between specific components. For detailed information about securing the NFM-P, including firewall port restrictions, see the *NSP NFM-P Planning Guide*.

For detailed information about securing the NFM-T, including firewall port restrictions, see the *NFM-T Firewall Configuration Guide*.

User authentication for shared-mode deployments is achieved using the NSP CAS.

8.2 IP + Optical (small scale) installation workflow

8.2.1 Description

Follow this workflow to install the components that make up an IP + Optical (small scale) deployment.

Note: The components of an NSP shared-mode deployment can be installed together, or added over time. Component release compatibility is described in the *NSP Release Notice*.

Note: User group properties are module-specific. This means that, when a user of a specific NSP module requires authorization to access an additional module, that user's group property must be re-created within the new module in order for them to access those module applications. Instructions for creating a user group property within a module are in the required module documentation.

Note: Before you attempt to install an NSP component, you must review and comply with the deployment requirements in the planning guide for that component.

8.2.2 Stages

1

Install the NFM-P, as described in the *NSP NFM-P Installation and Upgrade Guide*; configure the NFM-P to use the NSP PKI server for TLS.

2

Install the NFM-T, as described in the *NFM-T HW and OS Installation Guide* and the *NFM-T Installation Guide*.

3

Perform 16.5 “To integrate an NFM-T system with an NFM-P system” (p. 230).

8.3 IP + Optical (small scale) upgrade workflow

8.3.1 Description

Follow this workflow to upgrade the components that make up an IP + Optical (small scale) deployment.

Note: You must upgrade the NFM-P first.

8.3.2 Stages

1

Upgrade the NFM-P, as described in the *NSP NFM-P Installation and Upgrade Guide*.

2

Upgrade the NFM-T, as described in the *NFM-T HW and OS Installation Guide* and the *NFM-T Installation Guide*.

9 IP + Optical deployment

9.1 Overview

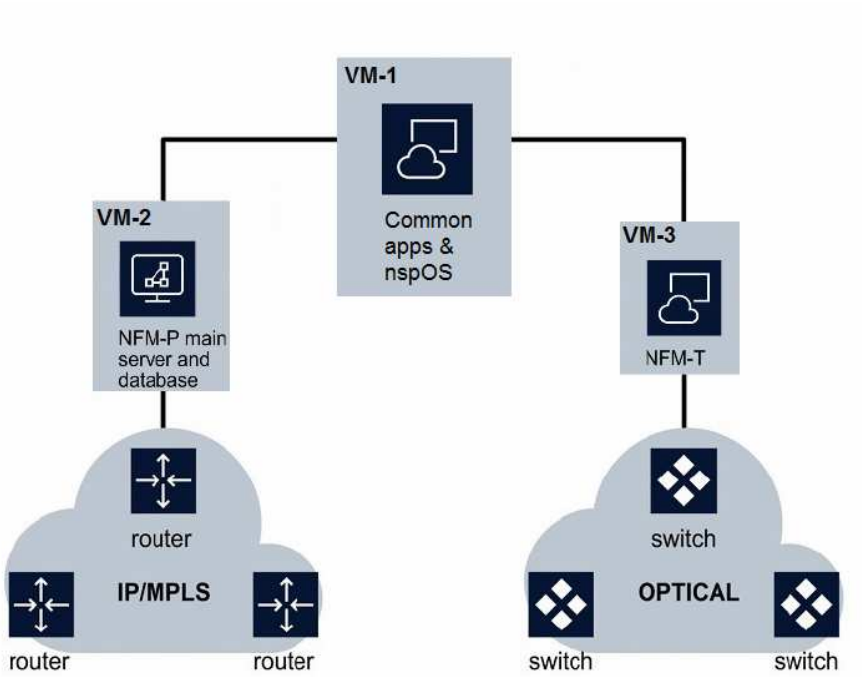
9.1.1 Functionality

An IP + Optical deployment consists of the NFM-P module and the NFM-T product, as well as an nspOS host system. IP + Optical NSP deployments allow for IP/MPLS network management functions and transport network management functions.

9.1.2 Sample deployment diagram

The following figure shows an example of an IP + Optical deployment on virtual machines.

Figure 9-1 IP + Optical deployment sample diagram



9.1.3 Component summary

The components in the following table, and their corresponding applications, are available in this deployment type.

Table 9-1 IP + Optical deployment components

Component	Corresponding applications
Common to NSP	Fault Management
	Network Supervision
	Service Supervision
	Supervision Manager
	Telemetry
NFM-P	Analytics
	Inventory Manager
	Link Utilization
	Network Functions Manager - Packet
	Subscriber Manager
	VNF Manager
	Wireless NE View
	Wireless Supervision
NFM-T	Network Functions Manager - Transport

Note: In addition to the purchase of the corresponding component, the availability of certain applications may be further dependent on the purchase of specific license types.

9.1.4 Redundancy

IP + Optical deployments can be installed in either a standalone configuration or a redundant configuration.

Table 9-2, “IP + Optical deployment redundancy options” (p. 50) provides information about redundancy options for different components of the deployment.

Table 9-2 IP + Optical deployment redundancy options

Component or VM	Redundancy options	Notes
NRC-P/NSD	• 1+1 (warm standby) • 3+3 (high availability with disaster recovery)	If the redundant deployment includes a VSR-NRC, the VSR-NRC must also be in a redundant configuration.
NFM-P	1+1 (warm standby)	—
NFM-T	1+1 (classic HA)	—

See the *NSP System Administrator Guide* for comprehensive descriptions of various redundancy failure and recovery scenarios.

9.1.5 Security/authentication

The NFM-P server component interfaces are TLS-secured using the NSP PKI server or custom certificates. The use of a firewall is supported between specific components. For detailed information about securing the NFM-P, including firewall port restrictions, see the *NSP NFM-P Planning Guide*.

For detailed information about securing the NFM-T, including firewall port restrictions, see the *NFM-T Firewall Configuration Guide*.

The nspOS host system is TLS-secured using the NSP PKI server or custom certificates. See 12.2 “NSP user accounts” (p. 86) for more information.

User authentication for shared-mode deployments is achieved using the NSP CAS.

Note: Only unsecured connections are supported between NFM-T and ZooKeeper/Kafka.

9.2 IP + Optical installation workflow

9.2.1 Description

Follow this workflow to install the components that make up an IP + Optical deployment.

Note: The components of an NSP shared-mode deployment can be installed together, or added over time. Component release compatibility is described in the *NSP Release Notice*.

Note: User group properties are module-specific. This means that, when a user of a specific NSP module requires authorization to access an additional module, that user's group property must be re-created within the new module in order for them to access those module applications. Instructions for creating a user group property within a module are in the required module documentation.

Note: Before you attempt to install an NSP component, you must review and comply with the deployment requirements in the planning guide for that component.

9.2.2 Stages

1

Install an NSP server to host the nspOS + common applications. Perform one of the following procedures based on the NFM-P and NFM-T deployment types:

a. 14.2 “To install a standalone NSP server” (p. 121)

b. 14.3 “To install a redundant NSP server” (p. 124)

c. 14.4 “To install NSP servers in HA mode with redundancy” (p. 127)

2

Install the NFM-P, as described in the *NSP NFM-P Installation and Upgrade Guide*; configure the NFM-P to use the NSP PKI server for TLS.

3

If you are adding the NSP server to an existing NFM-P system, perform 16.2 “To integrate NSP servers with an NFM-P system” (p. 205).

4

Install the NFM-T, as described in the *NFM-T HW and OS Installation Guide* and the *NFM-T Installation Guide*.

5

If you are adding the NSP server to an existing NFM-T system, perform 16.3 “To integrate NSP servers with an NFM-T system” (p. 211).

NFM-T information must be added to the NSP server's*config.yml* file, then the *install.sh* script must be run in order to capture these changes.

6

Perform 14.11 “To map external user groups to predefined NFM-T roles” (p. 151).

7

Disable any NSP applications that the deployment does not support. Perform “To enable or disable NSP applications” in the *NSP System Administrator Guide*.

Part II: NSP server commissioning

Overview

Purpose

This part of the *NSP Deployment and Installation Guide* describes the configuration required on a station before you attempt to deploy an NSP component on the station.

Contents

10 NSP disk partitioning

10.1 Overview

10.1.1 Purpose

This chapter describes the disk configuration and partitioning requirements for NSP components in trial and live deployments.

10.1.2 Contents

10.2 Disk partitioning for trial deployments

10.2.1 Trial partitioning requirements

CAUTION

Service Disruption

Each disk partition described in this section must be a mounted partition and not a symbolic link.

NSP servers do not support the use of symbolic links to represent partitions.

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

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

The following table lists the partition requirements for the trial deployment of an NSP server that hosts the NRC-P, NRC-P Sim, NRC-X, or NSD and NRC-P.

Table 10-1 Trial partitioning scheme, NSP server

Partition	Content	Size (Gbytes)
swap	Swap space	16
/	Root	26
/home	User home directories	0.5
/tmp	Temporary files	6
/var	System data	64

Table 10-1 Trial partitioning scheme, NSP server (continued)

Partition	Content	Size (Gbytes)
/var/log	System logs	6
var/log/audit	System audit logs	6
/opt/nsp	NSD and NRC software, operating data, and backups	90
/opt/nsp/os	nspOS software, operating data, and backups	90
/extra	NSP software storage	15

The following table lists the partition requirements for the trial deployment of an NSP Flow Collector Controller.

Table 10-2 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
/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

The following table lists the partition requirements for the trial deployment of an NSP Flow Collector.

Table 10-3 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

Table 10-3 Trial partitioning scheme, NSP Flow Collector (continued)

Disks required: one 300-Gbyte or larger		
Partition	Content	Size (Gbytes)
/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

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

Table 10-4 Trial partitioning scheme, collocated NSP Flow Collector Controller and 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

The following table lists the partition requirements for the trial deployment of an NSP analytics server.

Table 10-5 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

Table 10-5 Trial partitioning scheme, NSP analytics server (continued)

Disks required: one 300-Gbyte		
Partition	Content	Size (Gbytes)
/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

The following table lists the partition requirements for the trial deployment of an MDM server.

Table 10-6 Trial partitioning scheme, MDM server

Partition	Content	Size (GBytes)
/	Root	26
/extra	Application software, and so on	15
/home	User home directories	1
/opt/nsp	MDM software and operating data	40
/tmp	Temporary files	6
/var	System data	64
/var/log	System logs	6
/var/log/audit	System audit logs	6
/swap	Swap space	16

Table 10-7 Trial partitioning scheme, WFM virtual machine

Partition	Content	Size (GBytes)
/	Root	26
/extra	Application software, and so on	15
/home	User home directories	0.5
/opt/nsp	WFM software and operating data	100
/tmp	Temporary files	6
/var	System data	64
/var/log	System logs	6
/var/log/audit	System audit logs	6
/swap	Swap space	16

10.3 Disk partitioning for live deployments

10.3.1 Live partitioning requirements

CAUTION

Service Disruption

Each disk partition described in this section must be a mounted partition and not a symbolic link.

NSP servers do not support the use of symbolic links to represent partitions.

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

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

The following table lists the partition requirements for the live deployment of an NSP server that hosts the NRC-P, NRC-P Sim, NRC-X, or NSD and NRC-P.

Table 10-8 Live partitioning scheme, NSP server

Partition	Content	Size (Gbytes)
swap	Swap space	16
/	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	NSD and NRC software, operating data, and backups	100
/opt/nsp/os	nspOS software, operating data, and backups	100
/opt/nsp/os/pgsql	PostgreSQL software and data (not applicable to NRC-X)	200
/extra	NSP software storage	50

The following table lists the partition requirements for the live deployment of an NSP Flow Collector Controller.

Table 10-9 Live partitioning scheme, NSP Flow Collector Controller

Disks required: two 300-Gbyte (RAID 0)		
Partition	Content	Size (Gbytes)
swap	Swap space	16
/	Root	26

Table 10-9 Live partitioning scheme, NSP Flow Collector Controller (continued)

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

The following table lists the partition requirements for the live deployment of an NSP Flow Collector.

Table 10-10 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

The following table lists the partition requirements for the live deployment of an NSP Flow Collector Controller and Flow Collector that are collocated on one station.

Table 10-11 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

Table 10-11 Live partitioning scheme, collocated NSP Flow Collector Controller and Flow Collector (continued)

Disks required: two 300-Gbyte		
Partition	Content	Size (Gbytes)
/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

The following table lists the partition requirements for the live deployment of an NSP analytics server.

Table 10-12 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

The following table lists the partition requirements for the live deployment of an MDM server.

Table 10-13 Live partitioning scheme, MDM server

Partition	Content	Size (GBytes)
/	Root	26
/extra	Application software, and so on	15

Table 10-13 Live partitioning scheme, MDM server (continued)

Partition	Content	Size (GBytes)
/home	User home directories	1
/opt/nsp	MDM software and operating data	40
/tmp	Temporary files	6
/var	System data	64
/var/log	System logs	6
/var/log/audit	System audit logs	6
/swap	Swap space	16

Table 10-14 Live partitioning scheme, WFM virtual machine

Partition	Content	Size (GBytes)
/	Root	26
/extra	Application software, and so on	15
/home	User home directories	0.5
/opt/nsp	WFM software and operating data	100
/tmp	Temporary files	6
/var	System data	64
/var/log	System logs	6
/var/log/audit	System audit logs	6
/swap	Swap space	16

11 NSP RHEL OS configuration

11.1 Overview

11.1.1 Purpose

This chapter describes the following:

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

11.1.2 Contents

11.2 Introduction

11.2.1 Description

This chapter describes the following RHEL OS deployment and configuration methods:

- using a qcow2 VM image; see 11.3 “RHEL OS deployment in a VM” (p. 63)
- by manual package installation; see 11.6 “Manual RHEL OS installation requirements” (p. 71)

Before you attempt to install or upgrade an NSP server, see the *NSP Planning Guide*, which contains important information such as firewall port requirements and restrictions.

For information about using the NSP Lab Installer, the NSP qcow2 installation utility for lab or trial deployments, see the *NSP Lab Installer Reference*.

11.3 RHEL OS deployment in a VM

11.3.1 Description

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

After you deploy the image as described in 11.4 "To deploy the RHEL OS for NSP using a qcow2 image" (p. 63), you can install and upgrade the NSP server software in the VM.

Note: The OS installation includes all required and optional packages. See 11.6.3 "Required RHEL environment and OS packages" (p. 72) for a list of the required and optional packages.

11.4 To deploy the RHEL OS for NSP using a qcow2 image

11.4.1 Purpose

This procedure describes how to create one or more RHEL OS instances for the installation of NSP servers.

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

11.4.2 Steps

Prepare required images

1

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

2

Download the following file from OLCS to a local directory on the station:

- NSP_RHEL7_*yy_mm*.qcow2

where *yy_mm* represents the year and month of the file issue

3

Open a console window.

4

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

5

Perform one of the following:

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

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

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

where

raw_image is the raw disk image name specified in Step 4

size is the required disk size, in Gbytes

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

For 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 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

6

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

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

For each disk image created in Step 5 that you want to convert to non-sparse format, enter the following:

```
# cp --sparse=never raw_image.img non-sparse_raw_image.img ↲
```

raw_image is a raw disk image name specified in Step 5

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

Deploy VMs

7

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

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

--disk path="*image_n*", device=disk,bus=virtio,format=raw,io=native, cache=none --network bridge=*bridge_name* --import ↵

where

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

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

instance is the name to assign to the VM

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

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

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

8

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

9

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

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

Note: The /etc/hosts file on each NSP server must contain entries for the NFM-P main servers if the integrated NFM-P is configured to use hostnames (and not public-ip), and if DNS is not used. NFM-P systems use hostnames by default.

10

Perform one of the following; see Chapter 10, "NSP disk partitioning" for specific disk partitioning information.

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

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

1. Enter the following commands:

   # **mkdir -p /extra** ↵

   # **mkdir -p /opt/nsp** ↵

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

- /var/log/audit

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

```
# fdisk /dev/virtual_device ↵
```

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

3. Enter the following to reboot the VM:

```
# systemctl reboot ↵
```

4. After the reboot, perform one of the following.
   a. If you are using LVM, perform the following steps.
      1. Enter the following sequence of commands for each sub-disk:

```
# pvcreate /dev/virtual_devicen ↵
# vgcreate vg2 /dev/virtual_devicen ↵
```

      where
      virtual_device is the virtual device name, for example, vda in a KVM VM
      n is the number associated with the sub-disk
      2. Go to Step 11.
   b. If you are not using LVM, perform the following steps.
      1. Enter the following for each sub-disk:

```
# mkfs.ext4 -L path /dev/devicen ↵
```

      where
      path is the directory path associated with the sub-disk, for example, /opt/nsp
      device is the device name, for example, vda in a KVM VM
      n is the device number associated with the sub-disk
      2. Open the /etc/fstab file using a plain-text editor such as vi.
      3. Add one line in the following format for each sub-disk:

```
/dev/virtual_devicen  path   fs_type   defaults        0 0
```

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

```
# mount -a ↵
```

      6. Go to Step 12.

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

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

where

device is the device name for the disk

group is the name to assign to the volume group, and must be unique in the VM

Configure LVM

11

Create the LVM volumes and partitions.

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

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

1. Enter the following to create a logical volume:

   # **lvcreate -n *volume* -L *size*G *group* /dev/*device*** ↵

   where

   volume is the name to assign to the logical volume

   size is the volume size from your Platform Sizing Response

   group is the name to assign to the volume group, and must be unique in the VM

   device is the device name

2. Enter the following:

   # **mkdir *directory*** ↵

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

3. Enter the following:

   # **mkfs.ext4 -L *directory* /dev/*group*/*volume*** ↵

   where

   directory is the directory associated with the volume

   group is the volume group

   volume is the logical volume name

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

5. Add an entry in the following format:

   /dev/*group*/*partition directory fs_type* noatime 0 0

   where

   group is the volume group

   partition is the partition name

   directory is the associated directory path

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

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

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

   # **mount -a** ↵

Install and configure product software

12

Install and configure the NSP server software on the VMs.

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

END OF STEPS

11.5 To apply an NSP RHEL qcow2 OS update

11.5.1 Description

If you are upgrading the NSP in a VM created using the NSP RHEL OS qcow2 image described in 11.4 “To deploy the RHEL OS for NSP using a qcow2 image” (p. 64), you must apply a RHEL update to the OS before you can upgrade the component.

Note: The procedure applies only to a VM OS deployed using the NSP RHEL OS qcow2 image.

Note: If required, you can roll back an applied update by using the ‘yum history’ command to do the following.

1. Obtain the yum transaction ID.
2. Undo the transaction.

See the RHEL OS documentation for more information.

11.5.2 Steps

1

Log in to the NSP server station as the root user.

2

Open a console window.

3

Enter the following to stop the NSP server:

nspdctl stop ↵

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*_QCOW2_UPDATE_*yy_mm*.tar.gz

where

n is the major RHEL version, for example, 7

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_QCOW2_UPDATE_yy_mm.tar.gz ↵
```

The update files are extracted to the following directory:

/opt/OSUpdate/rhel*version-yy.mm.dd*

where

version is the RHEL version, for example, 7.5

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

8

Enter the following:

```
# cd rhelversion-yy.mm.dd ↵
```

9

Enter the following to install the update:

```
# yum install * ↵
```

10

If you are upgrading from Release 18.12 or earlier, perform the following steps.

1. Open the /etc/default/grub file using a plain-text editor such as vi.
2. Locate the following line:

   ```
   GRUB_CMDLINE_LINUX_DEFAULT="parameter_1 parameter_2...parameter_n
   nomodeset"
   ```

3. Remove the nomodeset parameter so that the line reads as follows:

GRUB_CMDLINE_LINUX_DEFAULT="*parameter_1 parameter_2...parameter_n*"

4. Enter the following:

   # **grub2-mkconfig -o /boot/grub2/grub.cfg** ↵

11

Enter the following:

systemctl reboot ↵

The station reboots.

12

After the reboot, remove the /opt/OSUpdate directory to conserve disk space.

13

Applying the update may leave outdated and inactive OS kernel instances on the station.

To remove any previous kernel instances, enter the following as the root user:

package-cleanup --oldkernels --count=1 ↵

14

Close the console window.

END OF STEPS

11.6 Manual RHEL OS installation requirements

11.6.1 Introduction

This section describes the manual installation of the RHEL OS for an NSP server.

Each NSP server requires the following:

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

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

Note: The RHEL SELinux function is not supported; you must disable this function before you attempt to install or upgrade any NSD or NRC module.

11.6.2 Using the yum utility

To simplify package management, Nokia recommends that you use the RHEL yum utility to install and remove OS packages.

The package installation syntax is the following:

yum -y install *package_1 package_2 ... package_n* ↵

The package removal syntax is the following:

yum -y remove *package_1 package_2 ... package_n* ↵

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

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

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

Note: If a package has dependencies on one or more additional packages that are not listed in the package documentation, the yum utility installs the additional packages.

11.6.3 Required RHEL environment and OS packages

During the RHEL OS installation for an NSP server, you must do the following.

1. Specify “Minimal Install” as the Software Selection in the RHEL installer.
2. Install specific OS packages, as described in 11.6.4 “RHEL OS packages to install” (p. 71).
3. Remove specific OS packages, as described in 11.6.5 “RHEL OS packages to remove” (p. 77).
4. Upgrade or install specific OS packages, as required, depending on the RHEL version; see 11.6.6 “Special RHEL OS package requirements” (p. 78).
5. Optionally, install one or more packages listed in 11.6.7 “Optional RHEL OS packages” (p. 84).

11.6.4 RHEL OS packages to install

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 on each station in an NSP system if you do not require the gnome desktop.

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

systemctl gdm stop ↵

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

systemctl disable gdm ↵

You must install a set of RHEL OS packages that are common to each NSP server. Most of the common packages are available from the RHEL ISO disk image and the default RHEL package repository. Such packages are listed in "Required packages, RHEL ISO image or default RHEL repository" (p. 72).

You must also install additional packages that are available only from the RHEL optional package repository. Such packages are listed in "Required packages, RHEL optional package repository" (p. 76).

Required packages, RHEL ISO image or default RHEL repository

The RHEL ISO image and default package repository each contain the following OS packages that you must install.

To facilitate the package installation, copy the following command block and paste it in a CLI:

```
yum -y install @base @gnome-desktop @legacy-x @x11
yum -y install autofs bc.x86_64 binutils.x86_64 compat-libcap1.x86_64
yum -y install dialog elfutils-libelf-devel.x86_64 elfutils.x86_64
yum -y install firefox.x86_64 ftp gcc.x86_64 gcc-c++.x86_64 glibc.i686
yum -y install glibc.x86_64 glibc-devel.i686 glibc-devel.x86_64
yum -y install gtk2.i686 haproxy.x86_64 hdparm.x86_64 irqbalance.x86_64
yum -y install keepalived.x86_64 keyutils-libs-devel.x86_64
yum -y install krb5-devel.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64
yum -y install libaio-devel.i686 libaio-devel.x86_64
yum -y install libcom_err-devel.x86_64 libffi-devel.x86_64 libgcc.i686
yum -y install libgcc.x86_64 libgcrypt-devel.x86_64
yum -y install libgpg-error-devel.x86_64 libibverbs.x86_64
yum -y install libkadm5.x86_64 libselinux-devel.x86_64
yum -y install libsepol-devel.x86_64 libstdc++.i686 libstdc++.x86_64
yum -y install libstdc++-devel.i686 libstdc++-devel.x86_64
yum -y install libverto-devel.x86_64 libXi.i686 libXi.x86_64
yum -y install libxml2-devel.x86_64 libxslt-devel.x86_64
yum -y install libXrender.i686 libXtst.i686 libXtst.x86_64 lshw.x86_64
yum -y install lsof.x86_64 make.x86_64 man mcelog net-snmp
yum -y install net-snmp-utils ntp numactl-devel.i686
yum -y install numactl-devel.x86_64 openssh.x86_64
yum -y install openssh-askpass.x86_64 openssh-clients.x86_64
yum -y install openssh-server.x86_64 openssl-devel.x86_64
yum -y install pcre-devel.x86_64 procps python-devel.x86_64
yum -y install rsync.x86_64 tcpdump.x86_64 unzip.x86_64 which
yum -y install xinetd.x86_64 xz-devel.x86_64 zip.x86_64
```

Table 11-1 Required OS packages from default RHEL repository or ISO image

Package	Description
@base	Base package group
@gnome-desktop	Gnome package group
@legacy-x	Legacy X package group

Table 11-1 Required OS packages from default RHEL repository or ISO image (continued)

Package	Description
@x11	X11 package group
autofs	A tool for automatically mounting and unmounting filesystems
bc.x86_64	GNU's bc (a numeric processing language) and dc (a calculator)
binutils.x86_64	A GNU collection of binary utilities
compat-libcap1.x86_64	Library for getting and setting POSIX.1e capabilities
dialog	A utility for creating TTY dialog boxes
elfutils.x86_64	A collection of utilities and DSOs to handle compiled objects
elfutils-libelf-devel.x86_64	Development support for libelf
firefox.x86_64	Mozilla Firefox web browser
ftp	The standard UNIX FTP client
gcc.x86_64	Various compilers, for example, C, C++, Objective-C, and Java
gcc-c++.x86_64	C++ support for GCC
glibc.i686	The GNU libc libraries
glibc.x86_64	The GNU libc libraries
glibc-devel.i686	Object files for development using standard C libraries
glibc-devel.x86_64	Object files for development using standard C libraries
gtk2.i686	The GIMP ToolKit (GTK+), a library for creating GUIs for X
haproxy.x86_64	TCP/HTTP proxy and load balancer for high availability environments
hdparm.x86_64	Utility for displaying and/or setting hard disk parameters
irqbalance.x86_64	Daemon that evenly distributes IRQ load across multiple CPUs
keepalived.x86_64	Load balancer and high availability service
keyutils-libs-devel.x86_64	Development package for building Linux key management utilities
krb5-devel.x86_64	Development files needed to compile Kerberos 5 programs
ksh.x86_64	The Original ATT Korn Shell
libaio.i686	Linux-native asynchronous I/O access library
libaio.x86_64	Linux-native asynchronous I/O access library
libaio-devel.i686	Development files for Linux-native asynchronous I/O access
libaio-devel.x86_64	Development files for Linux-native asynchronous I/O access
libcom_err-devel.x86_64	Common error description library
libffi-devel.x86_64	GCC development for FFI
libgcc.i686	GCC version 4.8 shared support library

Table 11-1 Required OS packages from default RHEL repository or ISO image (continued)

Package	Description
libgcc.x86_64	GCC version 4.4 shared support library
libgcrypt-devel.x86_64	Development files for the libgcrypt package
libgpg-error-devel.x86_64	Development files for the libgpg-error package
libibverbs.x86_64	Core user space library that implements hardware abstracted verbs protocol
libkadm5.x86_64	Kerberos 5 Administrative libraries
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++.i686	GNU Standard C++ Library
libstdc++.x86_64	GNU Standard C++ Library
libstdc++-devel.i686	Header files and libraries for C++ development
libstdc++-devel.x86_64	Header files and libraries for C++ development
libverto-devel.x86_64	Development files for libverto
libXi.i686	X.Org X11 libXi runtime library
libXi.x86_64	X.Org X11 libXi runtime library
libxml2-devel.x86_64	Libraries, includes, etc. to develop XML and HTML applications
libXrender.i686	X.Org X11 libXrender runtime library
libxslt-devel.x86_64	Development libraries and header files for libxslt
libXtst.i686	X.Org X11 libXtst runtime library
libXtst.x86_64	X.Org X11 libXtst runtime library
lshw.x86_64	Hardware lister
lsof.x86_64	Provides a utility to list information about open files
make.x86_64	GNU tool which simplifies the build process for users
man	A set of documentation tools: man, apropos and whatis
mcelog	Tool to translate x86-64 CPU Machine Check Exception data
net-snmp	SNMP Agent Daemon and documentation
net-snmp-utils	SNMP clients such as snmpget and snmpwalk
ntp	The NTP daemon and utilities
numactl-devel.i686	Development package for building Applications that use numa
numactl-devel.x86_64	Development package for building Applications that use numa
openssh.x86_64	Open source implementation of SSH protocol versions 1 and 2
openssh-askpass.x86_64	Passphrase dialog for OpenSSH and X

Table 11-1 Required OS packages from default RHEL repository or ISO image (continued)

Package	Description
openssh-clients.x86_64	Open-source SSH client application
openssh-server.x86_64	Open source SSH server daemon
openssl-devel.x86_64	Files for development of applications which will use OpenSSL
pcre-devel.x86_64	Development files for PCRE
procps	OS utilities for /proc
python-devel.x86_64	The libraries and header files needed for Python development
rsync.x86_64	A program for synchronizing files over a network
tcpdump.x86_64	Command-line packet analyzer and network traffic capture; used by technical support for debugging
unzip.x86_64	A utility for unpacking zip files
which	Displays where a particular program in your path is located
xinetd.x86_64	A secure replacement for inetd
xz-devel.x86_64	Development libraries and headers for liblzma
zip.x86_64	A file compression utility

Required packages, RHEL optional package repository

The RHEL optional package repository contains the OS packages listed in Table 11-2, “Required OS packages from RHEL optional package repository” (p. 76) that you must install.

To facilitate the package installation, copy the following command and paste it in a CLI:

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

Table 11-2 Required OS packages from RHEL optional package repository

Package name	Description
compat-libstdc++-33.i686	Compatibility standard C++ libraries
compat-libstdc++-33.x86_64	Compatibility standard C++ libraries

The package in Table 11-3, “Required OS package from RHEL optional package repository for Workflow Manager” (p. 77) is required if you intend to use the Workflow Manager application, and is not to be installed otherwise.

To facilitate the package installation, copy the following command and paste it in a CLI:

```
yum -y install libyaml-devel.x86_64
yum -y install python2-oauthlib socat
```

Table 11-3 Required OS package from RHEL optional package repository for Workflow Manager

Package name	Description
libyaml-devel.x86_64	Development files for LibYAML applications
python2-oauthlib	A Generic Implementation of the OAuth Request-Signing Logic
socat	Multipurpose relay for bidirectional data transfer

11.6.5 RHEL OS packages to remove

After you install the required OS packages on an NSP server station, you must remove packages that are installed by default but not required by the NSP.

For all RHEL 7 versions, you must remove the packages listed in Table 11-4, “RHEL OS packages to remove” (p. 77).

To facilitate the package removal, copy the following command block and paste it in a CLI:

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

Table 11-4 RHEL OS packages to remove

Package	Description
anaconda-core.x86_64	Core of the Anaconda installer
anaconda-gui.x86_64	Graphical user interface for the Anaconda installer
anaconda-tui.x86_64	Textual user interface for the Anaconda installer
avahi.x86_64	Local network service discovery
biosdevname	Utility that provides an optional convention for naming network interfaces
dnsmasq.x86_64	A lightweight DHCP/caching DNS server
gnome-boxes.x86_64	A simple GNOME 3 application to access remote or virtual systems

Table 11-4 RHEL OS packages to remove (continued)

Package	Description
initial-setup.x86_64	Initial system configuration utility
initial-setup-gui.x86_64	Graphical user interface for the initial-setup utility
libstoragemgmt.x86_64	Storage array management library
libstoragemgmt-python.noarch	Python2 client libraries and plug-in support for libstoragemgmt
libvirt-daemon-config-network.x86_64	Default configuration files for the libvirtd daemon
libvirt-daemon-driver-network.x86_64	Network driver plugin for the libvirtd daemon
libvirt-daemon-driver-qemu.x86_64	Qemu driver plugin for the libvirtd daemon
libvirt-daemon-kvm.x86_64	Server side daemon & driver required to run KVM guests
libvirt-gconfig.x86_64	libvirt object APIs for processing object configuration
libvirt-gobject.x86_64	libvirt object APIs for managing virtualization hosts
NetworkManager-libreswan.x86_64	NetworkManager VPN plugin for libreswan
NetworkManager-libreswan-gnome.x86_64	NetworkManager VPN plugin for libreswan - GNOME files
NetworkManager-team.x86_64	Team device plugin for NetworkManager
NetworkManager-tui.x86_64	NetworkManager curses-based UI
qemu-kvm.x86_64	QEMU metapackage for KVM support
qemu-kvm-common.x86_64	QEMU common files needed by all QEMU targets
setroubleshoot.x86_64	Helps troubleshoot SELinux problem
setroubleshoot-plugins.noarch	Analysis plugins for use with setroubleshoot
setroubleshoot-server.x86_64	SELinux troubleshoot server
subscription-manager-initial-setup-addon.x86_64	Initial setup screens for subscription manager

11.6.6 Special RHEL OS package requirements

An NSP server requires:

- specific versions of some packages; see “Special package version requirements, all RHEL versions” (p. 79)
- for RHEL 7.3 or 7.4, the removal of packages not listed in Table 11-4, “RHEL OS packages to remove” (p. 77); see “Special RHEL 7.3 or 7.4 package requirements” (p. 79)
- for RHEL 7.6, the installation or removal of specific packages, as described in “Special RHEL 7.6 package requirements” (p. 79)

Special package version requirements, all RHEL versions

An NSP server requires the version of each RHEL 7 package quoted in Table 11-5, “Required RHEL OS package versions” (p. 78), or a later version. After the initial OS installation, if a listed package version is lower than the minimum required, you must upgrade the package.

To facilitate the package upgrade, copy the following command block and paste it in a CLI:

```
yum -y install nspr.x86_64 nss-softokn-freebl.i686
yum -y install nss-softokn-freebl.x86_64 nss-softokn.x86_64
yum -y install nss-util.x86_64
```

Table 11-5 Required RHEL OS package versions

Package	Minimum version required
nspr.x86_64	4.19.0-1.el7
nss-softokn-freebl.i686	3.36.0-5.el7
nss-softokn-freebl.x86_64	3.36.0-5.el7
nss-softokn.x86_64	3.36.0-5.el7
nss-util.x86_64	3.36.0-1.el7

Special RHEL 7.3 or 7.4 package requirements

For RHEL 7.3 or 7.4, in addition to the packages listed in 11.6.5 “RHEL OS packages to remove” (p. 77), you must also remove the packages listed in Table 11-6, “OS packages to remove, RHEL 7.3 or 7.4” (p. 79).

To facilitate the package removal, copy the following command and paste it in a CLI:

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

Note: The packages are required by RHEL 7.5 and later because of a package dependency introduced in RHEL 7.5.

Table 11-6 OS packages to remove, RHEL 7.3 or 7.4

Package	Description
NetworkManager.x86_64	Network connection manager and user applications
NetworkManager-wifi.x86_64	Wifi plugin for NetworkManager

Special RHEL 7.6 package requirements

For RHEL 7.6, you must do the following:

- Install the packages listed in Table 11-7, “Additional OS packages, RHEL 7.6” (p. 80).
- Remove the packages listed in Table 11-8, “OS packages to remove, RHEL 7.6” (p. 81).

Table 11-7, “Additional OS packages, RHEL 7.6” (p. 79) lists the additional packages that you must install for RHEL 7.6.

To facilitate the package installation, copy the following command block and paste it in a CLI:

```
yum -y install bpftool c-ares gcc-gfortran hyphen-en
yum -y install javapackages-tools.noarch libcurl-devel.x86_64
yum -y install libgfortran libquadmath libquadmath-devel
yum -y install libverto-libevent libyaml-devel.x86_64 nfs-utils orca
yum -y install python-babel python-javapackages python-jinja2
yum -y install python-jsonpatch python-jsonpointer python-markupsafe
yum -y install python-paramiko python-pillow python-prettytable
yum -y install python-pygments python-requests python-urllib3
yum -y install python2-oauthlib socat tigervnc-server.x86_64
```

Table 11-7 Additional OS packages, RHEL 7.6

Package	Description
bpftool	Inspection and simple manipulation of eBPF programs and maps
c-ares	A library that performs asynchronous DNS operations
gcc-gfortran	Fortran 95 support for gcc
hyphen-en	English hyphenation rules
javapackages-tools.noarch	Macros and scripts for Java packaging support
libcurl-devel.x86_64	A Tool for Transferring Data from URLs
libgfortran	Fortran runtime
libquadmath	GCC __float128 shared support library
libquadmath-devel	GCC __float128 support
libverto-libevent	libevent module for libvert
libyaml-devel.x86_64	Development files for LibYAML applications
nfs-utils	NFS utilities and supporting clients and daemons for the kernel NFS server
orca	GNOME screen reader for people with visual impairments
python-babel	Internationalization utilities
python-javapackages	Module for handling various files for Java packaging
python-jinja2	Python template engine
python-jsonpatch	Apply JSON-Patches (RFC 6902)
python-jsonpointer	Identify specific nodes in a JSON document (RFC 6901)
python-markupsafe	XML/HTML/XHTML markup safe string package for Python
python-paramiko	SSH2 protocol library
python-pillow	Python image processing library

Table 11-7 Additional OS packages, RHEL 7.6 (continued)

Package	Description
python-prettytable	Python library for displaying data in ASCII table format
python-pygments	Syntax highlighting package written in Python
python-requests	Python HTTP for Humans
python-urllib3	HTTP library with thread-safe connection pooling, file post, and more
python2-oauthlib	A Generic Implementation of the OAuth Request-Signing Logic
socat	Multipurpose relay for bidirectional data transfer
tigervnc-server.x86_64	Server for the VNC remote display system

Table 11-8, “OS packages to remove, RHEL 7.6” (p. 81) lists the packages to remove from RHEL 7.6.

To facilitate the package removal, copy the following command block and paste it in a CLI:

```
yum -y remove anaconda-user-help anaconda-widgets audit-libs-python
yum -y remove checkpolicy cryptsetup-python cyrus-sasl
yum -y remove cyrus-sasl-gssapi daxctl-libs fcoe-utils glade-libs
yum -y remove glusterfs-cli gnome-initial-setup ipxe-roms-qemu
yum -y remove iscsi-initiator-utils iscsi-initiator-utils-iscsiuio
yum -y remove isomd5sum kernel-devel keybinder3 ldns
yum -y remove libblockdev-nvdimm libcgroup libconfig libgovirt
yum -y remove libnm-gtk librdmacm libreport-anaconda
yum -y remove libreport-plugin-bugzilla
yum -y remove libreport-rhel-anaconda-bugzilla libreswan
yum -y remove libsemanage-python libtimezonemap libuser-python
yum -y remove libverto-tevent lldpad mtools ndctl ndctl-libs
yum -y remove netcf-libs nmap-ncat numad oddjob oddjob-mkhomedir
yum -y remove policycoreutils-python pykickstart pyparted pyserial
yum -y remove python-blivet python-coverage python-di python-IPy
yum -y remove python-meh-gui python-nss python-ntplib
yum -y remove python-pwquality python-pyblock python2-blockdev
yum -y remove python2-subprocess32 pytz radvd realmd seabios-bin
yum -y remove seavgabios-bin setools-libs sgabios-bin spice-server
yum -y remove unbound-libs yajl
```

Table 11-8 OS packages to remove, RHEL 7.6

Package	Description
anaconda-user-help	Anaconda built-in help system
anaconda-widgets	A set of custom GTK+ widgets for use with anaconda
audit-libs-python	Python Bindings for libaudit
checkpolicy	SELinux policy compiler

Table 11-8 OS packages to remove, RHEL 7.6 (continued)

Package	Description
cryptsetup-python	Python bindings for libcryptsetup
cyrus-sasl	Implementation of Cyrus SASL API
cyrus-sasl-gssapi	Plugin for the GSSAPI SASL mechanism
daxctl-libs	Management library for "Device DAX" devices
fcoe-utils	FCoE userspace management tools
glade-libs	Widget library for Glade UI designer
glusterfs-cli	GlusterFS CLI
gnome-initial-setup	GNOME Initial Setup Assistant
ipxe-roms-qemu	Network boot loader roms supported by QEMU, .rom format
iscsi-initiator-utils	iSCSI daemon and utility programs
iscsi-initiator-utils-iscsiuio	Userspace configuration daemon required for some iSCSI hardware
isomd5sum	Utilities for working with md5sum implanted in ISO images
kernel-devel	Development files needed for building kernel modules
keybinder3	A library for registering global keyboard shortcuts
ldns	A library for developing the Domain Name System
libblockdev-nvdimm	The NVDIMM plugin for the libblockdev library
libcgroup	Library to control and monitor control groups
libconfig	C++ bindings development files for libconfig
libgovirt	A GObject library for interacting with oVirt REST API
libnm-gtk	Private libraries for NetworkManager GUI support
librdmacm	Userspace RDMA Connection Manager
libreport-anaconda	Default configuration for reporting anaconda bugs
libreport-plugin-bugzilla	libreport's bugzilla plugin
libreport-rhel-anaconda-bugzilla	Default configuration for reporting anaconda bugs to Red Hat Bugzilla
libreswan	IPsec implementation with IKEv1 and IKEv2 keying protocols
libsemanage-python	semanage python bindings for libsemanage
libtimezonemap	Time zone map widget for Gtk+
libuser-python	Python bindings for the libuser library
libverto-tevent	Python bindings for the libuser library
lldpad	Intel LLDP Agent
mtools	Tools to access MS-DOS filesystems without kernel drivers

Table 11-8 OS packages to remove, RHEL 7.6 (continued)

Package	Description
ndctl	Manage "libnvdimm" subsystem devices (Non-volatile Memory)
ndctl-libs	Management library for "libnvdimm" subsystem devices (Non-volatile Memory)
netcf-libs	Libraries for netcf
nmap-ncat	Nmap's Netcat replacement
numad	Userspace daemon that automatically binds workloads to NUMA node
oddjob	A D-Bus service which runs odd jobs on behalf of client applications
oddjob-mkhomedir	An oddjob helper which creates and populates home directories
policycoreutils-python	SELinux policy core python utilities
pykickstart	A python library for manipulating kickstart files
pyparted	Python module for GNU parted
pyserial	Python serial port access library
python-blivet	A python module for system storage configuration
python-coverage	Code coverage measurement for Python
python-di	Python library for dependency injection support
python-IPy	Class and Tools for Handling of IPv4 and IPv6 Addresses and Networks
python-meh-gui	Graphical user interface for the python-meh library
python-nss	Python bindings for Network Security Services (NSS)
python-ntplib	Python module that offers a simple interface to query NTP servers
python-pwquality	Library for password quality checking -- Python bindings
python-pyblock	Python modules for dealing with block devices
python2-blockdev	Python2 gobject-introspection bindings for libblockdev
python2-subprocess32	Backport of subprocess module from Python 3.2 to Python 2
pytz	World Timezone Definitions for Python
radvd	A Router Advertisement daemon
realmd	Kerberos realm enrollment service
seabios-bin	Seabios for x86
seavgabios-bin	Seavgabios for x86
setools-libs	Policy analysis support libraries for SELinux
sgabios-bin	Sgabios for x86
spice-server	Implements the server side of the SPICE protocol
unbound-libs	Libraries used by the unbound server and client applications

Table 11-8 OS packages to remove, RHEL 7.6 (continued)

Package	Description
yajl	Yet Another JSON Library Tools

11.6.7 Optional RHEL OS packages

Table 11-9, “Optional RHEL OS packages” (p. 84) lists the optional packages that you can install.

To facilitate the package installation, copy the following command and paste it in a CLI:

```
yum -y install nfs-utils
```

Table 11-9 Optional RHEL OS packages

Package	Description
nfs-utils	NFS utilities and supporting clients and daemons for the kernel

12 NSP communication and security

12.1 NSP inter-component and internal communication

12.1.1 Inter-component NSP communication

An NSP system employs various mechanisms and protocols for inter-component communication that are beyond the scope of system deployment. The material in this chapter focuses mainly on the deployment and initial configuration of NSP system security. For more information about NSP communication, see the *NSP Architecture Guide*.

Note: Communication between NSP components is performed using IPv4 only; IPv6 communication is not supported.

NFM-P, NFM-T, or other product or NSP module communication with the NSD and NRC is secured using TLS. Communication among the components in a module such as the NFM-P is also secured using TLS.

Note: The NSD and NRC modules use TLS 1.2; TLS 2.0 is not supported.

See 12.7 “NSP TLS configuration and management” (p. 90) for information about deploying TLS in an NSP system.

For information about NFM-P TLS deployment, see the *NSP NFM-P Installation and Upgrade Guide*.

Communication between the NSD and NRC modules and the NFM-T is performed using REST over HTTPS. For information about NFM-T TLS deployment, see the NFM-T product documentation.

12.1.2 Internal NSP communication

Transactional communication involving nspOS subsystems such as the ZooKeeper registry, Kafka notification system, and PostgreSQL database can also be secured using TLS in a Release 19.6 or later NSP system. TLS for nspOS is disabled by default for compatibility with system components at earlier releases.

Internal NSP communication is TLS-secured using an internally generated certificate signed by an internal CA. The use of an internal CA rather than a publicly trusted CA prevents intruder access to internal functions through the use of any other certificate.

Note: In order to enable nspOS security, all NSP modules, components, and integrated products must be at Release 19.6 or later.

Note: If all components of an NSP system are at Release 19.6 or later, enabling nspOS security is strongly recommended.

Note: Only unsecured connections are supported between NFM-T and ZooKeeper/Kafka.

See 13.3.2 “NSP component parameters” (p. 109) for information about enabling nspOS security.

12.1.3 NFM-P bandwidth requirement

The bandwidth requirement between the NFM-P and the NSP modules with which it communicates, such as the NRC-P and NSD, depends on the number of NEs, LSPs, and services in the NFM-P network, as well as the frequency of NE updates that are pushed to other modules.

Optimum performance during module re-synchronization with the NFM-P is attained when 50 Mb/s of bandwidth is available. Service provisioning operations typically require less bandwidth; Nokia recommends 25 Mb/s.

Network latency affects how long it takes to re-synchronize a large amount of data; Nokia recommends that the latency between components not exceed 100 ms.

12.1.4 NFM-T bandwidth requirement

The bandwidth requirement between the NFM-T and the NSP modules with which it communicates depends on the number of optical nodes and services in the NFM-T network.

Nokia recommends 10 Mbps of bandwidth between the NFM-T and the NSP. High round-trip network latency may affect GUI performance, and must not exceed 100 ms.

12.2 NSP user accounts

12.2.1 RHEL user accounts

The NSD and NRC modules require a RHEL user account called “nsp” in the nsp user group. The installation of a component such as the NSD and NRC, NRC-X, or MDM creates the group and account. The nsp user owns all NSP processes, and only the nsp user can start or stop a server. Server uninstallation does not remove the nsp user account, user group, or home directory.

The nsp home directory is /opt/nsp. The initial nsp password is randomly generated, and must be changed by the root user. Root user privileges are required only for component installation or upgrade, and for low-level support functions.

12.3 NSP user authentication

12.3.1 Description

For increased security, local NSP user authentication is not supported. The NSP requires an external authentication source that is specified during system installation. If the NSP system includes an NFM-P, the NFM-P may be used as an authentication source. Other external sources may also be defined, for example, RADIUS, LDAP, or TACACS+.

If the NSP system does not include an NFM-P, another external authentication source must be defined, or the NSP installation fails. See 13.3.3 “NSP SSO parameters” (p. 113) for configuration information.

For a shared-mode NSP system, 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.

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

Note: In an NSP deployment that does not include the NSD and NRC, it is best practice not to enable the Access Control function in the NSP User Manager application, as it unnecessarily duplicates the NFM-P user management function.

Access Control in the User Manager is disabled by default; see the *NSP System Administrator Guide* for configuration information.

Table 12-1, “NSP authentication source comparison” (p. 86) describes the advantages and disadvantages of various authentication sources.

Table 12-1 NSP 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. NSD/NRC users can continue to access the Launchpad and applications 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.	

12.4 NSP login security

12.4.1 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 defines the interval, in seconds, during which further login attempts by the user from the same source address are blocked, if the login threshold is exceeded.

See 13.3.3 “NSP SSO parameters” (p. 113) for information about the **login_throttling** parameters in the NSP configuration file.

12.4.2 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.

See 13.3.3 “NSP SSO parameters” (p. 113) for information about the **login_failure** parameters in the NSP configuration file.

12.5 To configure the NSP security statement

12.5.1 Purpose

Use this procedure to configure the security statement that is displayed on the NSP login page.

12.5.2 Steps

Preserve the system security statement

1

Perform the following steps if upgrading an NSP deployment that includes the NFM-P, and NSD and NRC, from an earlier release of NSP to NSP Release 17.3 or later.

Note: These steps do not have to be performed if upgrading from 5620 SAM Release 14.0 R7 to NSP Release 17.6 or later.

1. Copy the existing security statement from the NFM-P Java client.
2. Paste the copied statement into an empty file, and save the file in text format.
3. Copy the file to a secure location that is unaffected by the system upgrade activity.

Upgrade or install the NSD and NRC and start the nspOS

2

Perform one of the following:

a. Upgrade or install your standalone NSD and NRC system, as described in 14.2 “To install a standalone NSP server” (p. 121).

b. Upgrade or install your redundant NSD and NRC system, as described in 14.3 “To install a redundant NSP server” (p. 124).

3

Start the nspOS.

Configure the NSP security message

4

Log in to the NSP server as the admin user.

5

From the NSP Launchpad, go to More → Settings → NSP System Settings → Security Statement.

6

Perform one of the following:

a. Paste the security statement that was copied in Step 1.

b. Add the appropriate security statement.

Note: The security statement is not displayed the first time that the NSP login page is opened, but is displayed in subsequent sessions.

END OF STEPS

12.6 To suppress security warnings in NSP browser sessions

12.6.1 Description

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.

12.6.2 Steps

1

Perform one of the following.

a. If you deployed TLS using an NSP PKI server, transfer the ca.pem certificate file from the PKI server to each client station on which you want to suppress the browser warnings.

b. If you deployed TLS using the manual method, transfer your certificate file to each client station on which you want to suppress the browser warnings.

2

Perform one of the following.

a. Import the certificate to the certificate store of a client station OS.

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

Perform the appropriate procedure in the OS documentation to import the certificate; specify the certificate file as the certificate source.

Note: Such a procedure varies by OS type and version.

b. Import the certificate to the certificate store of a client browser.

Perform the appropriate procedure in the browser documentation to import the certificate; specify the certificate file as the certificate source.

Note: Such a procedure varies by browser type and version.

3

Open a browser session and verify that the required NSP applications open without the display of security warnings.

END OF STEPS

12.7 NSP TLS configuration and management

12.7.1 Automated TLS deployment using an NSP PKI server

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

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

Benefits of automated TLS deployment

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

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

See 12.8 “To configure and enable an NSP PKI server” (p. 91) for information about using an NSP PKI server to deploy TLS.

Functional description

The NSP PKI server is a standalone utility that implements TLS certificate signing requests, or CSRs, from requesting entities in an NSP system. A PKI server is available on a station to which you extract an NSP software package.

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

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

Note: The NSP messaging subsystems require a separate TLS certificate that is used internally. The certificate is generated and distributed automatically during an installation, or during an upgrade to Release 19.6 or later, and requires that the PKI server is running during the deployment operation. The separate internal certificate is required regardless of the TLS configuration method you choose for system-wide NSP communication.

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

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

For a PKI server to implement TLS on an NSP component, the component configuration must include the PKI server information.

If a PKI server is specified:

- but no keystore and truststore files are specified, the PKI server generates a TLS certificate using the specified alias, which is mandatory
- but no keystore and truststore passwords are specified, the default password, which is available from technical support, is used

12.8 To configure and enable an NSP PKI server

12.8.1 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 the PKI server for distribution to requestors

After you perform the procedure, the PKI server:

- creates a local private root CA service
- generates a TLS certificate and uses the CA service to sign it, or imports a certificate
- polls for certificate requests

- distributes the certificate to each requestor

Note: You require root user privileges on a station.

12.8.2 Steps

1

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

NSP_installer_directory/tools/pki

where *NSP_installer_directory* is the directory where the NSP software package was extracted

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

2

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

3

Open a console window.

4

Navigate to the directory that contains the pki-server file. The default installation location is:

NSP_installer_directory/tools/pki

where *NSP_installer_directory* is the directory where the NSP software package was extracted

5

If you have a set of signed certificate files that you want the PKI server to import and distribute to requestors, copy the files to the directory that contains the pki-server file. The files must be named:

- ca.key — private RSA key of the CA
- ca.pem — X.509 public key certificate signed using ca.key

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

6

Perform one of the following.

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

```
# ./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 you are importing a certificate, as described in Step 5, or have previously configured the root CA parameters for the PKI server, go to Step 21.

8

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]?
```

9

Enter y ↵. The following prompt is displayed:

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

10

Enter your company name.

The following prompt is displayed:

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

11

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

The following prompt is displayed:

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

12

Enter your state or province name.

The following prompt is displayed:

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

13

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.
```

14

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 21.

```
**********************************************************************************
No Internal Root CA detected on the filesystem.
**********************************************************************************
Creating new Internal Root CA Identity.
```

15

The following prompt is displayed:

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

16

Enter your company name.

The following prompt is displayed:

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

17

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

The following prompt is displayed:

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

18

Enter your state or province name.

The following prompt is displayed:

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

19

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
```

20

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

21

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*]

22

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.

23

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 modules 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.

24

Close the console window.

END OF STEPS

12.9 To migrate to the NSP PKI server

12.9.1 Purpose

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

Note: This procedure should only be used if all modules in the existing deployment were configured using the deprecated ROOT CA method.

12.9.2 Steps

1

Copy over the 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 'MyStorepassword' -deststorepass 'MyStorepassword'
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 package 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

Start the PKI server. Execute:

```
./pki-server
```

Note: The PKI server now uses the existing certificates within the file system. If ca.key and ca.pem files are not added as directed, the PKI server creates new files.

END OF STEPS

12.10 To enable TLS communication to the NFM-T using a custom certificate

12.10.1 Purpose

Use this procedure to enable TLS communication to an NFM-T system using a custom TLS certificate.

12.10.2 Steps

1

Retrieve the server.crt file from the */usr/Systems/Global_Instance/APACHE/conf/tls.crt* directory on the NFM-T server.

2

Place the server.crt file in the *NSP_installer_directory*/tls/nfmt directory, where *NSP_installer_directory* is the directory where the NSP software package was extracted.

END OF STEPS

12.11 To manually generate a TLS keystore

12.11.1 Purpose

A TLS keystore provides identity verification and encryption on all northbound and internal interfaces. You can manually generate a keystore file for distribution and use in an NSP system.

You can use the Java keytool utility to generate a TLS keystore file that contains a self-signed security certificate. The keytool utility is included in each Java Development Kit, or JDK, and Java Runtime Environment, or JRE.

Note: The keytool utility that you use must be from the Java version that the NSP uses. After an NSP server installation, you can find the keytool utility in /opt/nsp/os/jre/bin on the server. If the NSP is not yet installed, ensure that you use the keytool utility from the supported Java version specified in the *NSP Planning Guide*.

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

12.11.2 Steps

1

Enter the following:

Note: You must enclose a password that contains a special character in single quotation marks; for example:
-keypass 'Mypassword' -storepass 'Mypassword'

path*/keytool -genkeypair -keystore *filename* -keypass *keyPassword* -storepass *storePassword* -keyalg rsa -alias *aliasName* -dname "CN=*commonName*, OU=*organizationalUnit*, O=*organization*, L=*location*, ST=*state*, C=*country*" -validity 7300 -ext bc=ca:true -ext san=*sanString ↵

where

path is the path to the keytool utility

filename is the absolute path to the Java KeyStore file that will hold the public/private key pair that is generated

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

storePassword is the password to access the contents of the keystore

aliasName is the human-readable identifier for the key pair that is used to differentiate between different keys in a keystore

commonName is the name of the keystore owner

organizationalUnit is the name of the organizational unit to which the keystore owner belongs

organization is the name of the organization to which the keystore owner belongs

location is the name of the city in which the keystore owner resides

state is the name of the state or province in which the keystore owner resides

country is the name of the country in which the keystore owner resides

sanString is a list of all interfaces on the NSP server(s), prefixed with the “IP:” string. This list must contain the loopback (127.0.0.1) interface. For example, a redundant NSP deployment with two servers having the IP addresses 10.0.0.1 and 10.0.0.2 would use: -ext san=IP:127.0.0.1,IP:10.0.0.1,IP:10.0.0.2. If hostnames were used during installation, they must be included, prefixed with the “DNS:” string. For example, -ext san=IP:127.0.0.1,DNS:*hostname*.nokia.com.

2

Use the custom_keystore_path parameter, under the TLS section, to point to the generated keystore file. You should also set the other TLS values to match the parameters specified in the preceding command.

END OF STEPS

12.12 To enable TLS communication with the NFM-P using a non-custom certificate

12.12.1 Purpose

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

12.12.2 Steps

1

Retrieve the cacerts.trustStore file from the */opt/nsp/nfmp/server/nms/config/tls/trustStore/* directory on the NFM-P server.

2

Extract the certificate from the trustStore using the Java keytool utility. Execute the following command:

/opt/nsp/os/jre/bin/keytool keytool -exportcert -keystore cacerts.trustStore -alias *certAlias* -storepass *truststorePassword* -rfc -file nfmp.pem ↵

where

certAlias is the alias of the certificate in the NFM-P trustStore

truststorePassword is the password for the trustStore container

3

Place the generated nfmp.pem file in the *NSP_installer_directory*tls/nfmp directory, where *NSP_installer_directory* is the directory where the NSP software package was extracted.

END OF STEPS

13 NSP deployment configuration

13.1 Introduction

13.1.1 Description

This chapter describes how to create the following files that are required for deploying one or more NSP components:

- NSP hosts file—see 13.2 “NSP hosts file” (p. 101)
- NSP configuration file—see 13.3 “NSP configuration file” (p. 108)

Note: If you specify a server hostname in the NSP configuration file, and add an entry for the same server in the NSP hosts file, you must specify the hostname, and not the server IP address, in the NSP hosts file.

13.2 NSP hosts file

13.2.1 Description

The NSP hosts file specifies the addresses of the NSP servers that are to host the deployed components. Depending on the deployment, you must configure one or more of the sections in the file.

Note: An example hosts file is in the following directory:
NSP_installer_directory/NSD_NRC_*R_r*/examples
It is strongly recommended to use a modified copy of the example hosts file for installation.

Note: A hosts file section for a system element begins with an [*element*] tag, for example, [nspos]. Section tags for optional elements may be preceded by a # character, for example, #[fcc], which directs the NSP installer to skip the section and not deploy the element.
In order to enable the deployment of a system element, you must remove the leading # character from the section tag.

Table 13-1 NSP hosts file sections and parameters

Deployed component	Required hosts file entry
nspOS + common applications (standalone)	**`[nspos]`** ***`IPaddress`*** where *IPaddress* is the IP address of the server that is to host the nspOS software; in a NAT environment, the private IP address

Table 13-1 NSP hosts file sections and parameters (continued)

Deployed component	Required hosts file entry
NSD + NRC-P (standalone)	**[nspos]** ***IPaddress*** **[sdn]** ***IPaddress*** **sros="{'ip':'*VSR-NRCaddress*', 'router_id':'*VSR-NRCrouterID*'}"** where *IPaddress* is the IP address of the server where the NSD and NRC software will be installed. This should be the same server where the nspOS software will be installed. *VSR-NRCaddress* is the IP address of the VSR-NRC with which the NSD and NRC modules will communicate *VSR-NRCrouterID* is the router ID of the VSR-NRC with which the NSD and NRC modules will communicate
NSD + NRC-P (standalone) with collocated WFM **This configuration is for lab or trial deployments only**	**[nspos]** ***IPaddress*** **[sdn]** ***IPaddress*** **sros="{'ip':'*VSR-NRCaddress*', 'router_id':'*VSR-NRCrouterID*'}"** **[wfm]** ***IPaddress*** **advertised_address = *advertised address*** where *IPaddress* is the IP address of the server where the nspOS software will be installed. This should be the same server where the NSD and NRC software, and the WFM application will be installed. *VSR-NRCaddress* is the IP address of the VSR-NRC with which the NSD and NRC modules will communicate *VSR-NRCrouterID* is the router ID of the VSR-NRC with which the NSD and NRC modules will communicate *advertised address* is the advertised IP address of the server where the WFM software will be installed

Table 13-1 NSP hosts file sections and parameters (continued)

Deployed component	Required hosts file entry
NSD + NRC-P (standalone) with distributed WFM	**[nspos]** ***IPaddress*** **[sdn]** ***IPaddress*** **sros="{'ip':'*VSR-NRCaddress*', 'router_id':'*VSR-NRCrouterID*'}"** **[wfm]** ***WFM_IPaddress*** **advertised_address =** ***advertised address*** where *IPaddress* is the IP address of the server where the nspOS software will be installed. This should be the same server where the NSD and NRC software will be installed. *VSR-NRCaddress* is the IP address of the VSR-NRC with which the NSD and NRC modules will communicate *VSR-NRCrouterID* is the router ID of the VSR-NRC with which the NSD and NRC modules will communicate *WFM_IPaddress* is the IP address of the server where the WFM application will be installed *advertised address* is the advertised IP address for the server where the WFM application will be installed
NRC-X (standalone)	**[nrcx]** ***IPaddress*** where *IPaddress* is the IP address of the server where the NRC-X software will be installed.
Datacenters (1+1 redundancy deployments)	**[datacenter1_name]** **dc1_member_address** **[datacenter2_name]** **dc2_member_address** **[datacenter1_name:vars]** dc=*location1* **[datacenter2_name:vars]** dc=*location2* where *datacenter1_name* is the unique name of the primary server *dc1_member_address* is the IP address of the primary server *location1* is the datacenter in which the primary server resides *datacenter2_name* is the unique name of the standby server *dc2_member_address* is the IP address of the standby server *location2* is the datacenter in which the standby server resides

Table 13-1 NSP hosts file sections and parameters (continued)

Deployed component	Required hosts file entry
nspOS + common applications (1+1 redundancy)	**[nspos:children]** **datacenter1_name** **datacenter2_name** where *datacenter1_name* is the unique name of the primary server *datacenter2_name* is the unique name of the standby server
NSD + NRC-P (1+1 redundancy)	**[sdn]** **<primary server address> dc=<location> sros="{'ip':'<VSR-NRC address>';'router_id':'<VSR-NRC ID>'}"** **<standby server address> dc=<location> sros="{'ip':'<VSR-NRC address>';'router_id':'<VSR-NRC ID>'}"** where *primary server address* is the IP address of the primary server where the NSD and NRC software resides. This should be the same primary server where the nspOS software resides. *location* is the datacenter in which the server resides. This string must be unique to each server in the redundant deployment. *VSR-NRC address* is the IP address of the VSR-NRC with which the server will communicate. This can be the same, or unique, for each NSD and NRC server. *VSR-NRC ID* is the router ID of the VSR-NRC with which the server will communicate. This can be the same, or unique, for each NSD and NRC server. *standby server address* is the IP address of the standby server where the NSD and NRC software resides. This should be the same standby server where the nspOS software resides.
NSD + NRC-P (1+1 redundancy) with collocated WFM **This configuration is for lab or trial deployments only**	**[nspos:children]** **datacenter1_name** **datacenter2_name** **[sdn:children]** **datacenter1_name** **datacenter2_name** **[wfm:children]** **datacenter1_name** **datacenter2_name** where *datacenter1_name* is the unique name of the primary server *datacenter2_name* is the unique name of the standby server

Table 13-1 NSP hosts file sections and parameters (continued)

Deployed component	Required hosts file entry
NSD + NRC-P (1+1 redundancy) with distributed WFM	**[nspos:children]** **datacenter1_name** **datacenter2_name** **[sdn:children]** **datacenter1_name** **datacenter2_name** **[wfm:children]** **datacenter3_name** **datacenter4_name** where *datacenter1_name* is the unique name of the primary nspOS/NSD and NRC server *datacenter2_name* is the unique name of the standby nspOS/NSD and NRC server *datacenter3_name* is the unique name of the primary WFM server *datacenter4_name* is the unique name of the standby WFM server
NRC-X (1+1 redundancy)	**[nrcx]** **datacenter1_name** **datacenter2_name** where *datacenter1_name* is the unique name of the primary server *datacenter2_name* is the unique name of the standby server

Table 13-1 NSP hosts file sections and parameters (continued)

Deployed component	Required hosts file entry
Datacenters (3+3 redundancy)	**[datacenter1_name]** **dc1_member1_address** **dc1_member2_address** **dc1_member3_address** **[datacenter2_name]** **dc2_member1_address** **dc2_member2_address** **dc2_member3_address** **[datacenter1_name:vars]** **vip=datacenter1_vip** **dc=location1** **virtual_router_id=id1** **[datacenter2_name:vars]** **vip=datacenter2_vip** **dc=location2** **virtual_router_id=id2** where *datacenter1_name* is the unique name of the first HA cluster *dc1_member1_address*, *dc1_member2_address*, and *dc1_member3_address* are the IP addresses of the members of the first HA cluster *datacenter2_name* is the unique name for the second HA cluster *dc2_member1_address*, *dc2_member2_address*, and *dc2_member3_address* are the IP addresses of the members of the second HA cluster *datacenter1_vip* is the VIP address of the first HA cluster *location_1* is the datacenter in which the first HA cluster resides *id1* is the virtual router ID of the first HA cluster *datacenter2_vip* is the VIP address of the second HA cluster *location_2* is the datacenter in which the second HA cluster resides *id2* is the virtual router ID of the second HA cluster
NSD + NRC-P (3+3 redundancy)	**[sdn:children]** **datacenter1_name** **datacenter2_name** where *datacenter1_name* is the unique name of the first HA cluster *datacenter2_name* is the unique name for the second HA cluster

Table 13-1 NSP hosts file sections and parameters (continued)

Deployed component	Required hosts file entry
MDM	**[mdm]** ***ip address1*** ***ip address2*** ***[...]*** ***ip address_x*** where *ip address1*, *ip address2*, and *ip address_x* are the IP addresses of the MDM servers. You can deploy a standalone MDM instance or a highly available MDM server cluster.
NSP Flow Collector Controller	**[fcc]** Add one line like the following for each NSP Flow Collector Controller to install; specify one address for a standalone deployment, and two for a redundant deployment: ***ip_address* advertised_address=*advertised_address* ansible_host=*ansible_host*** where *ip_address* 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. *advertised_address* is the NSP Flow Collector Controller IP address that is reachable by each NSP Flow Collector; in a NAT environment: • If the Flow Collector Controller and all Flow Collectors are on the same side of the NAT firewall, the private IP address is typically required. • If the Flow Collector Controller and all Flow Collectors are separated by the NAT firewall, the public IP address is typically required. • If some Flow Collectors are inside, and some outside the NAT firewall, the public IP address is required, and the network must allow access to the Flow Collector Controller public address from inside the firewall. *ansible_host* is the NSP Flow Collector Controller IP address that is reachable from the station on which the NSP installer is run; typically the public IP address in a NAT environment

Table 13-1 NSP hosts file sections and parameters (continued)

Deployed component	Required hosts file entry
NSP Flow Collector	**[fc]** Add one line like the following for each NSP Flow Collector to install: ***ip_address* ansible_host=*ansible_host* fc_mode=*mode*** where *ip_address* is the NSP Flow Collector IP address; in a NAT environment, specify the private IP address *ansible_host* is the NSP Flow Collector IP address that is reachable from the station on which the NSP installer is run; typically the public IP address in a NAT environment *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 and PGW-EDR records • SYS—enables the collection of IPFIX system Cflowd and Netflow v5 records

13.3 NSP configuration file

13.3.1 Description

The NSP configuration file, which specifies the NSP deployment criteria, includes the following:

- component-specific parameters
- SSO parameters that apply to the entire NSP system

The SSO section of the configuration file specifies the NSP remote user authentication sources, for example, RADIUS, LDAP, or the NFM-P.

Based on your requirements, you must edit the sections of the configuration file 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.

To reduce complexity, the installation and SSO parameters are listed and described in separate tables; see the following for information:

- 13.3.2 “NSP component parameters” (p. 109)
- 13.3.3 “NSP SSO parameters” (p. 113)

A line in the file that begins with ## is a comment line, and is not to be modified. A line that begins with # is configurable.

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.

NFM-T manual installation

If the install parameter in the **nfmt** section of the configuration file is set to false, the NSP cannot integrate with the NFM-T, and the oms-server.conf file must be used instead. The file is populated as follows:

```
oms {
    OMSServers=[ {
        id="<nfmt id>"
        OMSMain={
            host="<primary address>"
            host2="<standby address>"
            username="<username>"
            password="<password>"
        }
    } ]
    tls-enabled="<tls enabled>"
    tls-directory="<tls directory>"
}
```

where

nfmt id is the unique identifier for the NFM-T system

primary address is the IP address of the standalone NFM-T server, or the primary NFM-T server in a redundant deployment

standby address is the IP address of standby NFM-T server in a redundant deployment

username is the username used when logging in to the NFM-T server

password is the password used when logging in to the NFM-T server

tls enabled specifies whether TLS security is enabled for the NFM-T server, true or false

tls directory specifies the directory in which TLS certificates are stored, if TLS security is enabled

13.3.2 NSP component parameters

Table 13-2, “Component parameters, NSP configuration file” (p. 110) lists and describes the NSP configuration-file sections and parameters that are specific to the components of an NSP deployment.

Note: If you are deploying the VSR-NRC, the VSR-NRC specified by the IP address and router ID in the **sros** section of the configuration file must be configured as described in 14.13 “To configure the VSR-NRC” (p. 154).

Note: If you are deploying the NRC-T, the primary and standby IP addresses in the **nrct** section of the configuration file must match the addresses in the **nfmt** section.

Table 13-2 Component parameters, NSP configuration file

Section and parameters	Description	
auto_start	Whether NSP starts automatically after installation Default: true	
nspos — inter-component communication parameters		
rest	System-wide REST parameters	
session	ttlInMins	REST token time to live, in minutes Default: 60
	maxNumber	Maximum number of concurrent REST session tokens Default: 50
secure	Whether internal service communication between NSP components is secured using TLS You can set the parameter to true only if the NSP system does not include the NFM-T, and all NSP components are at Release 19.6 or later. Default: false	
tls — TLS parameters		
pki_server	PKI server IP address or hostname Default: none	
pki_server_port	PKI server port Default: 2391	
pki_org	Organization name for TLS certificate Default: Nokia	
pki_cn	Common name for TLS certificate Default: NSP	
custom_keystore_path	If you are providing custom TLS keystore, keystore path and filename Default: none	
custom_truststore_path	If you are providing custom TLS truststore, truststore path and filename Default: none	
custom_keystore_password	If you are providing custom TLS keystore, keystore password Default: none	

Table 13-2 Component parameters, NSP configuration file (continued)

Section and parameters	Description
custom_truststore_password	If you are providing custom TLS truststore, truststore password Default: none
custom_key_alias	If you are providing custom TLS keystore, alias of required key in keystore Default: alias
regenerate_certs	Whether to force TLS certificate regeneration Default: true
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 all NSP components are at Release 19.6 or later, and the NSP system is not integrated with the NFM-T. Default: false
cert_provided	Whether custom TLS certificate to be used for communication with NFM-P Default: false
resync_augmentation_scripts_path	Path to scripts that augment NFM-P resynchronization in NSD Default: /opt/nsp/configure/nfmpResyncAugmentationScripts
nfmt — NFM-T integration parameters	
primary_ip	IP address of primary NFM-T server Default: —
standby_ip	IP address of standby NFM-T server Default: none
username	Username for NFM-T access Default: none
password	Password for NFM-T access Default: none
cert_provided	Whether custom TLS certificate used for NFM-T communication Default: false
nrcf — NRC-P OpenFlow controller parameters	
tca	Threshold-crossing alarm parameters
enabled	Whether TCAs are to be sent to NRC-P Default: true
bgp	BGP parameters; requires NFM-P and CPAA

Table 13-2 Component parameters, NSP configuration file (continued)

Section and parameters	Description
cpaa_as_number	CPAA AS number Default: 65030
nrct — NRC-T integration parameters	
primary_ip	IP address of primary NRC-T server Default: none
standby_ip	IP address of standby NRC-T server Default: none
remote	Indicates to NRC-X that NRC-T server is part of different nspOs authentication realm Default: false
username	Username for authentication by NRC-T in remote authentication realm; required when remote parameter set to true Default: none
password	Password for authentication by NRC-T in remote authentication realm; required when remote parameter set to true Default: none
mdm — MDM customization parameters	
adaptor_directory	Optional local directory on NSP server that contains adaptor RPMs or adaptor Karaf kar files for import to MDM servers
aggregation_model_definitions	Optional local directory or .zip file on NSP server that contains aggregation-model definition .yang files
repository	Optional Maven repository URL for resolving feature artifacts
device_admin	NE control customizations for MDM
scheduler_pool_size	Worker pool size for NE discovery Default: 7
discovery_scan_period_in_mins	How often network is scanned, in minutes Default: 5
fault_tolerance	Number of offline MDM servers tolerated; if not exceeded, MDM system remains operational The value must not exceed half the number of MDM servers. Default: 1
ean — external application notification parameters	
max_subscribers	Maximum number of subscribers that receive external application notifications Default: 10
auxdb — NFM-P auxiliary database parameters; required when collected data from components such as MDM or NSP Flow Collectors is to be stored in auxiliary database	

Table 13-2 Component parameters, NSP configuration file (continued)

Section and parameters	Description
enabled	Whether NSP system includes auxiliary database Default: false
ip-list	Comma-separated list of auxiliary database station IP addresses accessible to the NSP Default: none

13.3.3 NSP SSO parameters

Table 13-3, “SSO parameters, NSP configuration file” (p. 113) lists and describes the parameters in the **sso** section of the NSP configuration file.

See 12.4 “NSP login security” (p. 87) for information about how the NSP manages login attempts using the parameters in the **throttling** and **login_failure** sections.

Note: TLS certificates for secure LDAP communication must be copied to the /tls/ldap directory in the NSP installation directory. If an LDAP certificate contains an IP address or hostname in the SAN field, the same IP address or hostname must be used in the config.yml file.

Note: The NSP configuration file determines the user authentication sources that will be used. If the “primary_ip” parameter in the **nfmp** section of the configuration file specifies an NFM-P system, that NFM-P system will be used as an authentication source by default. If “primary_ip” parameter in the **nfmp** section of the configuration file does not specify an NFM-P system, then another external authentication source must be specified (such as LDAP, RADIUS, or TACACS+) or the installation will fail. The external authentication source must have an account with administrator privilege to NSP (“admin” user group by default).

Table 13-3 SSO parameters, NSP configuration file

Section and parameters	Description
session — general user session parameters	
concurrent_limits_enabled	Whether a maximum concurrent session limit is enabled Default: true
max_sessions_per_user	Maximum number of concurrent sessions per user - does not apply to admin group Default: 10
max_sessions_for_admin	Maximum number of concurrent sessions for users in admin group Default: 10
nfmp — NFM-P authentication parameters	
enabled	Whether NFM-P is to perform user authentication Default: true

Table 13-3 SSO parameters, NSP configuration file (continued)

Section and parameters			Description
realms			Optional NFM-P realm list; specify a realm using the parameters below
	realm		NFM-P authentication realm name Default: sam
	display_name		Realm name to display Default: NFM-P 1
ldap — LDAP parameters			
enabled			Whether LDAP is to be used for authentication Default: true
servers			List of LDAP servers; specify a server using the parameters below
	type		LDAP server type Default: AUTHENTICATION/AD/ANONYMOUS
	url		LDAP server URL with IP address or hostname and port Default: —
	security		Type of LDAP server security Default: SSL/STARTTLS/NONE
	timeout		Timeout period, in seconds, for receiving an authentication response Default: 10
	user_base_dn		User base dn value Default: *example_only*
	user_filter		Filter criteria for username Default: *example_only*
	group_base_dn		Group base dn value Default: *example_only*
	group_search		Custom group search options
		filter	Group search filter criteria Default: *example_only*
		attribute_id	Group search attribute on which to filter Default: *example_only*
	bind		LDAP bind credentials for authenticated access only
		dn	User with authority to bind to LDAP server Default: *example_only*

Table 13-3 SSO parameters, NSP configuration file (continued)

Section and parameters	Description	
	credential	Password for bind user **Note:** The password must be enclosed in double quotation marks. Default: *example_only*
min_pool_size	Minimum pool size Default: 0	
max_pool_size	Maximum pool size Default: 10	
use_entry_resolver	Whether an entry resolver is to be used for extracting additional user information Default: *example_only*	
radius — RADIUS parameters		
enabled	Whether RADIUS is to be used for authentication Default: none	
address	Comma-separated list of RADIUS servers Default: none	
secret	Shared server secret **Note:** The shared secret value must be enclosed in double quotation marks. Default: nonw	
protocol	Protocol to use—PAP or CHAP Default: none	
retries	Maximum number of attempts to reach server Default: 3	
timeout	Timeout, in seconds, for attempts to reach RADIUS server Default: 60	
failover_on_exception	Whether second server is tried if first server fails with exception Default: none	
failover_on_rejection	Whether second server is tried if first server fails with rejection Default: none	
authentication_port	RADIUS port Default: 1812	
vendor_id	Vendor ID for VSA search Default: 123	
role_VSA_id	VSA ID used to identify group Default: 3	
tacacs — TACACS+ parameters		

Table 13-3 SSO parameters, NSP configuration file (continued)

Section and parameters	Description
enabled	Whether TACACS+ authentication is to be used Default: none
address	Comma-separated list of TACACS+ servers Default: none
secret	Shared server secret **Note:** The shared secret must be enclosed in double quotation marks. Default: none
protocol	Protocol to use Default: PAP
timeout	Timeout, in seconds, for attempts to reach TACACS+ server Default: 7
failover_on_exception	Whether second server is tried if first server fails with exception Default: none
failover_on_rejection	Whether second server is tried if first server fails with rejection Default: none
authentication_port	TACACS+ port Default: 49
default_group	Default group to assign if no group defined on server Default: none
VSA_enabled	Whether VSA search is enabled Default: true
role_VSA_id	Role used for VSA search Default: sam-security-group
VSA_service_id	VSA search service identifier Default: sam-app
throttling — user login throttling parameters	
enabled	Whether to enable login throttling Default: none
rate_threshold	Login failure threshold used for calculating login failure rate; see rate_seconds parameter Default: 3
rate_seconds	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

Table 13-3 SSO parameters, NSP configuration file (continued)

Section and parameters	Description
lockout_period	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	
enabled	Whether to lock out users who have more consecutive login failures than specified by the threshold parameter Default: none
threshold	Maximum number of consecutive login failures before user lockout Default: 3
lockout_minutes	Number of minutes to lock the user out after the threshold parameter value is exceeded Default: 1

Note: Where an LDAP user is authorized for multiple group profiles, NSP will only assign the first returned group value for that user's authorization.

Part III: NSP system deployment

Overview

Purpose

This part of the *NSP Deployment and Installation Guide* provides procedures for deploying and integrating NSP components, and procedures for NSP system conversion to a different deployment type.

Contents

14 NSP installation

14.1 Introduction

14.1.1 Description

This chapter provides procedures for NSP server installation in standalone, redundant, or HA with redundancy deployments.

The chapter also includes procedures for installing the following:

- MDM adaptors—see 14.5 “To install MDM adaptors” (p. 130)
- NRC-T—see 14.6 “To install the NRC-T” (p. 131)
- NSP analytics servers—see 14.7 “To install an NSP analytics server” (p. 133)
- NSP Flow Collector Controllers and NSP Flow Collectors—see 14.8 “To install NSP Flow Collector Controllers and NSP Flow Collectors” (p. 140)
- VSR-NRC—see 14.12 “VSR-NRC installation” (p. 153)

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.

For information about installing the NFM-P, see the *NSP NFM-P Installation and Upgrade Guide*.

For information about using the NSP Lab Installer, the qcow2 installation utility for lab or trial deployments, see the *NSP Lab Installer Reference*.

Note: See the NSP module compatibility matrix in the *NSP Release Notice* to ensure that the proposed deployment results in a supported configuration.

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

14.2 To install a standalone NSP server

14.2.1 Purpose

Use this procedure to install a standalone NSP server.

Note: By supplying new values for the parameters within the configuration file, then executing the installation commands, the capabilities of an existing NSP server can be updated. See 15.2 “To upgrade a standalone NSP server” (p. 160) for more information.

14.2.2 Before you begin

Before executing the NSP installer, ensure that your system meets the hardware and software requirements described in the *NSP Planning Guide*.

Note: NSD and NRC modules will not initialize without proper license files (NSD, NRC-P, NRC-X), which must be obtained from Nokia personnel.

Note: Installation of an NSP server requires IP reachability between the server and any external systems with which the modules will integrate, such as NFM-P or NFM-T. Similarly, installation of the NRC-X module requires IP reachability between its server and the server that will host the other NSD and NRC modules.

14.2.3 Steps

CAUTION

Deployment failure

The RHEL OS of any NSP module requires specific versions of some RHEL packages. If the required package versions are not installed, the NSP installation fails.

See 11.6.6 "Special RHEL OS package requirements" (p. 78) for the required package versions.

1

Download the NSP installer package from OLCS and extract it on any station running a supported version of RHEL 7. This does not have to be the station on which the NSP server will be installed, as the installer can perform remote installations.

Note: When performing remote operations, SSH connections are used between the station where the NSP installer package is extracted and the stations that the installer configures. Therefore, SSH connections must be possible between these systems without the use of passwords, which requires the configuration of SSH keys, or the *--ask-pass* argument to be used when running the install.sh or uninstall.sh utilities, which requires that all systems share the same root user SSH password.

An NSD_NRC_*R_r* directory is created in the current directory, where *R_r* is the NSD and NRC release identifier in the form *MAJOR_minor*.

Note: In subsequent steps, the directory is called the NSP installer directory or *NSP_installer_directory*.

2

Enter the following to navigate to the NSP installer directory:

```
cd NSD_NRC_R_r ↵
```

3

Create a hosts file in the NSP installer directory that contains the required entries based on the components that the NSP server will host. See 13.2 “NSP hosts file” (p. 101) for more information.

Note: A sample hosts file can be found in the */<loadpath>/NSD_NRC_<R_r>/examples/hosts* directory. It is highly recommend that a modified copy of this file be used during installation.

4

Create a .yml or .json configuration file in the NSP installer directory that includes only the configuration blocks that apply to your deployment. See 13.3 “NSP configuration file” (p. 108) for more information.

Note: A sample configuration file can be found at */<loadpath>/NSD_NRC_<R_r>/examples/config.yml*. It is highly recommend that a modified copy of this file be used during installation.

5

Copy the required license files to the *NSP_installer_directory*/license directory.

6

If the TLS block of the configuration file was populated in Step 4, copy the TLS certificates to the appropriate directories, as required; for example, *NSP_installer_directory*/tls/nfmp or *NSP_installer_directory*/tls/nfmt.

7

If LDAP authentication settings were configured in Step 4, copy the LDAP server certificate to the *NSP_installer_directory*/tls/ldap directory.

8

Perform 12.8 “To configure and enable an NSP PKI server” (p. 91) to enable the configuration of TLS in the system.

9

Perform one of the following to install the NSP server:

a. If the NRC-X module is being added to an existing NSD and NRC system, execute the following commands as root user to install the NRC-X module individually:

```
cd bin ↵

./install.sh --target nrcxIPaddress ↵
```

where *nrcxIPaddress* is the IP address of the server where the NRC-X software will be deployed.

b. Otherwise, execute the following commands as root user to install the components specified in the hosts file:

```
cd bin ↵

./install.sh ↵
```

10

If the auto_start parameter was set to false in Step 4, execute the following commands to start the NSP server:

```
systemctl start nspos-nspd ↵

nspdctl --host <nspServer_IP_address> start ↵
```

Where *nspServer_IP_address* is the IP address of the desired NSP server.

Note: If the NRC-X module was installed, these commands must also be performed on the server where the NRC-X software is deployed.

END OF STEPS

14.3 To install a redundant NSP server

14.3.1 Purpose

Use this procedure to install an NSP server with 1+1 redundancy, which requires the installation of both a primary NSP server instance and a standby NSP server instance. See the *NSP Planning Guide* for more information about redundant deployments.

Note: The NSP server instances will not initialize without a redundant license, which must be obtained from Nokia personnel.

14.3.2 Before you begin

Before executing the NSP installer, ensure that your system meets the hardware and software requirements described in the *NSP Planning Guide*.

Note: If the NSP servers will host NSD and NRC modules, NRC-P, NRC-X, and/or NSD licenses must be obtained from Nokia personnel and placed in the license folder. These modules will not initialize without a valid license file in this folder.

Note: Installation of an NSP server requires IP reachability between the modules and any external systems with which the modules will integrate, such as NFM-P or NFM-T. For information about installing these components, see their respective documentation suites.

14.3.3 Steps

CAUTION

Deployment failure

The RHEL OS of any NSP module requires specific versions of some RHEL packages. If the required package versions are not installed, the NSP installation fails.

See 11.6.6 "Special RHEL OS package requirements" (p. 78) for the required package versions.

1

Download the NSP installer package from OLCS and extract it on any system running a supported version of RHEL 7. This does not have to be the system on which the NSP server will be installed, as the installer can perform remote installations.

Note: When performing remote operations, SSH connections are used between the station where the NSP installer package is extracted and the stations that the installer configures. Therefore, SSH connections must be possible between these systems without the use of passwords, which requires the configuration of SSH keys, or the *--ask-pass* argument to be used when running the install.sh or uninstall.sh utilities, which requires that all systems share the same root user SSH password.

An NSD_NRC_*R_r* directory is created in the current directory, where *R_r* is the NSD and NRC release identifier in the form *MAJOR_minor*.

Note: In subsequent steps, the directory is called the NSP installer directory or *NSP_installer_directory*.

2

Enter the following to navigate to the NSP installer directory:

```
cd NSD_NRC_R_r ↵
```

3

Create a hosts file in the NSP installer directory that contains the required entries based on the components that the NSP server will host. See 13.2 "NSP hosts file" (p. 101) for more information.

Note: A sample hosts file can be found in the */<loadpath>/NSD_NRC_<R_r>/examples/hosts* directory. It is highly recommend that a modified copy of this file be used during installation.

Note: If deploying NSP servers that will host NRC-X in a redundant configuration, note that the NRC-X reads an NSD and NRC file containing PostgreSQL database information. If it attempts to read the version of the file located on the standby NSD and NRC server, the NRC-X will not initialize. To prevent this, modify the */opt/nsp/configure/config/pgsql.conf* file on the NRC-X server so that the primary NSD and NRC server is listed first.

4

Create a .yml or .json configuration file in the NSP installer directory that includes only the configuration blocks that apply to your deployment. See 13.3 “NSP configuration file” (p. 108) for more information.

Note: A sample configuration file can be found at */<loadpath>/NSD_NRC_<R_r>/examples/config.yml*. It is highly recommend that a modified copy of this file be used during installation.

5

If the TLS block of the configuration file was populated in Step 4, copy the TLS certificates to the appropriate directories, as required; for example, *NSP_installer_directory*/tls/nfmp or *NSP_installer_directory*/tls/nfmt.

6

Start the NSP PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 12.8 “To configure and enable an NSP PKI server” (p. 91).

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

7

Install the NSP servers. Execute the following commands:

```
cd bin ↵

./install.sh ↵
```

The NSP servers are automatically deployed on both servers.

8

If the auto_start parameter was set to false in Step 4, enter the following sequence of commands on each NSP server:

```
systemctl start nspos-nspd ↵

nspdctl --host <nspServer_IP_address> start ↵
```

Where *nspServer_IP_address* is the IP address of the desired NSP server.

The NSP servers start.

9

If no other components are to be deployed, stop the NSP PKI server by entering CTRL+C in the console window.

10

Close the open console windows.

END OF STEPS

14.4 To install NSP servers in HA mode with redundancy

14.4.1 Purpose

Use this procedure to install NSP servers in HA mode with redundancy. This requires the installation of an active cluster of three NSP servers, as well as a standby cluster of three NSP servers. See the *NSP Planning Guide* for more information about HA deployments with redundancy.

Note: The NSP servers will not initialize without an HA+DR license, which must be obtained from Nokia personnel.

14.4.2 Before you begin

Before executing the NSP installer, ensure that your system meets the hardware and software requirements described in the *NSP Planning Guide*.

Note: An NRC-P or NSD license must be obtained from Nokia personnel and placed in the license folder. The modules will not initialize without a valid license file in this folder.

Note: Installation of NSP servers requires IP reachability between the modules and any external systems with which the modules will integrate, such as NFM-P or NFM-T. For information about installing these components, see their respective documentation suites.

14.4.3 Steps

CAUTION

Deployment failure

The RHEL OS of any NSP module requires specific versions of some RHEL packages. If the required package versions are not installed, the NSP installation fails.

See 11.6.6 “Special RHEL OS package requirements” (p. 78) for the required package versions.

1

Download the NSD and NRC installer package from OLCS and extract it on any system running a supported version of RHEL 7. This does not have to be the system on which the NSD and NRC modules are to be installed, as the installer is able to perform remote installations.

Note: When performing remote operations, SSH connections are used between the system where the NSD and NRC installer package was extracted and the system(s) on which it will execute its tasks. Therefore, SSH connections must be possible between these systems without the use of passwords. Otherwise, the *--ask-pass*argument must be

used when running the install.sh or uninstall.sh utilities, which will require that all systems share the same root user SSH password.

An NSD_NRC_*R_r* directory is created in the current directory, where *R_r* is the NSD and NRC release identifier in the form *MAJOR_minor*.

Note: In subsequent steps, the directory is called the NSP installer directory or *NSP_installer_directory*.

2

Enter the following to navigate to the NSP installer directory:

```
cd NSD_NRC_R_r ↵
```

3

Create a hosts file in the NSP installer directory that contains the required entries based on the components that the NSP server will host. See 13.2 “NSP hosts file” (p. 101) for more information.

Note: A sample hosts file can be found in the */<loadpath>/NSD_NRC_<R_r>/examples/hosts* directory. It is highly recommend that a modified copy of this file be used during installation.

4

If the deployment will support NAT, modify the host file entries as follows so as to include the internal IP addresses for each cluster member and the internal IP addresses for each datacenter VIP address. If the setup will support NAT, the internal IP addresses for each datacenter VIP address must be specified:

```
dc1_member1_internal_advertised_address=dc1_member1_address

[datacenter1_name:vars]

vip=datacenter1_vip_internal

vip_advertised_address=datacenter1_vip

dc=location1
```

5

Create a .yml or .json configuration file in the NSP installer directory that includes only the configuration blocks that apply to your deployment. See 13.3 “NSP configuration file” (p. 108) for more information.

Note: A sample configuration file can be found at */<loadpath>/NSD_NRC_<R_r>/examples/config.yml*. It is highly recommend that a modified copy of this file be used during installation.

Note: If installing the NRC-X in HA mode with redundancy, the auto_start parameter should be set to false and the NRC-X should not be started until all nspOS host servers have been started successfully.

6

Copy the required license files to the *NSP_installer_directory*/license directory.

7

Start the NSP PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 12.8 “To configure and enable an NSP PKI server” (p. 91).

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

8

Install the NSP servers. Execute the following commands:

```
cd bin ↵
```

```
./install.sh ↵
```

The NSP servers are automatically deployed to all servers.

9

If the auto_start parameter was set to false in Step 5, enter the following sequence of commands on each NSP server:

```
systemctl start nspos-nspd ↵
```

```
nspdctl --host <nspServer_IP_address> start ↵
```

Where *nspServer_IP_address* is the IP address of the desired NSP server.

The NSP servers start.

10

Verify that the NSP services have started correctly and assumed their expected roles. Execute:

```
nspdctl --host <nspServer_IP_address> status
```

Where *nspServer_IP_address* is the IP address of the desired NSP server.

11

If NRC-X servers were installed, it is possible that their active datacenter will initially be different from that of the NSP servers where nspOS was installed. To correct this, execute:

1. On the lead member of the active datacenter: **`nspdctl to-standby`**
2. On the lead member of the standby datacenter: **`nspdctl to-active`**

12

If no other components are to be deployed, stop the NSP PKI server by entering CTRL+C in the console window.

13

Close the open console windows.

END OF STEPS

14.5 To install MDM adaptors

14.5.1 Purpose

MDM adaptor packages must be installed to allow NEs to be discovered using MDM and managed using NSP applications. The distribution of adaptors to the MDM servers is managed by the NSP installer. This procedure can be performed while the MDM server is running.

Perform this procedure as the root user on the station where the NSP installer was extracted.

Note: The NSP adaptors are available for the purpose of evaluation in a lab environment and as a starting point for your custom development. These adaptors have been validated only against specific network configurations. See the readme file for your adaptor package for the list of tested NEs.

Because your requirements or configuration may differ from the tested configurations, it is strongly recommended not to use the adaptors in a production network.

Contact your Nokia representative to obtain adaptors, and technical support for assistance with adaptor customization.

14.5.2 Prerequisites

For MDM adaptors to be installed, the following must be performed:

- an MDM adaptor directory must be created on a server that is available to the NSP installer.
- The `adaptor_directory` parameter in the config.yml file must be updated to provide the path to the adaptor directory. See 13.3 “NSP configuration file” (p. 108) for more information.

14.5.3 Steps

1

Extract the *package*.tar.gz files into the MDM adaptor directory.

2

Enter the following to navigate to the NSP installer directory:

```
# cd NSP_installer_directory/NSD_NRC_R_r ↵
```

where `R_r` is the NSD and NRC release identifier in the form MAJOR_minor.

3

Execute the following command to install the adaptors:

```
# tools/mdm/mdm-files.sh ↵
```

The NSP adaptors are now installed. It may take up to 30 minutes for all the adaptors to be loaded.

Compatible network elements can be discovered via the NSP Device Administrator application. See the application online help for information about creating discovery rules and discovering devices.

END OF STEPS

14.6 To install the NRC-T

14.6.1 Purpose

Use this procedure to install the NRC-T product for use with NSP. The NRC-T system shares a host server with the NFM-T.

14.6.2 Before you begin

Prior to installing an NRC-T server, ensure that the following criteria are met:

- An NFM-T server running Release 18.7.0.79 or later has been deployed
- A directory entitled *NFMT-<release_load>* exists within the */DEPOT* directory
- The NFM-T release software is available from the */DEPOT/NFMT-<release_load>* directory

14.6.3 Steps

1

Login to the server that will host the NRC-T software as the root user.

2

Download the *NRCT_<software_load>.tar.gz* file and the *autoinstall<version>.noarch.rpm* file to the */DEPOT/NFMT-<release_load>* directory.

where

<software_load> is the numbered NRC-T software release, such as 18.8.0.4.

<version> is the numbered autoinstall version, such as 187-6.0-102.

<release_load> is the numbered NFM-T software release, such as 18.7.0.79.

3

Verify the *cksum*.

4

Extract the NRC-T software package. Execute the following command:

cd /DEPOT/NFMT-<release_load>;tar -xvzy NRCT_<software_load>.tar.gz

where

<release_load> is the numbered NFM-T software release, such as 18.7.0.79.

<software_load> is the numbered NRC-T software release, such as 18.8.0.4.

5

Start the NSP PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 12.8 “To configure and enable an NSP PKI server” (p. 91).

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

6

Install the new autoinstall. Execute:

rpm -Uvh autoinstall<release_load>.noarch.rpm

Where *<version>* is the numbered autoinstall version, such as 187-6.0-102.

7

Enable the NRC-T option in the Autoinstall configurator (AI-C). Execute:

touch /var/autoinstall/NRCT

8

Ensure that NRC-T 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 NSP PKI server by entering CTRL+C in the console window.

11

Perform 16.4 “To integrate NSP servers with an NRC-T system” (p. 221).

END OF STEPS

14.7 To install an NSP analytics server

14.7.1 Purpose

The following steps describe how to install the NSP analytics server software on a station.

Note: You require the following user privileges:

- on each main server station—root, nsp
- on the analytics server station—root

Note: Performing the procedure creates the nsp user account 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

14.7.2 Steps

CAUTION

Deployment failure

The RHEL OS of any NSP module requires specific versions of some RHEL packages. If the required package versions are not installed, the NSP installation fails.

See 11.6.6 "Special RHEL OS package requirements" (p. 78) for the required package versions.

You must perform the steps on each NSP analytics server station.

Install analytics server packages

1

Log in as the root user on the analytics server station.

2

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

3

Open a console window.

4

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.

5

Navigate to the directory that contains the downloaded installation files.

6

Enter the following:

```
# chmod +x *.rpm ↵
```

7

Enter the following:

```
# yum install *.rpm ↵
```

The yum utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/N]:
```

8

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
```

The package installation is complete when the following is displayed:

```
Complete!
```

Configure analytics server

9

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 the *NSP NFM-P Installation and Upgrade Guide*.

1. 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.

2. Enter the following:

   # **chown nsp:nsp *keystore_file*** ↵

   where *keystore_file* is the absolute path of the keystore file

3. Enter the following:

   # **chown nsp:nsp *truststore_file*** ↵

   where *truststore_file* is the absolute path of the truststore file

10

Enter the following to switch to the nsp user:

su - nsp ↵

11

Enter the following:

bash$ **cd /opt/nsp/analytics/bin** ↵

12

Enter the following:

bash$ **./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
```

13

Enter YES.

The script displays a series of prompts.

14

At each prompt, enter a parameter value; to accept a default in brackets, press ↵.

The following table lists and describes each parameter.

Table 14-1 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 server Default: —
Is NSPOS secure(true/false)	Whether the Kafka, PostgreSQL, and ZooKeeper communication is secured using TLS; the value must match the NSD/NRC [nspos] secure parameter value Default: false

Table 14-1 NSP analytics server parameters (continued)

Parameter	Description
Primary PostgreSQL Repository Database Host	The primary report results repository, which is the IP address or hostname of one of the following: • if the NSP system includes only the NFM-P, the primary or standalone NFM-P main server • if the NSP system includes the NSD and NRC, the primary or standalone NSD and NRC server 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 • if the NSP system includes the NSD and NRC, the standby NSD and NRC server Default: —
Auxiliary Data Source DB Host 1	If the system includes an auxiliary database, the IP address or hostname of that auxiliary database station Default: —
Auxiliary Data Source DB Host 2	If the system includes an auxiliary database, the IP address or hostname of that auxiliary database station Default: —
Auxiliary Data Source DB Host 3	If the system includes an auxiliary database, the IP address or hostname of that auxiliary database station Default: —
Auxiliary Data Source DB Port	If the system includes an auxiliary database, the auxiliary database port Default: 5433
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
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: —

Table 14-1 NSP analytics server parameters (continued)

Parameter	Description
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
Secure Zookeeper Client Mode (true/false)	Whether communication with the ZooKeeper host servers is secured using TLS; the value must match the NSD/NRC [nspos] secure parameter value You can set the parameter to true only if all NSP components are at Release 19.6 or later. Default: false
Zookeeper Connection String	The IP address or hostname, and port of each ZooKeeper host server, 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 Secure ZooKeeper Client Mode 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** • **if the NSP system includes the NSD and NRC, the NSD and NRC servers** Default: —

15

Start the NSP PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 12.8 “To configure and enable an NSP PKI server” (p. 91).

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

16

Enter the following to install the analytics server software:

```
bash$ ./AnalyticsAdmin.sh install ↵
```

Note: The analytics server starts automatically after the installation.

The following message and prompt are displayed:

```
date time Installing Analytics Server...
Do you have existing TLS certificates?(yes/no)
```

17

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
   ```

18

If you do not have TLS keystore and truststore files, perform the following steps.

1. Enter no ↵.

   The following prompt is displayed:

   ```
   Enter the Path where the TLS Certificates should be created:
   ```

2. Enter the absolute path of a directory that is owned by the nsp user, for example, /opt/nsp.

   The following message and prompt are displayed:

```
The path that will contain the keystore and the truststore is:
path
Set the keystore password:
```

3. Enter the keystore password.

   The following prompt is displayed:

   ```
   Set the truststore password:
   ```

4. Enter the truststore password.

   The following messages are displayed:

   ```
   The files nsp.keystore and nsp.truststore have been created
   TLS Config has been updated
   ```

19

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
```

20

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
```

21

If no other components are to be deployed, stop the NSP PKI server by entering CTRL+C in the console window.

22

Close the open console window.

END OF STEPS

14.8 To install NSP Flow Collector Controllers and NSP Flow Collectors

14.8.1 Purpose

Use this procedure to install standalone or redundant NSP Flow Collector Controllers, and one or more NSP Flow Collectors.

Note: You can install NSP Flow Collector Controllers and NSP Flow Collectors independently, or as part of a deployment that includes the NSD/NRC or NFM-P.

Note: For smaller deployments, you can collocate an NSP Flow Collector Controller and an NSP Flow Collector on one station, as described in the procedure.

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.

14.8.2 Steps

CAUTION

Deployment failure

The RHEL OS of any NSP module requires specific versions of some RHEL packages. If the required package versions are not installed, the NSP installation fails.

See 11.6.6 "Special RHEL OS package requirements" (p. 78) for the required package versions.

1

Perform one of the following.

a. If you are installing NSP Flow Collectors for an NSP system that includes a Release 18.12 or earlier NFM-P, perform the Flow Collector installation procedure in the *NSP NFM-P Installation and Upgrade Guide* for the NFM-P release, and not this procedure.

b. If you are installing NSP Flow Collectors or Controllers for a system that includes a Release 19.3 or later NFM-P, perform the Flow Collector and Controller installation procedure in the *NSP Deployment and Installation Guide* release that matches the NFM-P release.

2

Download the NSP installer package from OLCS and extract it on any station running a supported version of RHEL 7. This does not have to be the station on which an NSP Flow Collector Controller or a 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 NSD and NRC release identifier in the form *MAJOR_minor*.

Note: When performing remote operations, SSH connections are used between the station where the NSP installer package is extracted and the stations that the installer configures. Therefore, SSH connections must be possible between these systems without the use of passwords, which requires the configuration of SSH keys, or the *--ask-pass* argument to be used when running the install.sh or uninstall.sh utilities. In such a scenario, the root user on each station must have the same SSH password.

3

Open a console window.

4

Enter the following as the root user:

```
# cd NSP_installer_directory/NSD_NRC_R_r ↵
```

5

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
  - if the NSP system includes the NSD and NRC, the NSD and NRC servers
- [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 13.2 “NSP hosts file” (p. 101) for configuration information.

Note: An example hosts file is in the following directory:
NSP_installer_directory/NSD_NRC_*R_r*/examples
It is strongly recommended to use a modified copy of the example hosts file for installation.

6

Create a .yml or .json configuration file in the NSP installer directory that includes:

- multi-component deployment—required section or sections for each component that you are installing
- independent deployment—**tls** section only, PKI server configuration mandatory

See 13.3 “NSP configuration file” (p. 108) for more information.

Note: Example .yml and .json configuration files are in the following directory:
NSP_installer_directory/NSD_NRC_*R_r*/examples
It is strongly recommended to use a modified copy of an example configuration file for installation.

7

Start the NSP PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 12.8 “To configure and enable an NSP PKI server” (p. 91).

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

8

Enter the following:

```
# cd bin ↵
```

9

Enter the following:

```
# ./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 installed on the stations.

Start NSP Flow Collector Controllers

10

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

11

Perform Step 13 to Step 20 for each NSP Flow Collector Controller.

12

Go to Step 21.

13

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

14

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.

15

Click on the NFM-P Configuration tab.

16

Configure the parameters in the following table.

Table 14-2 NSP Flow Collector Controller parameters, NFM-P Configuration tab

Parameter	Description
XML API	
User Name	The NFM-P username for XML API file transfers
Password	The NFM-P user password for XML API file transfers
HTTP	
Use Secure HTTP (HTTPS)	Whether HTTPS is used for file transfers
JMS	
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	
Transfer Option	The method to use for file transfers from an NFM-P main server
NFM-P-1 **NFM-P-2 (required for redundant NFM-P system)**	
IP Address/Host name	The public IP address or hostname of the main server
HTTP	
HTTP Port	The TCP port on the main server for non-secure communication
HTTPS Port	The TCP port on the main server for secure communication
JMS	
JNDI Port	The TCP port on the main server for JMS communication
File Transfer	
SFTP Port	The TCP port on the main server for file transfers, if TLS is enabled
SFTP User Name	The username required for secure file transfers from the main server
SFTP Password	The password required for secure file transfers from the main server
FTP Port	The TCP port on the main server for file transfers, if TLS is not enabled
FTP User Name	The username required for non-secure file transfers from the main server
FTP Password	The password required for non-secure file transfers from the main server

17

Click Save NFM-P configuration.

18

Click on the Operations tab.

19

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.

20

If the NSP system is an HA deployment, you must synchronize the Flow Collector Controller configuration between data centers.

1. Transfer the following file from the NSP Flow Collector Controller station to the primary ZooKeeper host station in the active data center:

   /opt/nsp/flow/fcc/sample/bin/syncFccZkExtrConfig.sh

   The primary ZooKeeper host is one of the following:
   - if the NSP system includes only the NFM-P, the standalone or primary NFM-P main server
   - if the NSP system includes the NSD and NRC, the standalone or primary NSD and NRC server
2. Log in to the primary ZooKeeper host station as the nsp user.
3. Open a console window.
4. Enter the following:

   `bash$ syncFccZkExtrConfig.sh /opt/nsp/os/zookeeper/bin primary_ZK_host:port standby_ZK_host:port sync ↵`

   where

   primary_ZK_host is the IP address of the current station, the primary ZooKeeper host in the active data center

   standby_ZK_host is the IP address of the primary ZooKeeper host in the standby data center

   port is the ZooKeeper port, 2281

   For example:

syncFccZkExtrConfig.sh /opt/nsp/os/zookeeper/bin 203.0.113.10:2281 198.51.100.10:2281 sync

5. Close the console window.
6. Log in as the root user on the standby Flow Collector Controller station.
7. Open a console window.
8. Enter the following:

   ```
   # systemctl stop nsp-flow-nfmpclient.service ↵
   ```

9. Enter the following:

   ```
   # systemctl start nsp-flow-nfmpclient.service ↵
   ```

10. Close the console window.

Restore NFM-P configuration

21

If you are re-installing one or more NSP Flow Collectors as part of the *NSP NFM-P Installation and Upgrade Guide* NSP Flow Collector upgrade procedure, you must merge the contents of the old and new configuration files.

Perform the following steps for each affected NSP Flow Collector.

1. Log in as the root user on the new NSP Flow Collector station.
2. Copy the files in the /opt/nsp/flow/fc/cfg directory to a secure location on another station
3. Copy the following saved NSP Flow Collector configuration files from the NFM-P release to an empty directory on a remote station.

   Note: Depending on the NSP Flow Collector configuration and the NFM-P release from which you are upgrading, some files may not be present.

   - AACfdAggregationPolicy.xml
   - AaCfdCollectionPolicy.xml
   - CfdCounterDisplayInfo.xml
   - CfdEdrResultsTransfer.properties
   - CfdIpdrResultsTransfer.properties
   - CfdLkEnv.properties
   - CfdResultsPersistencePolicy.xml
   - CfdRuntime.properties
   - CfdScheduler.properties
   - CfdSpecialStudyPolicy.xml
   - CfdState.properties
   - CfdStorage.properties
   - CfdSubnetSummPolicy.csv
   - CfdUappsPolicy.xml
   - IntervalConfigLog.properties
   - SysCfdAggregationPolicy.xml
   - SysCfdCollectionPolicy.xml

4. On the remote station, add a *.R_r* suffix to each filename, where *R_r* represents the release from which you are upgrading, for example, 18_12.

   As an example, the SysCfdCollectionPolicy.xml file is renamed SysCfdCollectionPolicy.xml.18_12.

5. On the NSP Flow Collector station, add a *.R_r* suffix to the name of each file listed in substep 3, where *R_r* represents the software release to which you are upgrading, for example, 19_3.
6. Copy the renamed files in the /opt/nsp/flow/fc/cfg directory on the NSP Flow Collector station to the directory on the remote station that contains the renamed NFM-P files from the earlier release.
7. On the remote station, navigate to the directory that contains both sets of renamed files.
8. Enter the following for each file to merge the old and new file contents to a new file::

   ```
   # merge old_file new_file filename
   ```

   where

   old_file is the old file name, for example, SysCfdCollectionPolicy.xml.18_12

   new_file is the old file name, for example, SysCfdCollectionPolicy.xml.19_3

   filename is the name to assign to the file that contains the merged contents, and is the original file name, for example, SysCfdCollectionPolicy.xml
9. Copy the merged files to the /opt/nsp/flow/fc/cfg directory on the NSP Flow Collector station.

Start NSP Flow Collectors

22

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

23

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.

Note: If you are re-installing an NSP Flow Collector as part of the *NSP NFM-P Installation and Upgrade Guide* NSP Flow Collector upgrade procedure and do not need to specify additional NEs, you can skip this step.

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.
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.

24

Click on the Aggregation Policy tab.

25

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.

26

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:

- 100 000 flows/s—1 minute

- 50 000 flows/s—5 minutes
- 25 000 flows/s—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.

27

Configure the transfer of BB NAT records in CSV format to a file server, if required.

Note: A minimum 1-Gbyte/s link is required between the NSP Flow Collector and the file server.

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

28

Enable or disable statistics collection by the NSP Flow Collector, if required.

1. Click on the Operations tab.
2. To enable statistics collection, click Enable Statistics Collection.
3. To disable statistics collection, click Disable Statistics Collection.

29

Click Save Configuration. The configuration is saved.

30

If no other components are to be deployed, stop the NSP PKI server by entering CTRL+C in the console window.

31

Close the open browser pages.

END OF STEPS

14.9 To manually align WFM virtual machines with a redundant NSP

14.9.1 Purpose

In a redundant NSP deployment with distributed WFM, the WFM virtual machine may be active at the standby site. For example, if the NSP is active at site A but the WFM does not appear on the Launchpad, the WFM may be active at site B. Perform this procedure to align the active Workflow Manager virtual machine with the active NSP site.

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

14.9.2 Steps

1

Log on to the active WFM virtual machine as the root user.

2

Open a console window.

3

Enter the following:

```
# nspdctl to-standby ↵
```

The virtual machine is now a standby WFM.

4

Log on to the standby WFM virtual machine as the root user.

5

Open a console window.

6

Enter the following:

```
# nspdctl to-active ↵
```

The virtual machine is now an active WFM.

End of steps

14.10 To install the NSP templates on the NFM-P

14.10.1 Purpose

In order to use the Service Fulfillment application 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.

14.10.2 Steps

1

Log in as the nsp user on the NSP server station that hosts the NSD and NRC modules.

2

Copy the following directory to the standalone NFM-P main server station, or in a redundant deployment, the primary NFM-P main server station:

/opt/nsp/configure/nfmpTemplates

3

Open the README file in the copied directory on the NFM-P main server station.

4

Follow the instructions in the README file to install the templates.

End of steps

14.11 To map external user groups to predefined NFM-T roles

14.11.1 Purpose

In shared-mode deployments that include the NFM-T product as a component, nspOS is hosted on a server different than the NFM-T product. When the CAS authenticates a user against an authentication source, and that user needs access to NFM-T, that user group property needs to be mapped to an NFM-T predefined role (except for read-only viewer access).

14.11.2 Steps

1

Install the NFM-T with “External LDAP” bench option. This tells the NFM-T to read from the following file in order to convert external user groups into NFM-T defined authorization profiles:

/opt/hpws/tomcat/webapps/oms1350/WEB-INF/classes/ext-aut-map.properties

See the *NFM-T Installation Guide*; Appendix E - Remote authentication; “External LDAP configuration” for more information.

2

Configure an LDAP server in the NFM-T bench options.

Note: In a shared-mode deployment that includes the NFM-T product as a component, LDAP server properties will not be used by either NFM-T or CAS.

3

After installing the NFM-T 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 NFM-T 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 NFM-T role

RadiusGroup is the group, configured within the RADIUS server, that is returned upon successful authentication

See the *NFM-T Installation Guide*; Appendix E - Remote authentication; “Post Installation actions” for more information.

4

Configure or install the nspOS instance to reference the needed authentication sources (RADIUS, AD, LDAP, and so on).

END OF STEPS

14.12 VSR-NRC installation

14.12.1 VSR-NRC installation instructions

For generic installation instructions that apply to the VSR-NRC as well, see the *Virtualized 7750 SR and 7950 XRS Simulator (vSIM) Installation and Setup Guide* for your release. The vSIM and the VSR-NRC are very similar, and information such as the installation and configuration workflow, the host machine requirements, and the creation of a VSR-NRC VM is common to both.

For information about enabling the VSR-NRC management and operation after the installation, see the *NSP Lab Installer Reference*.

14.12.2 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. Contact your Nokia account representative to obtain license files associated with a VSR-NRC purchase order or trial request. For information about software licensing, see the *Virtualized 7750 SR and 7950 XRS Simulator (vSIM) Installation and Setup Guide*.

14.12.3 Supported hardware

The VSR-NRC simulates a 7750 SR router. Nokia recommends the 7750 SR-1 chassis for the VSR-NRC. For information about the supported card configurations, see the *Virtualized 7750 SR and 7950 XRS Simulator (vSIM) Installation and Setup Guide*.

Note: The VSR-NRC does not support the simulation of 7950 XRS chassis types.

14.12.4 sysinfo SMBIOS properties

As described in the *Virtualized 7750 SR and 7950 XRS Simulator (vSIM) Installation and Setup Guide*, you create and start up the VSR-NRC VM on a host system using the QEMU-KVM hypervisor. The Linux **libvirt** package provides the Virtual Shell (**`virsh`**) command-line application to facilitate the administration of VMs. The **libvirt** domain XML file for a VSR-NRC VM defines the important properties of the VM. You can use any text editor to create the domain XML file. Then, you need to pass the domain XML filename as a parameter to the **`virsh create`** command to start up the VSR-NRC VM. For example, **`virsh create vsr-nrc1.xml`**.

The **libvirt** domain XML file also includes the sysinfo element, which presents SMBIOS information to the VSR-NRC. The SMBIOS provides a way to pass VSR-NRC-specific configuration information from the host to the guest so that the configuration information is available to the VSR-NRC software when it boots. Because the product entry begins with TIMOS:, the VSR-NRC software recognizes the content that follows as important initialization information. For example, the VSR-NRC properties in the sysinfo SMBIOS entry include chassis and card configuration, and the location of the license file.

The following figure shows an example of sysinfo SMBIOS properties for a VSR-NRC. For detailed information, see the *Virtualized 7750 SR and 7950 XRS Simulator (vSIM) Installation and Setup Guide*.

Figure 14-1 Example of VSR-NRC boot parameters in sysinfo SMBIOS entry

```
<sysinfo type='smbios'>
    <system>
      <entry name='product'>TIMOS:address=192.0.2.87/24@active
         chassis=SR-1
         slot=A
         card=cfm-c4-xp
         mda/5=icm2-10gb-xp-xfp
         static-route=0.0.0.0/1@192.0.2.1
         static-route=192.0.2.0/1@192.0.2.1
         license-file=ftp://userID:password@198.51.100.10/license.txt
         primary-config=ftp://userID:password@198.51.100.10/config.cfg
      </entry>
    </system>
</sysinfo>
```

14.13 To configure the VSR-NRC

14.13.1 Description

Use this procedure after installing the VSR-NRC to commission the device for management, to configure the VSR-NRC connection to the managed network, and to prepare the VSR-NRC for use with the NSD and NRC modules.

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

14.13.2 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 may need to be altered depending on your VSR-NRC chassis, card, and MDA types configured in the VSR-NRC *domain.xml* file.

configure system snmp no shutdown ↵

configure system snmp packet-size 9216 ↵

configure system security snmp community private rwa version both ↵

configure card 1 card-type cfm-c4-xp ↵

configure card 1 mcm 1 mcm-type mcm-xp ↵

configure card 1 mda 1 mda-type icm2-10gb-xp-xfp ↵

admin save ↵

admin reboot now ↵

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: You must choose “virtio” 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 *managementIP* ↵

configure router pcep pce no shutdown ↵

where *managementIP* is the IP address of the VSR-NRC

To configure PCCs

18

Execute the following commands on all 7750 SR routers that will peer with the VSR-NRC (PCE):

configure router pcep pcc peer *VSR-NRCmanagementIP* no shutdown ↵

configure router pcep pcc no shutdown ↵

where *VSR-NRCmanagementIP* is the IP address of the VSR-NRC with which the routers will peer.

END OF STEPS

15 NSP upgrade

15.1 Introduction

15.1.1 Description

This chapter describes standalone and redundant NSP server upgrades.

The chapter also describes:

- upgrading Release 18.6 or later NSP analytics servers; see 15.7 “To upgrade NSP analytics servers” (p. 195).
- upgrading Release 19 NSP Flow Collector Controllers and NSP Flow Collectors; see 15.6 “To upgrade NSP Flow Collector Controllers and NSP Flow Collectors” (p. 192).

Note: For information about upgrading a Release 18.3 or earlier analytics server, see the *NSP NFM-P Installation and Upgrade Guide*.

Note: For information about upgrading a Release 17 or 18 NSP Flow Collector, see the *NSP NFM-P Installation and Upgrade Guide*.

For information about upgrading the NFM-P, see the *NSP NFM-P Installation and Upgrade Guide*.

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

Note: If you have modified any NFM-P template files, contact technical support before you attempt an NSD and NRC or NFM-P upgrade; an upgrade overwrites customized template values.

Shared-mode upgrades

The components that comprise a shared-mode NSP deployment must be upgraded in a specific order, starting with the NSP servers. During the upgrade, the NSP Launchpad is unavailable, as is an NFM-P or NFM-T that is part of the NSP system. After the NSP server upgrade, the NFM-P and NFM-T can be upgraded in any order.

See the NSP module compatibility matrix in the *NSP Release Notice* to ensure that the proposed upgrade results in a supported configuration.

15.2 To upgrade a standalone NSP server

15.2.1 Purpose

Use this procedure to upgrade a standalone NSP server. Upgrades are supported from NSP Release 2.0 R1 and later. If you need to upgrade from NSP Release 1.1 R2 or earlier, contact your Nokia technical support representative.

15.2.2 Before you begin

Before executing the NSP installer, ensure that your system meets the hardware and software requirements described in the *NSP Planning Guide*.

Note: Before you attempt an upgrade, you must stop all NSP processes on the server, and perform a database backup using the backup procedure from the *NSP NSD and NRC Installation and Upgrade Guide* or *NSP Deployment and Installation Guide* for the NSP release from which you are upgrading.

If the NSP server is being upgraded from an earlier release of NSP to NSP Release 17.3 or later, and the NFM-P module will be part of the deployment, 12.5 “To configure the NSP security statement” (p. 88) must be performed.

If the NSP server is hosting the NSD and NRC modules, and is being upgraded from an earlier release of NSP to NSP Release 17.6 or later, all existing user data will be lost unless 15.4 “To port existing NSD and NRC users during an upgrade” (p. 186) is performed.

15.2.3 Steps

CAUTION

Deployment failure

The RHEL OS of any NSP module requires specific versions of some RHEL packages. If the required package versions are not installed, the NSP upgrade fails.

See 11.6.6 “Special RHEL OS package requirements” (p. 78) for the required package versions.

CAUTION

Deployment failure

Upgrades should not performed on an NSP server that has never been operational.

Confirm that the NSP server to be upgraded has been started successfully before performing this procedure.

1

Log on to the NSP server station as the root user.

2

Perform one of the following to stop the NSP server:

a. If the server is running NSP Release 2.0, execute:

```
/opt/nsp/scripts/nsp-control stop
```

b. If the server is running NSP Release 17 or later, enter the following commands:

```
# nspdctl --host nspServer_IP_address stop ↵
# systemctl stop nspos-nspd ↵
```

where *nspServer_IP_address* is the IP address of the NSP server

3

Enter the following to switch to the nsp user:

```
# su nsp ↵
```

4

If the NSD and NRC is at Release 2.0 R4 or earlier, enter the following command sequence:

```
bash$ cd /opt/nsp/server/tomcat/webapps/sdn/WEB-INF/ ↵
bash$ java -cp 'lib/*:system/lib/*' org.neo4j.consistency.
ConsistencyCheckTool /opt/nsp/server/tomcat/work/graph.db ↵
```

5

Enter the following to switch back to the root user:

```
bash$ su - ↵
```

6

Ensure that the supported version of RHEL 7 is running, as specified in the *NSP Planning Guide*. As root user, execute the following command on the NSP server:

Note: A server running an unsupported version of RHEL 7 must be upgraded to a supported version.

```
# cat /etc/redhat-release ↵
```

7

If the NSP server is deployed in a VM created using the NSP RHEL OS qcow2 image, perform 11.5 “To apply an NSP RHEL qcow2 OS update” (p. 69) on the NSP server station.

8

Download the NSP installer bundle from OLCS and extract it on any station running a supported version of RHEL 7. This does not have to be the station on which the NSP server is to be installed, as the installer can perform remote upgrades.

Note: When performing remote operations, SSH connections are used between the station where the NSP installer bundle is extracted and the stations that the installer configures. Therefore, SSH connections must be possible between these systems without the use of passwords, which requires the configuration of SSH keys, or the *--ask-pass* argument to be used when running the install.sh or uninstall.sh utilities, which requires that all systems share the same root user SSH password.

An NSD_NRC_*R_r* directory is created in the current directory, where *R_r* is the NSD and NRC release identifier in the form *MAJOR_minor*.

Note: In subsequent steps, the directory is called the NSP installer directory or *NSP_installer_directory*.

9

Enter the following to navigate to the NSP installer directory:

```
# cd NSD_NRC_R_r ↵
```

10

Create a hosts file in the NSP installer directory that contains the required entries based on the components that the NSP server is to host. See 13.2.1 “Description” (p. 101) for more information.

Note: A sample hosts file can be found in the */<loadpath>/NSD_NRC_<R_r>/examples/hosts* directory. It is highly recommend that a modified copy of this file be used during installation.

Note: The IP address of the server where a previous version of the NSP server is deployed must be used.

Note: A standalone NSP server can be upgraded and converted to a redundant NSP server simultaneously by populating the hosts file with the IP address of the station that is to be the standby NSP server. See 17.2 “To convert a standalone NSD and NRC system to a redundant NSD and NRC system” (p. 237) for more information.

11

Create a .yml or .json configuration file in the NSP installer directory that includes only the configuration blocks that apply to your deployment. See 13.3.1 “Description” (p. 108) for more information.

Note: A sample configuration file can be found at */<loadpath>/NSD_NRC_<R_r>/examples/config.yml*. It is highly recommend that a modified copy of this file be used during installation.

Note: If you are upgrading only the NSD and NRC in a shared-mode deployment that includes the NFM-P or NFM-T, you must set the auto_start parameter to false.

Note: The parameters other than the auto_start parameter must be configured to align with the parameters in the existing NSP system.

Note: If an NFM-P system is part of the NSP deployment, but will not be upgraded to Release 17.3 or later, SSO authentication cannot be delegated to the NFM-P.

12

Copy the required license files to the *NSP_installer_directory*/license directory.

13

If the TLS block of the configuration file was populated in Step 11, copy the TLS certificates to the appropriate directories, as required; for example, *NSP_installer_directory*/tls/nfmp or *NSP_installer_directory*/tls/nfmt.

14

If LDAP authentication settings were configured in Step 11, copy the LDAP server certificate to the *NSP_installer_directory*/tls/ldap directory.

15

Start the NSP PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 12.8 “To configure and enable an NSP PKI server” (p. 91).

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

16

Enter the following:

```
# cd NSD_NRC_R_r/bin ↵
```

17

Enter the following to install the NSP server software on the NSP server station:

Note: After the upgrade, the API certificate of each northbound system that is integrated with the NSP must be refreshed.

```
# ./install.sh ↵
```

The NSP server software is installed.

18

Perform 15.8 “To make changes required for NFM-T compatibility” (p. 202).

Apply NFM-P compatibility patch

19

CAUTION

Service disruption

Modifying the system configuration may have serious consequences that include service disruption. It is strongly recommended that you perform this step only with the assistance of technical support.

Contact your technical support representative before you attempt to perform the step.

Note: You must enable NSP compatibility with earlier NFM-P systems in the NSP deployment.
NSP release compatibility varies by system type; see the NSP module compatibility matrix in the *NSP Release Notice* for the release combinations that are supported in shared-mode deployments.

If you are upgrading only the NSD and NRC in a shared-mode deployment that includes the NFM-P, perform the following steps. Otherwise, go to Step 28.

1. Log in as the nsp user on the standalone or primary NFM-P main server station and enter the following:

   ```
   bash$ mkdir -p /opt/nsp/patches ↲
   ```

2. If the NFM-P system is redundant, log in as the nsp user on the standby NFM-P main server station and enter the following:

   ```
   bash$ mkdir -p /opt/nsp/patches ↲
   ```

3. Enter the following on the NSP server station to switch to the nsp user:

   ```
   # su nsp ↲
   ```

4. Enter the following:

   ```
   bash$ cd /opt/nsp/os/compatibility/nfmp ↲
   ```

5. Enter the following to copy the compatibility files to the NFM-P main server:

   ```
   bash$ scp -rp NFMP_R_r/* root@nfmp_server:/opt/nsp/patches ↲
   ```

   where

   nfmp_server is the main server IP address or hostname

   R_r is the NFM-P release, for example, 18_12

20

If you are configuring compatibility with a Release 18.5 or earlier NFM-P system that includes one or more NFM-P analytics servers, perform the following steps to enable NSP Analytics application compatibility.

1. Enter the following:

   ```
   bash$ mkdir -p /opt/nsp/patches/backup/wars/R.r ↲
   ```

where *R.r* identifies the current NSP release

2. Enter the following:

   ```
   bash$ mv /opt/nsp/os/app1-tomcat/webapps/Analytics.war
   /opt/nsp/patches/backup/wars/R.r/ ↵
   ```

3. Enter the following:

   ```
   bash$ rm -rf /opt/nsp/os/app1-tomcat/webapps/Analytics* ↵
   ```

21

Stop each NFM-P main server and prepare for the patch application.

Note: In a redundant NFM-P system, you must perform this step on the standby main server station first.

1. Log in to the NFM-P 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 to stop the main server:

   ```
   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:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/config/nspos/common-model/plugins
   ↵
   ```

7. Enter the following:

   ```
   bash$ mv mediation-policy-model.properties mediation-policy-model.
   properties.R_r ↵
   ```

   where *R_r* identifies the NFM-P release, for example, 18_12

22

Perform one of the following.

a. If the NFM-P is at Release 17.12, go to Step 23.

b. If the NFM-P is at Release 18.3, 18.6, or 18.9, go to Step 24.

c. If the NFM-P is at Release 18.12, go to Step 25.

d. If the NFM-P is at Release 19.3, go to Step 26.

23

Apply the compatibility patch to a Release 17.12 NFM-P system.

Note: In a redundant NFM-P system, you must perform the step on each main server station.

1. Perform each action in the following table 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 CLI window.

Action and commands
Create backup directories
mkdir -p /opt/nsp/patches/backup/alu_orbw/ mkdir -p /opt/nsp/patches/backup/modules/ mkdir -p /opt/nsp/patches/backup/nspos/ mkdir -p /opt/nsp/patches/backup/wars/
Back up OrbWeaver files
cd /opt/nsp/nms/lib/alu_orbw mv equipment-model-avro.jar /opt/nsp/patches/backup/alu_orbw/ mv fm-model-avro.jar /opt/nsp/patches/backup/alu_orbw/ mv nspos-kafka-messaging.jar /opt/nsp/patches/backup/alu_orbw/ mv nspos-model-messaging.jar /opt/nsp/patches/backup/alu_orbw/ mv registration-service.jar /opt/nsp/patches/backup/alu_orbw/ mv registration-service-core.jar /opt/nsp/patches/backup/alu_orbw/ mv service-model-avro.jar /opt/nsp/patches/backup/alu_orbw/
Back up module files
cd /opt/nsp/nms/lib/modules mv nms_server_registry.jar /opt/nsp/patches/backup/modules/
Back up adapter files
cd /opt/nsp/nms/lib/nspos mv nms_nspos_equipment_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_fm_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_mediation_policy_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_service_model_adapter.jar /opt/nsp/patches/backup/nspos/
Back up application .war files

Action and commands
cd /opt/nsp/nms/web/tomcat/webapps mv Assurance.war /opt/nsp/patches/backup/wars/ mv MapDaoServer.war /opt/nsp/patches/backup/wars/ mv NetworkSupervision.war /opt/nsp/patches/backup/wars/ mv ServiceSupervision.war /opt/nsp/patches/backup/wars/
Remove obsolete application directories
rm -rf /opt/nsp/nms/web/tomcat/webapps/Assurance rm -rf /opt/nsp/nms/web/tomcat/webapps/MapDaoServer rm -rf /opt/nsp/nms/web/tomcat/webapps/NetworkSupervision rm -rf /opt/nsp/nms/web/tomcat/webapps/ServiceSupervision
Switch to root user
su root
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 nspos-kafka-messaging.jar /opt/nsp/nms/lib/alu_orbw/ cp -p nspos-model-messaging.jar /opt/nsp/nms/lib/alu_orbw/ cp -p registration-service.jar /opt/nsp/nms/lib/alu_orbw/ cp -p registration-service-core.jar /opt/nsp/nms/lib/alu_orbw/ cp -p service-model-avro.jar /opt/nsp/nms/lib/alu_orbw/ cp -p nms_server_registry.jar /opt/nsp/nms/lib/modules/ 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_mediation_policy_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/

2. Go to Step 27.

24

Apply the compatibility patch to a Release 18.3, 18.6, or 18.9 NFM-P system.

Note: In a redundant NFM-P system, you must perform the step on each main server station.

1. Perform each action in the following table 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 CLI window.

Action and commands
Create backup directories
mkdir -p /opt/nsp/patches/backup/alu_orbw/ mkdir -p /opt/nsp/patches/backup/nspos/ mkdir -p /opt/nsp/patches/backup/wars/
Back up OrbWeaver files
cd /opt/nsp/nms/lib/alu_orbw mv equipment-model-avro.jar /opt/nsp/patches/backup/alu_orbw/ mv fm-model-avro.jar /opt/nsp/patches/backup/alu_orbw/ mv service-model-avro.jar /opt/nsp/patches/backup/alu_orbw/
Back up nspos adapter files
cd /opt/nsp/nms/lib/nspos mv nms_nspos_equipment_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_fm_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_mediation_policy_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_service_model_adapter.jar /opt/nsp/patches/backup/nspos/
Back up application .war files
cd /opt/nsp/nms/web/tomcat/webapps mv Assurance.war /opt/nsp/patches/backup/wars/ mv ServiceSupervision.war /opt/nsp/patches/backup/wars/
Remove obsolete application directories
rm -rf /opt/nsp/nms/web/tomcat/webapps/Assurance rm -rf /opt/nsp/nms/web/tomcat/webapps/ServiceSupervision
Switch to root user
su root
Apply compatibility-patch files

Action and commands
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_mediation_policy_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/

2. Go to Step 27.

25

Apply the compatibility patch to a Release 18.12 NFM-P system.

Note: The NFM-P system requires service pack NFMP_18_12-SP12, or a later Release 18.12 service pack.

Note: In a redundant NFM-P system, you must perform the following steps on each main server station.

1. Apply the latest available NFM-P service pack for Release 18.12.
2. Perform each action in the following table 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 CLI window.

Action and commands
Create backup directories
mkdir -p /opt/nsp/patches/backup/alu_orbw/ mkdir -p /opt/nsp/patches/backup/nspos/ mkdir -p /opt/nsp/patches/backup/wars/
Back up Orbweaver files

Action and commands
cd /opt/nsp/nms/lib/alu_orbw mv equipment-model-avro.jar /opt/nsp/patches/backup/alu_orbw/ mv fm-model-avro.jar /opt/nsp/patches/backup/alu_orbw/ mv nspos-kafka-messaging.jar /opt/nsp/patches/backup/alu_orbw/ mv nspos-model-messaging.jar /opt/nsp/patches/backup/alu_orbw/ mv registration-service.jar /opt/nsp/patches/backup/alu_orbw/ mv registration-service-core.jar /opt/nsp/patches/backup/alu_orbw/ mv service-model-avro.jar /opt/nsp/patches/backup/alu_orbw/
Back up nspos adapter files
cd /opt/nsp/nms/lib/nspos mv nms_nspos_equipment_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_fm_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_mediation_policy_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_service_model_adapter.jar /opt/nsp/patches/backup/nspos/
Back up application .war files
mv /opt/nsp/nms/web/tomcat/webapps/ServiceSupervision.war /opt/nsp/patches/backup/wars/
Remove obsolete application directories
rm -rf /opt/nsp/nms/web/tomcat/webapps/ServiceSupervision
Switch to root user
su root
Apply compatibility-patch files

Action and commands
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 nspos-kafka-messaging.jar /opt/nsp/nms/lib/alu_orbw/ cp -p nspos-model-messaging.jar /opt/nsp/nms/lib/alu_orbw/ cp -p registration-service.jar /opt/nsp/nms/lib/alu_orbw/ cp -p registration-service-core.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_mediation_policy_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/

3. Go to Step 27.

26

Apply the compatibility patch to a Release 19.3 NFM-P system.

Note: In a redundant NFM-P system, you must perform the steps on each main server station.

1. Perform each action in the following table 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 CLI window.

Action and commands
Create backup directories
mkdir -p /opt/nsp/patches/backup/alu_orbw/ mkdir -p /opt/nsp/patches/backup/nspos/
Back up Orbweaver files
cd /opt/nsp/nms/lib/alu_orbw mv equipment-model-avro.jar /opt/nsp/patches/backup/alu_orbw/ mv fm-model-avro.jar /opt/nsp/patches/backup/alu_orbw/
Back up nspos adapter files

Action and commands
cd /opt/nsp/nms/lib/nspos mv nms_nspos_equipment_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_fm_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_service_model_adapter.jar /opt/nsp/patches/backup/nspos/
Switch to root user
su root
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 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/

2. Go to Step 27.

27

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 back to the nsp user:

   `# 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 NFM-P main server console window.

Start NSP server

28

Enter the following on the NSP server station to switch back to the root user:

```
bash$ su - ↵
```

29

If you set the auto_start parameter to false in Step 11, enter the following sequence of commands:

```
# systemctl start nspos-nspd ↵
# nspdctl --host nspServer_IP_address start ↵
```

where *nspServer_IP_address* is the IP address of the NSP server

The NSP server starts.

30

If no other components are to be deployed, stop the NSP PKI server by entering CTRL+C in the console window.

31

Close the open console windows.

END OF STEPS

15.3 To upgrade redundant NSP servers

15.3.1 Purpose

Use this procedure to upgrade NSP servers in a 1+1 redundancy or HA mode deployment. NSP server s can only be deployed with redundancy if they are running NSP Release 17.3 and later. See the *NSP Planning Guide* for more information about redundant deployments.

Note: The NSP servers will not initialize without the required redundant license (1+1 or 3+3), which must be obtained from Nokia personnel.

Note: Upgrades are supported from NSP Release 2.0 R1 and later. If you need to upgrade from NSP Release 1.1 R2 or earlier, contact your Nokia support representative.

15.3.2 Before you begin

Before executing the NSP installer, ensure that your system meets the hardware and software requirements described in the *NSP Planning Guide*.

Note: If the NSP servers host the NSD and NRC modules, an NRC-P, NRC-X, and/or NSD license must be obtained from Nokia personnel and placed in the license folder. The modules will not initialize without a valid license file in this folder.

Note: Before you attempt an upgrade, you must stop all NSP processes on the primary and standby servers, and perform a database backup using the backup procedure from the *NSP NSD and NRC Installation and Upgrade Guide* or *NSP Deployment and Installation Guide* for the NSP release from which you are upgrading.

Note: If the NSD and NRC modules are being upgraded from an earlier release of NSP to NSP Release 17.3 or later, and the NFM-P module will be part of the deployment, 12.5 “To configure the NSP security statement” (p. 88) will need to be performed.

Note: If the NSD and NRC modules are being upgraded from an earlier release of NSP to NSP Release 17.6 or later, all existing user data will be lost unless 15.4 “To port existing NSD and NRC users during an upgrade” (p. 186) is performed.

15.3.3 Steps

CAUTION

Deployment failure

The RHEL OS of any NSP module requires specific versions of some RHEL packages. If the required package versions are not installed, the NSP upgrade fails.

See 11.6.6 “Special RHEL OS package requirements” (p. 78) for the required package versions.

CAUTION

Deployment failure

Upgrades should not performed on an NSP server that has never been operational.

Confirm that all NSP servers to be upgraded have been started successfully before performing this procedure.

1

Prepare each NSP server station for the upgrade.

Note: If the NSP servers are deployed with either 1+1 redundancy or in HA mode, you must perform this step on each station in the standby cluster first, followed by each station in the active cluster.

1. Log on to the NSP server station as the root user.
2. Enter the following command sequence to stop the NSP server:

   # **nspdctl --host *nspServer_IP_address* stop** ↵

   # **systemctl stop nspos-nspd** ↵

   where *nspServer_IP_address* is the IP address of the NSP server
3. Enter the following to switch to the nsp user:

   # **su nsp** ↵

4. If the NSD and NRC is at Release 2.0 R4 or earlier, enter the following command sequence to check the graphdb consistency:

   ```
   bash$ cd /opt/nsp/server/tomcat/webapps/sdn/WEB-INF/ ↵
   bash$ java -cp 'lib/*:system/lib/*' org.neo4j.consistency.
   ConsistencyCheckTool /opt/nsp/server/tomcat/work/graph.db ↵
   ```

5. Enter the following to switch back to the root user:

   ```
   bash$ su - ↵
   ```

6. Ensure that the supported version of RHEL 7 is running, as specified in the *NSP Planning Guide*. As root user, execute the following command on the NSP server:

   Note: A server running an unsupported version of RHEL 7 must be upgraded to a supported version.

   ```
   # cat /etc/redhat-release ↵
   ```

7. If the NSP server is deployed in a VM created using the NSP RHEL OS qcow2 image, perform 11.5 “To apply an NSP RHEL qcow2 OS update” (p. 69) on the NSP server station.

2

Download the NSP installer bundle from OLCS and extract it on any station running a supported version of RHEL 7. This does not have to be the station on which the NSP server is to be installed, as the installer can perform remote upgrades.

Note: When performing remote operations, SSH connections are used between the station where the NSP installer bundle is extracted and the stations that the installer configures. Therefore, SSH connections must be possible between these systems without the use of passwords, which requires the configuration of SSH keys, or the *--ask-pass* argument to be used when running the install.sh or uninstall.sh utilities, which requires that all systems share the same root user SSH password.

An NSD_NRC_*R_r* directory is created in the current directory, where *R_r* is the NSD and NRC release identifier in the form *MAJOR_minor*.

Note: In subsequent steps, the directory is called the NSP installer directory or *NSP_installer_directory*.

3

Enter the following to navigate to the NSP installer directory:

```
# cd NSD_NRC_R_r ↵
```

4

Create a hosts file in the NSP installer directory that contains the required entries based on the components that the NSP server is to host. See 13.2.1 “Description” (p. 101) for more information.

Note: A sample hosts file can be found in the */<loadpath>/NSD_NRC_<R_r>/examples/hosts* directory. It is highly recommend that a modified copy of this file be used during installation.

Note: The IP address of the server where a previous version of the NSP server is deployed must be used.

Note: If the NSP servers are deployed in HA mode, compare the hosts and config.yml files against the samples provided with the load in the */nsp-load-path/examples/* directory.

5

Create a .yml or .json configuration file in the NSP installer directory that includes only the configuration blocks that apply to your deployment.

Note: A sample configuration file can be found at */<loadpath>/NSD_NRC_<R_r>/examples/config.yml*. It is highly recommend that a modified copy of this file be used during installation.

The parameters are defined in Table 13-2, “Component parameters, NSP configuration file” (p. 110).

Note: If you are upgrading only the NSD and NRC in a shared-mode deployment that includes the NFM-P or NFM-T, you must set the auto_start parameter to false.

Note: The parameters other than the auto_start parameter must be configured to align with the parameters in the existing NSP system.

Note: If an NFM-P system is part of the NSP deployment, but will not be upgraded to Release 17.3 or later, SSO authentication cannot be delegated to the NFM-P.

6

Copy the required license files to the *NSP_installer_directory*/license directory.

7

If the TLS block of the configuration file was populated in Step 5, copy the TLS certificates to the appropriate directories, as required; for example, *NSP_installer_directory*/tls/nfmp or *NSP_installer_directory*/tls/nfmt.

8

If LDAP authentication settings were configured in Step 5, copy the LDAP server certificate to the *NSP_installer_directory*/tls/ldap directory.

9

Start the NSP PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 12.8 “To configure and enable an NSP PKI server” (p. 91).

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

10

Enter the following:

```
# cd NSD_NRC_R_r/bin ↵
```

11

Enter the following to install the NSP server software on each NSP server station:

Note: After the upgrade, the API certificate of each northbound system that is integrated with the NSP must be refreshed.

```
# ./install.sh ↵
```

The NSP server software is deployed to each server station and installed.

12

Perform 15.8 “To make changes required for NFM-T compatibility” (p. 202).

Apply NFM-P compatibility patch

13

CAUTION

Service disruption

Modifying the system configuration may have serious consequences that include service disruption. It is strongly recommended that you perform this step only with the assistance of technical support.

Contact your technical support representative before you attempt to perform the step.

Note: You must enable NSP compatibility with earlier NFM-P systems in the NSP deployment.
NSP release compatibility varies by system type; see the NSP module compatibility matrix in the *NSP Release Notice* for the release combinations that are supported in shared-mode deployments.

If you are upgrading only the NSD and NRC in a shared-mode deployment that includes the NFM-P, perform the following steps. Otherwise, go to Step 22.

1. Log in as the nsp user on the standalone or primary NFM-P main server station and enter the following:

   ```
   bash$ mkdir -p /opt/nsp/patches ↵
   ```

2. If the NFM-P system is redundant, log in as the nsp user on the standby NFM-P main server station and enter the following:

   ```
   bash$ mkdir -p /opt/nsp/patches ↵
   ```

3. Enter the following on the NSP server station to switch to the nsp user:

   ```
   # su nsp ↵
   ```

4. Enter the following:

   ```
   bash$ cd /opt/nsp/os/compatibility/nfmp ↵
   ```

5. Enter the following to copy the compatibility files to the NFM-P main server:

   bash$ **scp -rp NFMP_*R_r*/* root@*nfmp_server*:/opt/nsp/patches** ↵

   where

   nfmp_server is the main server IP address or hostname

   R_r is the NFM-P release, for example, 18_12

14

If you are configuring compatibility with a Release 18.5 or earlier NFM-P system that includes one or more NFM-P analytics servers, perform the following steps to enable NSP Analytics application compatibility.

1. Enter the following:

   bash$ **mkdir -p /opt/nsp/patches/backup/wars/*R.r*** ↵

   where *R.r* identifies the current NSP release

2. Enter the following:

   bash$ **mv /opt/nsp/os/app1-tomcat/webapps/Analytics.war /opt/nsp/patches/backup/wars/*R.r*/** ↵

3. Enter the following:

   bash$ **rm -rf /opt/nsp/os/app1-tomcat/webapps/Analytics*** ↵

15

Stop each NFM-P main server and prepare for the patch application.

Note: In a redundant NFM-P system, you must perform this step on the standby main server station first.

1. Log in to the NFM-P 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 to stop the main server:

   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:

   bash$ **cd /opt/nsp/nfmp/server/nms/config/nspos/common-model/plugins** ↵

7. Enter the following:

```
bash$ mv mediation-policy-model.properties mediation-policy-model.
properties.R_r ↲
```

where *R_r* identifies the NFM-P release, for example, 18_12

16

Perform one of the following.

a. If the NFM-P is at Release 17.12, go to Step 17.

b. If the NFM-P is at Release 18.3, 18.6, or 18.9, go to Step 18.

c. If the NFM-P is at Release 18.12, go to Step 19.

d. If the NFM-P is at Release 19.3, go to Step 20.

17

Apply the compatibility patch to a Release 17.12 NFM-P system.

Note: In a redundant NFM-P system, you must perform the step on each main server station.

1. Perform each action in the following table 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 CLI window.

2. Go to Step 21.

Action and commands
Create backup directories
mkdir -p /opt/nsp/patches/backup/alu_orbw/ mkdir -p /opt/nsp/patches/backup/modules/ mkdir -p /opt/nsp/patches/backup/nspos/ mkdir -p /opt/nsp/patches/backup/wars/
Back up OrbWeaver files
cd /opt/nsp/nms/lib/alu_orbw mv equipment-model-avro.jar /opt/nsp/patches/backup/alu_orbw/ mv fm-model-avro.jar /opt/nsp/patches/backup/alu_orbw/ mv nspos-kafka-messaging.jar /opt/nsp/patches/backup/alu_orbw/ mv nspos-model-messaging.jar /opt/nsp/patches/backup/alu_orbw/ mv registration-service.jar /opt/nsp/patches/backup/alu_orbw/ mv registration-service-core.jar /opt/nsp/patches/backup/alu_orbw/ mv service-model-avro.jar /opt/nsp/patches/backup/alu_orbw/
Back up module files

Action and commands
cd /opt/nsp/nms/lib/modules mv nms_server_registry.jar /opt/nsp/patches/backup/modules/
Back up adapter files
cd /opt/nsp/nms/lib/nspos mv nms_nspos_equipment_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_fm_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_mediation_policy_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_service_model_adapter.jar /opt/nsp/patches/backup/nspos/
Back up application .war files
cd /opt/nsp/nms/web/tomcat/webapps mv Assurance.war /opt/nsp/patches/backup/wars/ mv MapDaoServer.war /opt/nsp/patches/backup/wars/ mv NetworkSupervision.war /opt/nsp/patches/backup/wars/ mv ServiceSupervision.war /opt/nsp/patches/backup/wars/
Remove obsolete application directories
rm -rf /opt/nsp/nms/web/tomcat/webapps/Assurance rm -rf /opt/nsp/nms/web/tomcat/webapps/MapDaoServer rm -rf /opt/nsp/nms/web/tomcat/webapps/NetworkSupervision rm -rf /opt/nsp/nms/web/tomcat/webapps/ServiceSupervision
Switch to root user
su root
Apply compatibility patch files

Action and commands
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 nspos-kafka-messaging.jar /opt/nsp/nms/lib/alu_orbw/ cp -p nspos-model-messaging.jar /opt/nsp/nms/lib/alu_orbw/ cp -p registration-service.jar /opt/nsp/nms/lib/alu_orbw/ cp -p registration-service-core.jar /opt/nsp/nms/lib/alu_orbw/ cp -p service-model-avro.jar /opt/nsp/nms/lib/alu_orbw/ cp -p nms_server_registry.jar /opt/nsp/nms/lib/modules/ 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_mediation_policy_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/

18

Apply the compatibility patch to a Release 18.3, 18.6, or 18.9 NFM-P system.

Note: In a redundant NFM-P system, you must perform the step on each main server station.

1. Perform each action in the following table 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 CLI window.

2. Go to Step 21.

Action and commands
Create backup directories
mkdir -p /opt/nsp/patches/backup/alu_orbw/ mkdir -p /opt/nsp/patches/backup/nspos/ mkdir -p /opt/nsp/patches/backup/wars/
Back up OrbWeaver files
cd /opt/nsp/nms/lib/alu_orbw mv equipment-model-avro.jar /opt/nsp/patches/backup/alu_orbw/ mv fm-model-avro.jar /opt/nsp/patches/backup/alu_orbw/ mv service-model-avro.jar /opt/nsp/patches/backup/alu_orbw/
Back up nspos adapter files

Action and commands
cd /opt/nsp/nms/lib/nspos mv nms_nspos_equipment_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_fm_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_mediation_policy_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_service_model_adapter.jar /opt/nsp/patches/backup/nspos/
Back up application .war files
cd /opt/nsp/nms/web/tomcat/webapps mv Assurance.war /opt/nsp/patches/backup/wars/ mv ServiceSupervision.war /opt/nsp/patches/backup/wars/
Remove obsolete application directories
rm -rf /opt/nsp/nms/web/tomcat/webapps/Assurance rm -rf /opt/nsp/nms/web/tomcat/webapps/ServiceSupervision
Switch to root user
su root
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_mediation_policy_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/

19

Apply the compatibility patch to a Release 18.12 NFM-P system.

Note: The NFM-P system requires service pack NFMP_18_12-SP12, or a later Release 18.12 service pack.

Note: In a redundant NFM-P system, you must perform the steps on each main server station.

1. Apply the latest available NFM-P service pack for Release 18.12.
2. Perform each action in the following table 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 CLI window.

3. Go to Step 21.

Action and commands
Create backup directories
mkdir -p /opt/nsp/patches/backup/alu_orbw/ mkdir -p /opt/nsp/patches/backup/nspos/ mkdir -p /opt/nsp/patches/backup/wars/
Back up Orbweaver files
cd /opt/nsp/nms/lib/alu_orbw mv equipment-model-avro.jar /opt/nsp/patches/backup/alu_orbw/ mv fm-model-avro.jar /opt/nsp/patches/backup/alu_orbw/ mv nspos-kafka-messaging.jar /opt/nsp/patches/backup/alu_orbw/ mv nspos-model-messaging.jar /opt/nsp/patches/backup/alu_orbw/ mv registration-service.jar /opt/nsp/patches/backup/alu_orbw/ mv registration-service-core.jar /opt/nsp/patches/backup/alu_orbw/ mv service-model-avro.jar /opt/nsp/patches/backup/alu_orbw/
Back up nspos adapter files
cd /opt/nsp/nms/lib/nspos mv nms_nspos_equipment_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_fm_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_mediation_policy_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_service_model_adapter.jar /opt/nsp/patches/backup/nspos/
Back up application .war files
mv /opt/nsp/nms/web/tomcat/webapps/ServiceSupervision.war /opt/nsp/patches/backup/wars/
Remove obsolete application directories
rm -rf /opt/nsp/nms/web/tomcat/webapps/ServiceSupervision
Switch to root user
su root
Apply compatibility-patch files

Action and commands
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 nspos-kafka-messaging.jar /opt/nsp/nms/lib/alu_orbw/ cp -p nspos-model-messaging.jar /opt/nsp/nms/lib/alu_orbw/ cp -p registration-service.jar /opt/nsp/nms/lib/alu_orbw/ cp -p registration-service-core.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_mediation_policy_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/

20

Apply the compatibility patch to a Release 19.3 NFM-P system.

Note: In a redundant NFM-P system, you must perform the steps on each main server station.

1. Perform each action in the following table 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 CLI window.

2. Go to Step 21.

Action and commands
Create backup directories
mkdir -p /opt/nsp/patches/backup/alu_orbw/ mkdir -p /opt/nsp/patches/backup/nspos/
Back up Orbweaver files
cd /opt/nsp/nms/lib/alu_orbw mv equipment-model-avro.jar /opt/nsp/patches/backup/alu_orbw/ mv fm-model-avro.jar /opt/nsp/patches/backup/alu_orbw/
Back up nspos adapter files

Action and commands
cd /opt/nsp/nms/lib/nspos mv nms_nspos_equipment_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_fm_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_model_adapter.jar /opt/nsp/patches/backup/nspos/ mv nms_nspos_service_model_adapter.jar /opt/nsp/patches/backup/nspos/
Switch to root user
su root
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 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/

21

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 back to the nsp user:

   ```
   # 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 NFM-P main server console window.

Start NSP servers

22

If you set the auto_start parameter to false in Step 5, enter the following sequence of commands on each NSP server:

Note: If the NSP servers are deployed with either 1+1 redundancy or in HA mode, you must perform this step on each station in the standby cluster first, followed by each station in the active cluster.

```
# systemctl start nspos-nspd ↵
# nspdctl --host nspServer_IP_address start ↵
```

where *nspServer_IP_address* is the IP address of the NSP server

The NSP server starts.

23

If no other components are to be deployed, stop the NSP PKI server by entering CTRL+C in the console window.

24

If analytics servers are part of the NSP system, but are not being upgraded at this time, restart each analytics server by logging in to each analytics server station as nsp user and executing the following command:

```
bash$ /opt/nsp/analytics/bin/AnalyticsAdmin.sh stop
bash$/opt/nsp/analytics/bin/AnalyticsAdmin.sh start
```

25

Close the open console windows.

END OF STEPS

15.4 To port existing NSD and NRC users during an upgrade

15.4.1 Purpose

Use this procedure to port existing NSD and NRC users when upgrading from NSP Release 17.3.

15.4.2 Steps

1

Resynchronize all user data with the Keystone server. On the primary NSD and NRC server, execute:

```
curl -vk https://serverAddress:8543/sdn/api/v3/tenants/resync/KEYSTONE
-H 'Authorization: keystoneToken' ↵
```

where

serverAddress is the IP address of the primary NSD and NRC server

keystoneToken is the Keystone token currently being used by the NSD and NRC user

Note: This can also be done from https://*serverAddress*:8543/sdn/api/v3/tenants/resync/KEYSTONE
where *serverAddress* is the IP address of the primary NSD and NRC server.

Note: If the above command returns an error, execute the following command to trigger an automatic re-synchronization of the tenants:

```
# systemctl restart nspos-tomcat ↵
```

2

Back up all user credentials from the Keystone server. On the primary NSD and NRC server, enter:

```
curl -vk https://serverAddress:8543/sdn/api/v3/users -H
'Authorization: keystoneToken' ↵
```

where

serverAddress is the IP address of the primary NSD and NRC server

keystoneToken is the Keystone token currently being used by the NSD and NRC user

Note: This data can also be retrieved from https://*serverAddress*:8543/sdn/api/v3/users.
where *serverAddress* is the IP address of the primary NSD and NRC server.

Save the output data.

3

Back up all tenant credentials from the Keystone server. On the primary NSD and NRC server, execute:

```
curl -vk https://serverAddress:8543/sdn/api/v3/tenants -H
'Authorization: keystoneToken' ↵
```

where

serverAddress is the IP address of the primary NSD and NRC server

keystoneToken is the Keystone token currently being used by the NSD and NRC user

Note: This data can also be retrieved from https://*serverAddress*:8543/sdn/api/v3/tenants.
where *serverAddress* is the IP address of the primary NSD and NRC server.

Save the output data.

4

Back up all users assigned to each tenant. On the primary NSD and NRC server, execute the following for each user and tenant:

curl -vk https://*serverAddress*:8543/sdn/api/v3/tenants/*tenantUUID*/user/*userUUID* -H 'Authorization: *keystoneToken*' ↵

where

serverAddress is the IP address of the primary NSD and NRC server

tenantUUID is the UUID of the tenant to which the user is assigned

userUUID is the UUID of the user to be backed up

keystoneToken is the Keystone token currently being used by the NSD and NRC user

Note: This data can also be retrieved from https://*serverAddress*:8543/sdn/api/v3/tenants/*tenantUUID*/user/*userUUID*
where
serverAddress is the IP address of the primary NSD and NRC server
tenantUUID is the UUID of the tenant to which the user is assigned
userUUID is the UUID of the user to be backed up

Save the output data.

5

Back up all resources assigned to each tenant. On the primary NSD and NRC server, execute the following for each tenant:

curl -vk https://*serverAddress*:8543/sdn/api/v3/tenants/*tenantUUID*/resources -H 'Authorization: *keystoneToken*' ↵

where

serverAddress is the IP address of the primary NSD and NRC server

tenantUUID is the UUID of the tenant to which the resources are assigned

keystoneToken is the Keystone token currently being used by the NSD and NRC user

Note: This data can also be retrieved from https://*serverAddress*:8543/sdn/api/v3/tenants/*tenantUUID*/resources
where
serverAddress is the IP address of the primary NSD and NRC server
tenantUUID is the UUID of the tenant to which the resources are assigned

Save the output data.

6

Back up all tenants assigned to each user. On the primary NSD and NRC server, execute the following for each user:

curl -vk https://*serverAddress*:8543/sdn/api/v3/users/*userUUID*/tenants -H 'Authorization: *keystoneToken*' ↵

where

serverAddress is the IP address of the primary NSD and NRC server

userUUID is the UUID of the user to which the tenants are assigned

keystoneToken is the Keystone token currently being used by the NSD and NRC user

Note: This data can also be retrieved from https://*serverAddress*:8543/sdn/api/v3/users/*userUUID*/tenants
where
serverAddress is the IP address of the primary NSD and NRC server
userUUID is the UUID of the user to which the tenants are assigned

Save the output data.

7

Perform 14.2 “To install a standalone NSP server” (p. 121) or 14.3 “To install a redundant NSP server” (p. 124), as required.

8

Create users and user groups that match the output data. On the primary NSD and NRC server, execute:

```
curl -vk https://serverAddress/user-management/rest/api/v1/users -X
POST -H 'Content-Type: application/json' -H "Authorization: Bearer
NSPsystemToken" --data ' { "username":"userName","password":
"password","group":"groupName"}' ↵
```

where

serverAddress is the IP address of the primary NSD and NRC server

NSPsystemToken is the token currently used by the NSD and NRC system

userName is the name of the user being created

password is the password to be used by the user being created

groupName is the name of the group to which the user being created will belong

Note: Nokia recommends that the same name be provided for both the user and the user group.

9

Create matching NFM-P user groups. Perform the following:

1. Log in to an NFM-P GUI client as the admin user.
2. Navigate to Administration→Security→NFM-P User Security from the main menu. The NFM-P User Security - Security Management (Edit) form opens.
3. Click on the Scope of Command tab and click Create→Profile. The Scope of Command Profile (Create) form opens.
4. Configure the Profile Name parameter and click OK. The Scope of Command Profile (Create) form closes.
5. Click on the User Groups tab, then click Create. The User Group (Create) form opens.

6. Specify the matching NSD and NRC group name as the User Group parameter value.
7. Click Select in the Scope of Command panel and choose the Scope of Command Profile created in substep 4.
8. Click Select in the Span of Control panel and choose the default Span of Control.
9. Click OK to close the open forms and save your changes. The user group is created.

10

Assign user groups to same tenants as their users, based on the output data. On the primary NSD and NRC server, perform one of the following:

a. Go to https://*serverAddress*:8543/sdn/api/v3/tenants/*tenantUUID*/usergroup/*groupName*/role/*roleType*

where

serverAddress is the IP address of the primary NSD and NRC server

tenantUUID is the UUID of the tenant to which the user group will be assigned

groupName is the name of the user group that will be assigned to the tenant

roleType is the type of role that the users of the group will assume

b. Execute:

```
curl -vk https://serverAddress:
8543/sdn/api/v3/tenants/tenantUUID/usergroup/groupName/role/roleType
-X POST --header 'Content-Type: application/json' --header 'Accept:
application/json' --header "Authorization: Bearer NSPsystemToken" ↵
```

where

serverAddress is the IP address of the primary NSD and NRC server

tenantUUID is the UUID of the tenant to which the user group will be assigned

groupName is the name of the user group that will be assigned to the tenant

roleType is the type of role that the users of the group will assume

NSPsystemToken is token currently being used by the NSD and NRC system

Note: The tenant UUIDs are migrated as part of the upgrade executed in Step 7.

END OF STEPS

15.5 To backup and restore CDLs for NRC-X

15.5.1 Purpose

Direct upgrades are not supported for NSP servers hosting the NRC-X module. As a results, NRC-X users interested in deploying NSP Release 19.6 must perform a fresh installation. To prevent the loss of information, this procedure should performed.

15.5.2 Steps

1

Upgrade the NSP server(s) hosting the NSD module as described in 15.2 “To upgrade a standalone NSP server” (p. 160).

2

Stop all processes on the on the NSP server hosting the NRC-X module. Execute the following commands:

```
nspdctl --host <NRCX_SERVER_IP> stop
systemctl stop nspos-nspd
```

Where *NRCX_SERVER_IP* is the IP address of the NSP server hosting the NRC-X module.

3

4. Take a backup of the */opt/nsp/configure/config/nrcx-server.conf* file.

4

Perform the following in the NSD_NRC_19_3 folder:

1. Configure the config.yml file. See 13.3.1 “Description” (p. 108) for more information.
2. Configure the hosts file. See 13.2.1 “Description” (p. 101) for more information.
3. Add the NRC-X license to the license directory.

5

Execute:

```
./install.sh --target <NRCX_SERVER_IP> --ask-pass
```

6

Once the upgrade has completed, restore the *nrcx-server.conf* file.

7

Start the NSP server hosting the NRC-X module. Execute:

```
systemctl start nspos-nspd
nspdctl --host <NRCX_SERVER_IP> start
```

8

If there are synchronization errors with any of the NRC-T controllers, restart those controllers.

9

Once synchronization is successful for all controllers, backup the CDLs using the following REST command:

POST https://<NRC_SERVER_IP>:
8543/nrcx/api/nrcx-test/interdomainlink/backup

The */opt/nsp/server/tomcat/webapps/work/cdl-backup.json* file is created and must be saved or manually copied to a safe location.

10

Stop the server. Execute:

nspdctl stop

11

Drop the database and start the server. Execute:

rm -rf /opt/nsp/server/tomcat/work/data/databases/graph.db

nspdctl start

12

Restore the CDLs by copying the json file created in Step 9 to the same location and executing the following REST command:

POST https://<NRCX_SERVER_IP>:
8543/nrcx/api/nrcx-test/interdomainlink/restore

Note: This will restore only those CDLs which are not yet present in NRC-X.
The namespaces of NFM-T and NSP must be the same before and after the installation of NRC-X.

END OF STEPS

15.6 To upgrade NSP Flow Collector Controllers and NSP Flow Collectors

15.6.1 Purpose

Use this procedure to upgrade standalone or redundant Release 19 NSP Flow Collector Controllers and NSP Flow Collectors.

Note: You cannot upgrade an NSP Flow Collector or Flow Collector Controller to a collocated deployment that has both on one station.

15.6.2 Steps

CAUTION

Deployment failure

The RHEL OS of any NSP module requires specific versions of some RHEL packages. If the required package versions are not installed, the NSP installation fails.

See 11.6.6 "Special RHEL OS package requirements" (p. 78) for the required package versions.

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.

Start PKI server

3

Start the NSP PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 12.8 "To configure and enable an NSP PKI server" (p. 91).

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

Upgrade software

4

Download the NSP installer package from OLCS and extract it on any station running a supported version of RHEL 7. 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 NSD and NRC release identifier in the form *MAJOR_minor*.

Note: In subsequent steps, the directory is called the NSP installer directory or *NSP_installer_directory*.

Note: When performing remote operations, SSH connections are used between the station where the NSP installer package is extracted and the stations that the installer configures. Therefore, SSH connections must be possible between these systems without the use of passwords, which requires the configuration of SSH keys, or the *--ask-pass* argument to be used when running the install.sh or uninstall.sh utilities. In such a scenario, the root user on each station must have the same SSH password.

5

Log in as the root user on the station that has the downloaded NSP software package.

6

Enter the following to navigate to the NSP installer directory:

```
# cd NSP_installer_directory/NSD_NRC_R_r ↵
```

7

Enter the following:

```
# cd bin ↵
```

8

Enter the following:

```
# ./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.

Start NSP Flow Collector Controllers

9

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

10

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:

   `/opt/nsp/flow/fc/bin/flowCollector.bash start` ↵

   The NSP Flow Collector starts.
3. Close the console window.

11

If no other components are to be deployed, stop the NSP PKI server by entering CTRL+C in the console window.

12

Close the open console windows.

END OF STEPS

15.7 To upgrade NSP analytics servers

15.7.1 Purpose

The following steps describe how to upgrade the Release 18.6 or later analytics servers in an NSP system. Ensure that you record the information that you specify, for example, directory names, passwords, and IP addresses.

Note: For information about upgrading a Release 18.3 or earlier analytics server, see the *NSP NFM-P Installation and Upgrade Guide*.

Note: You must upgrade all analytics servers in the system as one uninterrupted operation.

Note: You require root and nsp user privileges on each analytics server station.

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

- # —root user
- bash$ —nsp user

15.7.2 Steps

CAUTION

Deployment failure

The RHEL OS of any NSP module requires specific versions of some RHEL packages. If the required package versions are not installed, the NSP upgrade fails.

See 11.6.6 "Special RHEL OS package requirements" (p. 78) for the required package versions.

Perform the following steps on each NSP analytics server station.

Stop analytics servers

1

If any analytics server is running, perform the following steps on the analytics server station to stop the server.

Note: You must ensure that no analytics server is running.

1. Log in as the nsp user on the station.
2. Open a console window.
3. Enter the following:

   ```
   bash$ /opt/nsp/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
   ```

Install new software

2

Start the NSP PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 12.8 "To configure and enable an NSP PKI server" (p. 91).

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

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

where

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

v is a version identifier

Note: In subsequent steps, the directory is called the NSP software directory.

4

Navigate to the NSP software directory.

Note: Ensure that the directory contains only the installation files.

5

Enter the following:

```
# chmod +x * ↵
```

6

Enter the following:

```
# yum install *.rpm ↵
```

For each package, the yum utility resolves any package dependencies and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

7

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
```

The package installation is complete when the following is displayed:

```
Complete!
```

Upgrade analytics server

8

Enter the following to switch back to the nsp user:

```
# exit ↵
```

9

Enter the following:

```
bash$ cd /opt/nsp/analytics/bin ↵
```

10

Enter the following:

```
bash$ ./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
```

11

Enter YES.

The script displays a series of prompts.

12

At each prompt, enter a parameter value; to accept a default in brackets, press ↵.

The following table lists and describes each parameter.

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 server
Is NSPOS secure (true/false)	Whether the Kafka, PostgreSQL, and ZooKeeper communication is secured using TLS; the value must match the NSD/NRC [nspos] secure parameter value
Primary PostgreSQL Repository Database Host	The primary report results repository, which is the IP address or hostname of one of the following: • if the NSP system includes only the NFM-P, the primary or standalone NFM-P main server • if the NSP system includes the NSD and NRC, the primary or standalone NSD and NRC server
Secondary PostgreSQL Repository Database Host	In a redundant system, the standby report results repository, which is the IP address or hostname of one of the following: • if the NSP system includes only the NFM-P, the standby NFM-P main server • if the NSP system includes the NSD and NRC, the standby NSD and NRC server
Auxiliary Data Source DB Host 1	If the system includes an auxiliary database, the IP address or hostname of that auxiliary database station
Auxiliary Data Source DB Host 2	If the system includes an auxiliary database, the IP address or hostname of that auxiliary database station
Auxiliary Data Source DB Host 3	If the system includes an auxiliary database, the IP address or hostname of that auxiliary database station

Table 15-1 NSP analytics server parameters (continued)

Parameter	Description
Auxiliary Data Source DB Port	If the system includes an auxiliary database, the auxiliary database port
Primary Oracle Data Source DB Host	The primary or standalone main database IP address 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, If the **nspos** secure parameter in the NSP configuration file is set to true, you must specify the PKI server.
PKI Server Port	If the TLS configuration is automated using a PKI server, the PKI server port
Secure Zookeeper Client Mode (true/false)	Whether communication with the ZooKeeper host servers is secured using TLS; the value must match the NSD/NRC [nspos] secure parameter value You can set the parameter to true only if all NSP components are at Release 19.6 or later.
Zookeeper Connection String	The IP address or hostname, and port of each ZooKeeper host server, 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 Secure ZooKeeper Client Mode 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** • **if the NSP system includes the NSD and NRC, the NSD and NRC servers**

13

Enter the following:

```
bash$ ./AnalyticsAdmin.sh upgrade ↵
```

The script displays the following messages and prompt:

```
Stopping Analytics Server
Analytics Application is not running
Starting Analytic Server Upgrade.
Version check passed. NSP version = R.r; Analytics server version =
R.r
Do you have existing TLS certificates?(yes/no)
```

14

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:

```
Upgrading Analytics Server ...This may take several minutes to
complete
date time  Upgrading Analytics Server
Updating DB TABLES After upgrade
Updated n Tables
date time Analytic Server upgrade is completed and starting server
date time Starting Analytics Application
Waiting for Analytics Server to come up
date time Analytics Server is UP and Running
Oracle Redundancy Configuration Detected
Analytics Server successfully started!
Deploying Reports After Upgrade
Start Deploying report
.
.
.
All reports successfully tracked
date time  Analytics Server upgraded successfully
```

15

If no other components are to be deployed, stop the NSP PKI server by entering CTRL+C in the console window.

16

Close the open console windows.

END OF STEPS

15.8 To make changes required for NFM-T compatibility

15.8.1 Steps

CAUTION

Service disruption

Modifying the system configuration may have serious consequences that include service disruption. It is strongly recommended that you perform this step only with the assistance of technical support.

Contact your technical support representative before you attempt to perform the step.

Note: You must enable NSP compatibility with earlier NFM-T systems in the NSP deployment. NSP release compatibility varies by system type; see the NSP module compatibility matrix in the *NSP Release Notice* for the release combinations that are supported in shared-mode deployments.

Note: If the NFM-T system being integrated with is running release 17.12, 18.3, or 18.7.1, it is required that TLSv1.0 and TLSv1.1 are enabled. Perform the 'To update the supported NSP TLS versions and ciphers' procedure from the NSP System Administrator Guide.

Note: For NSP release 19.6, the secure parameter in the **nspos** block of the configuration file must be set to “false” in order to successfully interact with NFM-T.

1

Perform one of the following based on your upgrade scenario:

Note: In a redundant NFM-T system, you must perform the steps on each NFM-T server.

a. If you are upgrading only the NSD and NRC in a shared-mode deployment that includes a Release 17.12 or 18.3 NFM-T, continue to Step 2.

b. If you are upgrading only the NSD and NRC in a shared-mode deployment that includes a Release 18.7.1 NFM-T, go to step Step 9.

Note: In this upgrade scenario, a compatibility patch is also required. Contact Nokia support for installation instructions.

c. If you are upgrading only the NSD and NRC in a shared-mode deployment that includes a

Release 19.2 NFM-T, go to step Step 14.

Upgrading a deployment that includes NFM-T Release 17.12 or 18.3

2

Log on to the NFM-T server as the root user and open a console window.

3

Download the following compressed archive file to a temporary directory on the server:

NFMT_*R.r*_SHAREDMODEJARS_B*nnn*.tar.gz

where

R.r is the NFM-T release, for example, 17.12

nnn is the patch identifier

4

Enter the following to extract the patch files from the archive:

tar xvfP NFMT_*R.r*_SHAREDMODEJARS_B*nnn*.tar.gz ↵

5

Enter the following to apply the compatibility patch:

/nokia/1350OMS/NMA/SHAREDMODEADAPTERJARS/R/sharedmodePostInstall.sh ↵

where *R* is the NFM-T major release, for example, 18

6

Enter the following to stop the Tomcat server:

/usr/Systems/Global_Instance/APACHE/script/tomcat_stop.sh ↵

7

Enter the following to start the Tomcat server:

/usr/Systems/Global_Instance/APACHE/script/tomcat_start.sh ↵

8

Close the console window. No further action required.

Upgrading a deployment that includes NFM-T Release 18.7.1

9

Login to NFM-T and open the /opt/hpws/tomcat/webapps/oms1350/WEB-INF/classes/NfmtAdapter.properties file.

10

Modify the following attributes to read as follows:

EQUIPMENTADAPTER_VERSION=18.6.0-rel

SERVICEADAPTER_VERSION=18.6.0-rel

11

Stop the NFM-T tomcat server. Execute the following command:

/usr/Systems/Global_Instance/APACHE/script/tomcat_stop.sh

12

Start the NFM-T tomcat server. Execute the following command:

/usr/Systems/Global_Instance/APACHE/script/tomcat_start.sh

13

Close the console window. No further action required.

Upgrading a deployment that includes NFM-T Release 19.2

14

Login to NFM-T and open the /opt/hpws/tomcat/webapps/oms1350/WEB-INF/classes/NfmtAdapter.properties file.

15

Modify the following attributes to read as follows:

EQUIPMENT_ENABLED=true

SERVICE_ENABLED=true

EQUIPMENTADAPTER_VERSION=18.6.0-rel

SERVICEADAPTER_VERSION=18.6.0-rel

16

Stop the NFM-T tomcat server. Execute the following command:

/usr/Systems/Global_Instance/APACHE/script/tomcat_stop.sh

17

Start the NFM-T tomcat server. Execute:

/usr/Systems/Global_Instance/APACHE/script/tomcat_start.sh

END OF STEPS

16 NSP system integration

16.1 Introduction

16.1.1 Description

This chapter provides procedures for the integration of standalone, redundant (1+1) or HA with DR (3+3) NSP servers with an existing NFM-P or NFM-T, and also describes the integration of the NFM-P and NFM-T. An integration operation creates a shared-mode NSP deployment.

See the NSP module compatibility matrix in the *NSP Release Notice* to ensure that the proposed integration results in a supported configuration.

16.2 To integrate NSP servers with an NFM-P system

16.2.1 Purpose

Use this procedure to add NSP servers to an existing NFM-P system, or to add an NFM-P system to an existing NSP server deployment, creating a shared-mode deployment.

In shared-mode deployments, Nokia recommends that a common root CA is used, to ensure trust between the modules. See 12.2 “NSP user accounts” (p. 86) for more information about configuring security across NSP components, including the generation of a common root CA.

NSP servers and NFM-P systems must be deployed with compatible releases. NSP release compatibility varies between NSP servers and NFM-P systems. See the NSP module compatibility matrix in the *NSP Release Notice* for supported release combinations for shared-mode deployments.

16.2.2 Steps

CAUTION

Service Disruption

Performing this procedure involves stopping and starting each NFM-P main server, which is service-affecting.

This procedure must only be performed during a maintenance period of low network activity.

CAUTION

Data loss

Adding an NFM-P system to an existing NSP server deployment that is hosting the NSD and NRC modules does not restore the Neo4j or PostgreSQL databases from the NFM-P system. The NFM-P system will be re-synchronized with the NSP server(s) and manual steps/procedures must be executed to recreate the data.

If adding an NFM-P system to an existing NSP server deployment that is hosting the NSD and NRC modules, system settings and user settings must be recreated within the NSP server(s).

Note: The following user privileges are required:

- on each NFM-P main server station — root, nsp
- on each NSP 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

Note: When performing remote operations, SSH connections are used between the system where the NSP installer package was extracted and the stations on which it executes tasks. Therefore, SSH connections must be possible between these systems without the use of passwords, which requires the configuration of SSH keys, or the *--ask-pass*argument to be used when running the db-restore.sh utility, which requires that all systems share the same root user SSH password.

Install NSP server

1

Perform 14.2 “To install a standalone NSP server” (p. 121) or 14.3 “To install a redundant NSP server” (p. 124).

Note: During installation, the auto_start parameter in the config.yml file must be set to false, so that the NSP server does not start upon completion. The **nfmp** block of the config.yml file must be populated as well. See 13.3.1 “Description” (p. 108) for more information.

Note: Ensure that a common Root CA is used when installing the NSP server.

Perform NFM-P data backup for integration

2

Stop the NFM-P system as described in the *NSP NFM-P Installation and Upgrade Guide*. If the NFM-P was deployed in a redundant configuration, both the primary and standby servers must be stopped.

3

The integration process moves some data from the NFM-P main database to the NSP PostgreSQL database. In the event that you need to back out of the system integration, you must restore the NFM-P main database from a backup.

Perform ”To back up the main database from the client GUI” in the *NFM-P Administrator Guide*. Performing the procedure also backs up the Neo4j and PostgreSQL databases, which must be restored on the NSP later in the procedure.

Note: Backing up the NFM-P main database from a CLI does not back up the Neo4j or PostgreSQL database; you must perform the backup using the client GUI.

The Neo4j and PostgreSQL database backup files are in the /opt/nsp/os/backup/ directory on the standalone or primary main server station, and have the following names:

- nspos-neo4j_backup_*timestamp*.tar.gz
- nspos-postgresql_backup_*timestamp*.tar.gz
  where *timestamp* is the backup creation time

4

As the nsp user, transfer the Neo4j and PostgreSQL backup files to the */tmp/nspos_migration* directory on the NSP server.

5

Execute the following commands to ensure that the NSP server services are in the inactive state:

```
bash$ nspdctl --host <nspServer_IP_address> status ↲
bash$ systemctl status nspos-nspd ↲
```

Where *nspServer_IP_address* is the IP address of the desired NSP server.

If the services are in the active state, execute the following commands:

```
bash$ sudo systemctl stop nspos-nspd ↲
bash$ nspdctl --host <nspServer_IP_address> stop ↲
```

Where *nspServer_IP_address* is the IP address of the desired NSP server.

Note: If the NSP system is redundant, the above commands must be executed on both the active and the standby servers.

Restore Neo4j database

6

If you are adding an NFM-P system to an NSP deployment that includes the NSD and NRC, go to Step 8.

If you are also adding the NSP servers to an existing NFM-T deployment, perform the following steps on each NSP server to restore the Neo4j database backup from either the NFM-P or NFM-T.

Note: The data set that is not restored will be lost, however, once that entity (NFM-P or NFM-T) comes online with nspOS, the data it provides to common applications will be re-synchronized into the nspOS Neo4j database. For example, in the case of the Fault Management application, alarms would be re-synchronized.

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

   ```
   bash$ su - ↵
   ```

2. Enter the following:

   ```
   # cd NSP_installer_directory/tools/database ↵
   ```

   where *NSP_installer_directory* is the directory that contains the extracted NSP software package

3. Enter the following:

   ```
   # ./db-restore.sh --target server_IP ↵
   ```

   where *server_IP* is the local NSP server IP address

   Note: The --target parameter is required only in a redundant NSP system.

   The following message and prompt are displayed:

   ```
   Verifying prerequisites...
   Starting database restore ...
   Backupset file to restore (.tar.gz format):
   ```

4. Enter the following and press ↵:

   ```
   /tmp/nspos_migration/nspos-neo4j_backup_timestamp.tar.gz
   ```

   where *timestamp* is the backup creation time

   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: /tmp/nspos_
   migration/nspos-neo4j_backup/nspos-neo4j_backup_timestamp.tar.gz?
   Press return to continue, or Ctrl+C to abort:
   ```

5. Press ↵.

   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
```

6. If the `failed` value is greater than zero, a restore failure has occurred; contact technical support for assistance.

Restore PostgreSQL database

7

If you are also adding the NSP servers to an existing NFM-T deployment, perform the following steps on each NSP server to restore the PostgreSQL database backup from either the NFM-P or NFM-T.

Note: The data set that is not restored will be lost, however, once that entity (NFM-P or NFM-T) comes online with nspOS, the data it provides to common applications will be re-synchronized into the nspOS PostgreSQL database. For example, in the case of the Fault Management application, alarms would be re-synchronized.

1. Enter the following:

   `# ./db-restore.sh --target server_IP` ↵

   where *server_IP* is the local NSP server IP address

   Note: The --target parameter is required only in a redundant NSP system.

   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 ↵:

   `/tmp/nspos_migration/nspos-postgresql_backup_timestamp.tar.gz`

   where *timestamp* is the backup creation time

   The following messages and prompt are displayed:

   ```
   PLAY [all] *********************************************
   [dbrestore : pause]
   Do you want to restore the nspOS PostgreSQL db from file:
   /tmp/nspos_migration/nspos-postgresql_backup_timestamp.tar.gz?
   Press return to continue, or Ctrl+C to abort:
   ```

3. Press ↵.

   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.

Start the NSP server(s)

8

Enter the following to start a standalone NSD and NRC server, or the designated primary server in a redundant deployment:

```
bash$ sudo systemctl start nspos-nspd ↵
```

9

Enter the following to display the server status:

```
bash$ nspdctl --host IP_address status ↵
```

where *IP_address* is the IP address of the NSP server

Confirm that *nspos-neo4j* and *nspos-postgresql* are both in the active (master) state.

10

If the NSP system is redundant, enter the following to start the standby NSP server:

```
# sudo systemctl start nspos-nspd ↵
```

11

Change the registry IP of the NFM-P server to the NSP server IP address(es). Any references to the loopback address or the NFM-P system IP address(es) must be removed.See the *NSP NFM-P Installation and Upgrade Guide* for specific instructions.

The NFM-P system must then be restarted (both the primary and standby servers, in a redundant deployment).

Reconfigure NSP analytics servers

12

Perform the following steps on each NSP analytics server to configure the server to use the PostgreSQL database and ZooKeeper registration service on the NSP servers instead of the NFM-P main servers.

1. Log in to the analytics server station as the nsp user.
2. Enter the following:

```
bash$ cd /opt/nsp/analytics/bin ↲
```

3. Enter the following:

```
bash$ ./AnalyticsAdmin.sh stop ↲
```

4. 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
```

5. Enter YES. The script displays the first in a series of prompts.
6. Configure the following parameters:
   - Primary PostgreSQL Repository Database Host
   - Secondary PostgreSQL Repository Database Host
   - PKI Server IP Address or Hostname
   - PKI Server Port
   - Secure Zookeeper Client Mode
   - Zookeeper Connection String

   For information about a parameter, see Table 14-1, “NSP analytics server parameters” (p. 135).
7. Enter the following:

```
bash$ ./AnalyticsAdmin.sh start ↲
```

The analytics server starts.

END OF STEPS

16.3 To integrate NSP servers with an NFM-T system

16.3.1 Purpose

Use this procedure to add NSP servers to an existing NFM-T system, or to add an NFM-T system to an existing NSP server deployment, creating a shared-mode deployment. This procedure can also be used to add NSP servers that are already part of a shared-mode deployment (that includes the NFM-P module) to an existing NFM-T system.

In shared-mode deployments, Nokia recommends that a common root CA is used, to ensure trust between the modules. See 12.2 “NSP user accounts” (p. 86) for more information about configuring security across NSP components, including the generation of a common Root CA.

NSP servers and NFM-T systems must be deployed with compatible releases. NSP release compatibility varies between NSP servers and NFM-T systems. See the NSP module compatibility matrix in the *NSP Release Notice* for supported release combinations for shared-mode deployments.

Note: If the NSP servers are to integrate with an NFM-T system that shares a host server with the NRC-T, perform 16.4 “To integrate NSP servers with an NRC-T system” (p. 221) instead.

CAUTION

Service Disruption

Performing this procedure requires stopping and starting NFM-T systems, which is service-affecting.

This procedure should only be performed during a maintenance period of low network activity.

CAUTION

Data loss

Adding an NFM-T system to an existing NSP server deployment that is hosting the NSD and NRC modules will not restore the Neo4j or PostgreSQL databases from the NFM-T system. The NFM-T system will be re-synchronized with the NSP server(s) and manual steps/procedures must be executed to recreate the data.

If adding an NFM-T system to an existing NSP server deployment that is hosting the NSD and NRC modules, system settings and user settings on the NFM-T system must be recreated within the NSP server(s).

16.3.2 Steps

Note: The *root* and *nsp* user privileges are required on each NFM-T host server station and each NSP server station.
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: When performing remote operations, SSH connections are used between the system where the NSP installer package was extracted and the stations on which it executes tasks. Therefore, SSH connections must be possible between these systems without the use of passwords, which requires the configuration of SSH keys, or the *--ask-pass*argument to be used when running the db-restore.sh utility, which requires that all systems share the same root user SSH password.

1

Perform 14.2 “To install a standalone NSP server” (p. 121) or 14.3 “To install a redundant NSP server” (p. 124).

Note: During installation, the auto_start parameter in the config.yml file must be set to false, so that the NSP server does not start upon completion. The **nfmt** block of the config.yml file must be populated as well. See 13.3.1 “Description” (p. 108) for more information. After modifying the config.yml file, the NSP server(s) should be stopped and install.sh should be executed again. When the script finishes, the NSP server(s) must be restarted.

Note: Ensure that a common Root CA is used when installing the NSP server.

2

Perform 15.8 “To make changes required for NFM-T compatibility” (p. 202).

Perform NFM-T data backup for integration

3

If the NFM-T system was deployed in a redundant configuration, enter the following on the standby NFM-T server to stop nspOS services:

```
bash$ nspdctl --host <nspServer_IP_address> stop ↵
```

Where *nspServer_IP_address* is the IP address of the standby NFM-T server.

4

enter the following on the standalone/primary NFM-T server and ensure nspOS services are running:

```
bash$ nspdctl --host <nspServer_IP_address> status ↵
```

Where *nspServer_IP_address* is the IP address of the active NFM-T server.

5

Begin the data backup operation. Execute:

```
bash$ nspdctl --host <nspServer_IP_address> backup -d nspos_migration
-f ↵
```

Where *nspServer_IP_address* is the IP address of the active NFM-T server.

6

Execute:

```
bash$ nspdctl --host <nspServer_IP_address> backup status ↵
```

Where *nspServer_IP_address* is the IP address of the active NFM-T server.

Output similar to the following is displayed:

```
Last-known backup status :  status
Last-known backup time   :  time
Last-known backup files  :  /opt/nsp/backup/nspos_
migration/nspos-neo4j_backup_timestamp.tar.gz
```

Ensure that the *status* value is `success`, and that the *time* value is current.

7

Execute:

```
bash$ nspdctl --host <nspServer_IP_address> stop ↵
```

Where *nspServer_IP_address* is the IP address of the active NFM-T server.

8

As nsp user, transfer the backup files located in the */opt/nsp/backup/nspos_migration/* directory to the */tmp/nspos_migration/* directory on the NSP server.

9

Execute the following commands to ensure that the NSP server services are in the inactive state:

```
bash$ nspdctl --host <nspServer_IP_address> status ↲
bash$ systemctl status nspos-nspd ↲
```

Where *nspServer_IP_address* is the IP address of the NSP server.

If the services are in the active state, execute the following commands:

```
bash$ nspdctl --host <nspServer_IP_address> stop ↲
```

Where *nspServer_IP_address* is the IP address of the NSP server.

Note: If the NSP server has been deployed in a redundant configuration, the above commands should be executed on both the active and standby servers.

Restore Neo4j database

10

If you are adding an NFM-T system to an NSP deployment that includes the NSD and NRC, go to Step 12.

If you are also adding the NSP servers to an existing NFM-P deployment, perform the following steps on each NSP server to restore the Neo4j database backup from either the NFM-P or NFM-T.

Note: The data set that is not restored will be lost, however, once that entity (NFM-P or NFM-T) comes online with nspOS, the data it provides to common applications will be re-synchronized into the nspOS Neo4j database. For example, in the case of the Fault Management application, alarms would be re-synchronized.

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

   ```
   bash$ su - ↲
   ```

2. Enter the following:

   ```
   # cd NSP_installer_directory/tools/database ↲
   ```

   where *NSP_installer_directory* is the directory that contains the extracted NSP software package

3. Enter the following:

   ```
   # ./db-restore.sh --target server_IP ↲
   ```

   where *server_IP* is the local NSP server IP address

   Note: The --target parameter is required only in a redundant NSP system.

   The following message and prompt are displayed:

```
Verifying prerequisites...
Starting database restore ...
Backupset file to restore (.tar.gz format):
```

4. Enter the following and press ↵:

   `/tmp/nspos_migration/nspos-neo4j_backup_`*`timestamp`*`.tar.gz`

   where *timestamp* is the backup creation time

   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: /tmp/nspos_
migration/nspos-neo4j_backup/nspos-neo4j_backup_timestamp.tar.gz?
Press return to continue, or Ctrl+C to abort:
```

5. Press ↵.

   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
```

6. If the `failed` value is greater than zero, a restore failure has occurred; contact technical support for assistance.

Restore PostgreSQL database

11

If you are also adding the NSP servers to an existing NFM-P deployment, perform the following steps on the standalone or primary NSP server to restore the PostgreSQL database backup from either the NFM-P or NFM-T.

Note: The data set that is not restored will be lost, however, once that entity (NFM-P or NFM-T) comes online with nspOS, the data it provides to common applications will be re-synchronized into the nspOS PostgreSQL database. For example, in the case of the Fault Management application, alarms would be re-synchronized.

1. Enter the following:

   `# ./db-restore.sh --target server_IP ↵`

   where *server_IP* is the local NSP server IP address

   Note: The --target parameter is required only in a redundant NSP system.

   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 ↵:

   `/tmp/nspos_migration/nspos-postgresql_backup_timestamp.tar.gz`

   where *timestamp* is the backup creation time

   The following messages and prompt are displayed:

   ```
   PLAY [all] *********************************************
   [dbrestore : pause]
   Do you want to restore the nspOS PostgreSQL db from file:
   /tmp/nspos_migration/nspos-postgresql_backup_timestamp.tar.gz?
   Press return to continue, or Ctrl+C to abort:
   ```

3. Press ↵.

   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.

Start the NSP server(s)

12

Enter the following to start a standalone NSP server, or the designated primary server in a redundant deployment:

```
bash$ sudo systemctl start nspos-nspd ↵
```

13

Enter the following to see the status of the services:

```
bash$ nspdctl --host <nspServer_IP_address> status ↵
```

Where *nspServer_IP_address* is the IP address of the desired NSP server.

Confirm that *nspos-neo4j* and *nspos-postgresql* are both in the active (master) state.

14

If the NSP server was deployed in a redundant configuration, enter the following to start the standby NSP server:

```
# sudo systemctl start nspos-nspd ↵
```

15

Start the NSP PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 12.8 “To configure and enable an NSP PKI server” (p. 91).

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

16

If you are using the automated TLS configuration method, go to step Step 28.

17

Create a ca.jks file. On the server where the PKI server is running, in the *NSP_installer_directory*/tools/pki directory, enter the following:

```
# openssl pkcs12 -export -inkey ca.key -in ca.pem -name test -out
key.p12
```

The output is as follows:

Enter Export Password: *exportPassword*

Verifying - Enter Export Password: *exportPassword*

where *exportPassword* is the export password chosen by the user.

18

Enter the following:

Note: You must enclose a password that contains a special character in single quotation marks; for example:
`-deststorepass 'Mypassword' -srcstorepass 'Mypassword'`

```
# path/keytool -importkeystore -srckeystore key.p12 -deststorepass
keystorePassword -srcstorepass keystorePassword -srcstoretype pkcs12
-destkeystore ca.jks
```

where

path is the path to the keytool utility

keystorePassword is the password provided on export of the key.

19

Create an nspOS.public file. Execute:

```
# cp ca.pem nspOS.public
```

20

On the NFM-T host server, enter the following commands, in sequence:

```
# mkdir /opt/tls
# cd /opt/tls
```

21

Transfer the ca.jks and nspOS.public files from the server where the PKI server is running to the /opt/tls directory on the NFM-T host server.

22

Generate the JKS keystore for NFM-T; enter the following:

Note: You must enclose a password that contains a special character in single quotation marks; for example:
`-storepass 'MyPassword' -keypass 'MyPassword'`
The storepass and keypass passwords must also be identical.

```
# path/keytool -genkeypair -keyalg RSA -keystore nfmtKeystore.jks
-alias nfmt -storepass keystorePassword -keypass keyPassword -dname
CN=NSP,O=Nokia -validity 7300
```

where

path is the path to the keytool utility

keystorePassword is the password used with the keystore. This must be the same keystore password provided in Step 18.

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

23

Generate a CSR from the created JKS file; enter the following:

Note: You must enclose a password that contains a special character in single quotation marks; for example:
`-storepass 'MyPassword'`

```
# path/keytool -certreq -keystore nfmtKeystore.jks -alias nfmt -file
nfmt.csr -storepass keystorePassword  -ext san=IP:127.0.0.1,IP:NFM-T
primary IP,IP:NFM-T standby IP -validity 7300
```

where

path is the path to the keytool utility

keystorePassword is the password used with the keystore

NFM-T primary IP is the IP address of the primary NFM-T host server

NFM-T standby IP is the IP address of the standby NFM-T host server

24

Sign the certificates using the CA of the PKI server; enter the following:

Note: You must enclose a password that contains a special character in single quotation marks; for example:
-storepass 'MyPassword' -keypass 'MyPassword'
The storepass and keypass passwords must also be identical.

```
# path/keytool -gencert -storepass keystorePassword -keystore ca.jks
-keypass keyPassword -alias test -ext ku:c=digitalSignature,
keyEncipherment -ext eku:c=serverAuth,clientAuth -rfc -ext honored=all
-infile nfmt.csr -outfile nfmt.public -validity 7300
```

where

path is the path to the keytool utility

keystorePassword is the password used with the keystore

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

25

Create an nfmtKeystore.jks.p12 file; enter the following:

Note: You must enclose a password that contains a special character in single quotation marks; for example:
-deststorepass 'MyPassword' -destkeypass 'MyPassword'
The deststorepass and destkeypass passwords must also be identical.

```
# path/keytool -importkeystore -noprompt -srckeystore nfmtKeystore.jks
-destkeystore nfmtKeystore.jks.p12 -deststoretype PKCS12
-deststorepass keystorePassword -destkeypass keystorePassword
-srcstorepass keyPassword -srckeypass keyPassword -alias nfmt
```

where

path is the path to the keytool utility

keystorePassword is the password used with the keystore

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

26

Create an nfmt.private file. Execute:

```
# openssl pkcs12 -in nfmtKeystore.jks.p12 -passin pass:keyPassword
-nodes -nocerts -out nfmt.private
```

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

27

In the /opt/tls directory, create a file called tls.info and add the following lines:

- custom_certificate_path=/opt/tls/nfmt.public
- custom_private_key_path=/opt/tls/nfmt.private
- nspOS_public_key=/opt/tls/nspOS.public

28

Perform one of the following:

a. If the NSP servers were deployed in a redundant (1+1) configuration, execute the following commands:

```
# cd /var/autoinstall/R18.3/
# ./utilities/nfmt-ext-nspOS-Integration.sh bench=benchName
ssl=/opt/tls/tls.info nspOS=Primary NSP IP\;Standby NSP IP
# ./utilities/execOnBench.sh benchName complete start
```

where

benchName is the name of the bench

Primary NSP IP is the IP address of the primary NSP server

Standby NSP IP is the IP address of the standby NSP server

b. If the NSP servers were deployed in an HA + DR (3+3) configuration, execute the following commands:

```
# cd /var/autoinstall/R18.3/
# ./utilities/nfmt-ext-nspOS-Integration.sh bench=benchName
ssl=/opt/tls/tls.info nspOS=NSP IP1, NSP IP2, NSP IP3\;NSP IP4, NSP
IP5, NSP IP6 VnspOS=VnspIP1\;VnspIP2
# ./utilities/execOnBench.sh benchName complete start
```

where

benchName is the name of the bench

NSP IP1 is the IP address of the first NSP server in the primary cluster

NSP IP2 is the IP address of the second NSP server in the primary cluster

NSP IP3 is the IP address of the third NSP server in the primary cluster

NSP IP4 is the IP address of the first NSP server in the standby cluster

NSP IP5 is the IP address of the second NSP server in the standby cluster

NSP IP6 is the IP address of the third NSP server in the standby cluster

VnspIP1 is the virtual IP address of the first NSP cluster

VnspIP2 is the virtual IP address of the second NSP cluster

29

If no other components are to be deployed, stop the NSP PKI server by entering CTRL+C in the console window.

30

Launch the NFM-T from the NSP Launchpad. Perform the following:

Note: If the NFM-T was deployed in a redundant configuration, these steps must be performed on both the primary and standby NFM-T servers.

1. From the NFM-T dashboard, choose *ADMINISTER→Schedule→Scheduler* from the drop-down menu to open the Scheduler GUI.
2. From the Scheduler GUI, select *SDN-DR-Monitor*, right click, and select *Activate* from the contextual menu.

END OF STEPS

16.4 To integrate NSP servers with an NRC-T system

16.4.1 Purpose

Use this procedure to integrate NSP servers with an NRC-T system that shares a host server with the NFM-T, or to add an NRC-T system to an existing NSP server deployment, creating a shared-mode deployment. This procedure can also be used to add NSP servers that are already part of a shared-mode deployment (that includes the NFM-P module) to an existing NRC-T system.

NSP servers and NRC-T systems must be deployed with compatible releases. NSP release compatibility varies between NSP servers and NRC-T systems. See the NSP module compatibility matrix in the *NSP Release Notice* for supported release combinations for shared-mode deployments.

16.4.2 Steps

1

Perform 14.6 “To install the NRC-T” (p. 131).

2

If the NSP servers were previously integrated with an NFM-T system, perform one of the following:

a. If the NFM-T system was installed using the config.yml file, add the NRC-T block to the config.yml and execute the bin/install.sh command. See 13.3.1 “Description” (p. 108) for more information

b. If the NFM-T system was installed using the oms-server.config file (as described in “NFM-T manual installation” (p. 109)), remove the NFM-T portion of the file and add it to the file at */opt/nsp/configure/config/nrcx-server.conf*, along with the following modifications:

```
Controllers {
```

```
resync_frequency=1
ControllerContext=
[
{
supportedDomains="Optics"
Controller=
{
name="nrct1"
serverIp="NRCT_address"
DR=true
port="8543"
controllerType="NRCT"
vendor="Nokia"
version="4"
secured="true"
}
},
{
supportedDomains="IP"
resync_frequency=1
Controller=
{
name="nsp1"
serverIp="NSP_address"
DR=true
port="8543"
controllerType ="NSP"
vendor="Nokia"
version="4"
secured="true"
}
}
]
}
FeatureSupport {
optical_provisioning="false"
}
```

3

Restart the nspOS services on the NSP server that is hosting the NRC-X module. Execute the following commands:

```
# nspdctl --host <nspServer_IP_address> stop
# nspdctl --host <nspServer_IP_address> start
```

Where *nspServer_IP_address* is the IP address of the NSP server.

Note: If Step 2 was performed, these commands must also be executed on the NSP server that is hosting the NSD and NRC-P modules.

4

Perform one of the following:

a. If working from an existing NFM-T deployment, continue to Step 5.

b. If this is a new instance of NFM-T, go to Step 14.

5

Verify that the nspOS services are running on the NFM-T host server. Execute:

```
# nspdctl --host <nfmtServer_IP_address> status
```

Where *nfmtServer_IP_address* is the IP address of the NFM-T host server.

6

Perform 15.8 “To make changes required for NFM-T compatibility” (p. 202).

7

Begin the data backup operation. Execute:

```
# nspdctl --host <nfmtServer_IP_address> backup -d nspos_migration -f
```

Where *nfmtServer_IP_address* is the IP address of the NFM-T host server.

8

Verify that the backup is successful. Execute:

```
# nspdctl --host <nfmtServer_IP_address> backup status
```

Where *nfmtServer_IP_address* is the IP address of the NFM-T host server.

Ensure that the status value is `success`.

9

Stop the nspOS services on both NOC and DRC. Execute:

```
# nspdctl --host <nfmtServer_IP_address> stop
# systemctl stop nspos-nspd
```

Where *nfmtServer_IP_address* is the IP address of the NFM-T host server.

10

As the nsp user, transfer the backup files located in the */opt/nsp/backup/nspos_migration/* directory on the NFM-T host server to the */tmp/nspos_migration/* directory on the NSP server.

11

Restore the Neo4j database on the NSP server.

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

   ```
   bash$ su - ↵
   ```

2. Enter the following:

   ```
   # cd NSP_installer_directory/tools/database ↵
   ```

where *NSP_installer_directory* is the directory that contains the extracted NSP software package

3. Enter the following:

   # ./db-restore.sh --target *server_IP* ↵

   where *server_IP* is the local NSP server IP address

   Note: The --target parameter is required only in a redundant NSP system.

   The following message and prompt are displayed:

```
Verifying prerequisites...
Starting database restore ...
Backupset file to restore (.tar.gz format):
```

4. Enter the following and press ↵:

   /tmp/nspos_migration/nspos-neo4j_backup_*timestamp*.tar.gz

   where *timestamp* is the backup creation time

   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: /tmp/nspos_
migration/nspos-neo4j_backup/nspos-neo4j_backup_timestamp.tar.gz?
Press return to continue, or Ctrl+C to abort:
```

5. Press ↵.

   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
```

6. If the `failed` value is greater than zero, a restore failure has occurred; contact technical support for assistance.

12

Restore the PostgreSQL database on the NSP server. Execute:

1. Enter the following:

   `# ./db-restore.sh --target server_IP` ↵

   where *server_IP* is the local NSP server IP address

   Note: The --target parameter is required only in a redundant NSP system.

   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 ↵:

   `/tmp/nspos_migration/nspos-postgresql_backup_timestamp.tar.gz`

   where *timestamp* is the backup creation time

   The following messages and prompt are displayed:

   ```
   PLAY [all] *********************************************
   [dbrestore : pause]
   Do you want to restore the nspOS PostgreSQL db from file:
   /tmp/nspos_migration/nspos-postgresql_backup_timestamp.tar.gz?
   Press return to continue, or Ctrl+C to abort:
   ```

3. Press ↵.

   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.

13

Start the nspOS services. Execute:

```
bash$ sudo systemctl start nspos-nspd
bash$ nspdctl --host <nspServer_IP_address> start
```

Where *nspServer_IP_address* is the IP address of the NFM-T host server.

14

Perform 15.8 “To make changes required for NFM-T compatibility” (p. 202).

15

Create a ca.jks file. On the server where the PKI server is running, in the *<NSPinstallerDirectory>/tools/pki* directory, execute:

```
# openssl pkcs12 -export -inkey ca.key -in ca.pem -name test -out
key.p12
```

Where *NSPinstallationDirectory* is the directory in which the NSP server was installed.

Note: The ca.pem and ca.key files used for installation must already be present in the *<NSPinstallerDirectory>/tools/pki* directory.

The output is as follows:

Enter Export Password: *exportPassword*

Verifying - Enter Export Password: *exportPassword*

Where *exportPassword* is the export password chosen by the user.

16

On the NSP server, enter the following:

Note: You must enclose a password that contains a special character in single quotation marks; for example:
-deststorepass 'MyStorePassword' -srcstorepass 'MyStorePassword'

```
# path/keytool -importkeystore -srckeystore key.p12 -deststorepass
keystorePassword -srcstorepass keystorePassword -srcstoretype pkcs12
-destkeystore ca.jks
```

where

path is the path to the keytool utility

keystorePassword is the password provided on export of the key.

17

Create an nspOS.public file. Execute:

```
# cp ca.pem nspOS.public
```

18

On the NFM-T host server, execute:

```
# mkdir /opt/tls
# cd /opt/tls
```

19

Transfer the newly-created ca.jks and nspOS.public files from the NSP server where the PKI server is running to the /opt/tls directory on the NFM-T host server.

20

Generate the JKS keystore for NFM-T; enter the following:

Note: You must enclose a password that contains a special character in single quotation marks; for example:
-storepass 'MyPassword' -keypass 'MyPassword'
The storepass and keypass passwords must also be identical.

```
# path/keytool -genkeypair -keyalg RSA -keystore nfmtKeystore.jks
-alias nfmt - storepass keystorePassword -keypass keyPassword -dname
CN=NSP,O=Nokia - validity 7300
```

where

path is the path to the keytool utility

keystorePassword is the keystore password specified in Step 14

keyPassword is the password of the private key in the keystore

21

Generate a CSR from the created JKS file; enter the following:

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

```
# path/keytool -certreq -keystore nfmtKeystore.jks -alias nfmt -file
nfmt.csr -storepass keystorePassword -ext san=IP:127.0.0.1,IP:<NFM-T
OTNE primary IP>,IP:<NFM-T OTNE standby IP> -validity 7300
```

where

path is the path to the keytool utility

keystorePassword is the password used with the keystore

NFM-T OTNE primary IP is the IP address of the primary NFM-T OTNE VM

NFM-T OTNE standby IP is the IP address of the standby NFM-T OTNE VM

22

Sign the certificates using the CA of the PKI server; enter the following:

Note: You must enclose a password that contains a special character in single quotation marks; for example:
-storepass 'MyPassword' -keypass 'MyPassword'
The storepass and keypass passwords must also be identical.

```
# path/keytool -gencert -storepass keystorePassword -keystore ca.jks
-keypass keyPassword -alias test -ext ku:c=digitalSignature,
keyEncipherment -ext eku:c=serverAuth,clientAuth -rfc -ext honored=all
-infile nfmt.csr -outfile nfmt.public -validity 7300
```

where

path is the path to the keytool utility

keystorePassword is the password used with the keystore

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

23

Create an nfmtKeystore.jks.p12 file; enter the following:

Note: You must enclose a password that contains a special character in single quotation marks; for example:
-deststorepass 'MyPassword' - destkeypass 'MyPassword'
The deststorepass and destkeypass passwords must also be identical.

```
# path/keytool -importkeystore -noprompt -srckeystore nfmtKeystore.jks
-destkeystore nfmtKeystore.jks.p12 -deststoretype PKCS12
-deststorepass keystorePassword - destkeypass keystorePassword
-srcstorepass keyPassword -srckeypass keyPassword -alias nfmt
```

where

path is the path to the keytool utility

keystorePassword is the password used with the keystore

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

24

Create an nfmt.private file. Execute:

```
# openssl pkcs12 -in nfmtKeystore.jks.p12 -passin pass:
keyPassword-nodes - nocerts -out nfmt.private
```

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

25

In the /opt/tls directory, create a file called tls.info and add the following lines:

- custom_certificate_path=/opt/tls/nfmt.public
- custom_private_key_path=/opt/tls/nfmt.private
- nspOS_public_key=/opt/tls/nspOS.public

26

Execute the following commands:

```
# cd /var/autoinstall/<release>/
# ./utilities/nfmt-ext-nspOS-Integration.sh bench=<benchName>
ssl=/opt/tls/tls.info nspOS=<Primary NSP IP>\;<Standby NSP IP>
# ./utilities/execOnBench.sh <benchName> complete start
```

where

release is the numbered NFM-T release

benchName is the name of the bench

Primary NSP IP is the IP address of the primary NSP server

Standby NSP IP is the IP address of the standby NSP server

27

If the NFM-T system was deployed in a High Availability configuration, then the following lines of the */usr/Systems/OTNE_<x>/env/Keywords.ksh* file need to be modified as follows on both NOC and DRC:

- export NSP_OS_ADDRESS="<NSP_IP>”
- export NSP_OS_CONFIGURED="false"

Where *NSP_IP* is the IP address of the NSP server upon which the active nspOS instance will reside.

28

Restart the NRC-T process within NFM-T from the system monitor.

29

Enter the following on the server that hosts the NRC-X module, and on the server that hosts the NSD and NRC-P modules, to import the NFM-T certificates:

Note: You must enclose a password that contains a special character in single quotation marks; for example:
`-storepass 'MyStorePassword'`

```
# scp root@<NFM-T VM IP>:/usr/Systems/Global_Instance/APACHE/conf/tls.crt/server.crt
```

```
# path/keytool -alias nfmt -file server.crt -import -keystore /opt/nsp/os/tls/nsp.truststore -storepass keystore_password
```

where

path is the path to the keytool utility

NFM-T VM IP is the IP address of the server that is hosting the NFM-T

keystore_password is the password used to access the contents of the keystrore

30

Restart the nspOS services on both the server hosting the NRC-X module and the server hosting the NSD and NRC-P modules. Execute:

```
# nspdctl --host <nspServer_IP_address> stop
```

```
# nspdctl --host <nspServer_IP_address> start
```

Where *nspServer_IP_address* is the IP address of the NSP server.

31

Launch the NFM-T from the NSP Launchpad.

32

Perform the following:

Note: If the NFM-T was deployed in a redundant configuration, the following must be performed on both the primary and standby servers.

1. From the NFM-T dashboard, choose ADMINISTER→Schedule→Scheduler from the drop-down menu. The Scheduler GUI opens.
2. From the Scheduler GUI, select SDN-DR-Monitor, right click, and select Activate from the contextual menu.

33

Ensure that all private keys are removed from temporary folders on both the host system and the OTNE.

END OF STEPS

16.5 To integrate an NFM-T system with an NFM-P system

16.5.1 Purpose

Use this procedure to add an existing NFM-T system to an existing NFM-P system, creating a shared-mode IP + Optical only deployment. In such shared-mode deployments, Nokia recommends that a common root CA is used, to ensure trust between the modules. See 12.2 “NSP user accounts” (p. 86) for more information about configuring security across NSP components, including the generation of a common root CA.

NFM-T and NFM-P systems must be deployed with compatible releases. NSP release compatibility varies between NFM-P and NFM-T systems. See the NSP module compatibility matrix in the *NSP Release Notice* for supported release combinations for shared-mode IP + Optical only deployments.

Note: This combined IP + Optical only deployment scenario, without a separate NSP server, is limited to networks with a maximum total of 50 network elements (NFM-P and NFM-T combined).

Note: This deployment scenario is only supported with redundant NFM-P and Classic HA NFM-T installations.

Note: This deployment scenario requires the NFM-P system to be running NSP Release 18.12 or higher, and the NFM-T system to be running NSP Release 18.7.1 or higher.

CAUTION

Service Disruption

Performing this procedure requires stopping and starting and NFM-P and NFM-T systems, which is service-affecting.

This procedure should only be performed during a maintenance period of low network activity.

CAUTION

Data loss

Adding an existing NFM-T system to an existing NFM-P system deployment will not restore the Neo4j or PostgreSQL databases from the NFM-T system. The NFM-T system will be re-synchronized with the NFM-P systems and manual steps/procedures must be executed to recreate the data

If adding an existing NFM-T system to an existing NFM-P system deployment, the NFM-T system's settings and user settings must be recreated within the NFM-P system.

16.5.2 Before you begin

Before performing an integration, a database backup should be performed. Use the database backup procedures available from the NFM-P and NFM-T documentation suites.

16.5.3 Steps

Note: The *root* and *nsp* user privileges are required on each NFM-T host server station and each NFM-P host server station.
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: When performing remote operations, SSH connections are used between the system where the NSP installer package was extracted and the stations on which it executes tasks. Therefore, SSH connections must be possible between these systems without the use of passwords, which requires the configuration of SSH keys, or the *--ask-pass*argument to be used when running the db-restore.sh utility, which requires that all systems share the same root user SSH password.

1

Stop the NFM-P system as described in the *NSP NFM-P Installation and Upgrade Guide*. Both the primary and standby servers must be stopped.

2

Stop the NFM-T system. Enter the following on both the standby and primary NFM-T servers to stop nspOS services:

```
bash$ nspdctl --host <NFM-T_Server_IP_address> stop ↵
```

Where *NFM-T_Server_IP_address* is the IP address of the desired NFM-T server.

3

Perform the following steps on both the primary and standby NFM-P servers:

1. As root user, execute:

```
# cd /opt/nsp/os/install/examples
```

2. Copy the NFM-T integration configuration from the config.json file.
3. Modify the config.json file in the /opt/nsp/os/install directory by adding the copied NFM-T integration configuration.
4. Edit the file to update the NFM-T credentials. Save and close the file.

4

On both NFM-P servers, execute samconfig to enable NFM-T integration:

```
# samconfig -m main
<main> apply
<main> exit
```

5

Start the NFM-P system as described in the *NSP NFM-P Installation and Upgrade Guide*. Both the primary and standby NFM-P servers must be started.

6

Perform 15.8 “To make changes required for NFM-T compatibility” (p. 202).

7

Create a ca.jks file. On the server where the PKI server is running, in the NSP_installer_ directory/tools/pki directory, enter the following:

```
# openssl pkcs12 -export -inkey ca.key -in ca.pem -name test -out
key.p12
```

The output is as follows:

Enter Export Password: *exportPassword*

Verifying - Enter Export Password: *exportPassword*

Where *exportPassword* is the export password chosen by the user.

8

Enter the following:

Note: You must enclose a password that contains a special character in single quotation marks; for example:
`-deststorepass 'MyStorePassword' -srcstorepass 'MyStorePassword'`

```
# path/keytool -importkeystore -srckeystore key.p12 -deststorepass
keystorePassword -srcstorepass keystorePassword -srcstoretype pkcs12
-destkeystore ca.jks
```

where

path is the path to the keytool utility

keystorePassword is the password provided on export of the key.

9

Create an nspOS.public file. Execute:

```
# cp ca.pem nspOS.public
```

10

On the NFM-T host server, enter the following commands, in sequence:

```
# mkdir /opt/tls
# cd /opt/tls
```

11

Transfer the ca.jks and nspOS.public files from the server where the PKI server is running to the /opt/tls directory on the NFM-T host server.

12

Generate the JKS keystore for NFM-T; enter the following:

Note: You must enclose a password that contains a special character in single quotation marks; for example:
`-storepass 'MyPassword' -keypass 'MyPassword'`
The storepass and keypass passwords must also be identical.

```
# path/keytool -genkeypair -keyalg RSA -keystore nfmtKeystore.jks
-alias nfmt -storepass keystorePassword -keypass keyPassword -dname
CN=NSP,O=Nokia -validity 7300
```

where

path is the path to the keytool utility

keystorePassword is the password used with the keystore. This must be the same keystore password provided in Step 8.

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

13

Generate a CSR from the created JKS file; enter the following:

Note: You must enclose a password that contains a special character in single quotation marks; for example:
`-storepass 'MyStorePassword'`

```
# path/keytool -certreq -keystore nfmtKeystore.jks -alias nfmt -file
nfmt.csr -storepass keystorePassword -ext san=IP:127.0.0.1,IP:NFM-T
primary IP,IP:NFM-T standby IP -validity 7300
```

where

path is the path to the keytool utility

keystorePassword is the password used with the keystore

NFM-T primary IP is the IP address of the primary NFM-T host server

NFM-T standby IP is the IP address of the standby NFM-T host server

14

Sign the certificates using the CA of the PKI server; enter the following:

Note: You must enclose a password that contains a special character in single quotation marks; for example:
-storepass 'MyPassword' -keypass 'MyPassword'
The storepass and keypass passwords must also be identical.

```
# path/keytool -gencert -storepass keystorePassword -keystore ca.jks
-keypass keyPassword -alias test -ext ku:c=digitalSignature,
keyEncipherment -ext eku:c=serverAuth,clientAuth -rfc -ext honored=all
-infile nfmt.csr -outfile nfmt.public -validity 7300
```

where

path is the path to the keytool utility

keystorePassword is the password used with the keystore

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

15

Create an nfmtKeystore.jks.p12 file; enter the following:

Note: You must enclose a password that contains a special character in single quotation marks; for example:
-deststorepass 'MyPassword' -destkeypass 'MyPassword'
The deststorepass and destkeypass passwords must also be identical.

```
# path/keytool -importkeystore -noprompt -srckeystore nfmtKeystore.jks
-destkeystore nfmtKeystore.jks.p12 -deststoretype PKCS12
-deststorepass keystorePassword -destkeypass keystorePassword
-srcstorepass keyPassword -srckeypass keyPassword -alias nfmt
```

where

path is the path to the keytool utility

keystorePassword is the password used with the keystore

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

16

Create an nfmt.private file. Execute:

```
# openssl pkcs12 -in nfmtKeystore.jks.p12 -passin pass:keyPassword
-nodes -nocerts -out nfmt.private
```

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

17

In the /opt/tls directory, create a file called tls.info and add the following lines:

- custom_certificate_path=/opt/tls/nfmt.public
- custom_private_key_path=/opt/tls/nfmt.private
- nspOS_public_key=/opt/tls/nspOS.public

18

Execute the following commands on the Active NFM-T system's host server to complete the integration:

```
# cd /var/autoinstall/R18.3/
# ./utilities/nfmt-ext-nspOS-Integration.sh bench=benchName
ssl=/opt/tls/tls.info nspOS=Primary NFM-P IP\;Standby NFM-P IP
# ./utilities/execOnBench.sh benchName complete start
```

where

benchName is the name of the bench

Primary NFM-P IP is the IP address of the primary NFM-P system

Standby NFM-P IP is the IP address of the standby NFM-P system

19

Launch the NFM-T from the NFM-P systems Launchpad. Perform the following on both the primary and standby NFM-T systems:

1. From the NFM-T dashboard, choose ADMINISTER→Schedule→Scheduler from the drop-down menu to open the Scheduler GUI.
2. From the Scheduler GUI, select SDN-DR-Monitor, right click, and select Activate from the contextual menu.

20

Disable the applications that are unsupported by the deployment.

1. Sign in to the NSP as an administrator.
2. Choose More, Settings from the NSP Launchpad.
3. Click App Deployment Control.
4. Expand each application category.
5. Deselect the following applications in the following categories:
   - **Analyze / Assure**—Analytics, Link Utilization, Subscriber Manager, Telemetry
   - **Manage Data Centers / SD WAN**—Inventory Management, Service Navigator
   - **Manage Wireless**—Wireless NE View, Wireless Supervision
   - **Administer NSP**—VNF Manager
6. Select the check box to indicate that you understand the implications of the changes.
7. Click Save.
8. Close the Settings window.

END OF STEPS

17 NSP system conversion

17.1 Introduction

17.1.1 Description

This chapter provides procedures for NSP system conversion operations such as the following:

- standalone NSP system conversion to HA or redundancy
- redundant NSP system conversion to HA with redundancy
- HA NSP system conversion to redundancy
- NSP system conversion to IPv6

Note: As a result of an NSP system conversion, you may need to update the configuration of other NSP components to support the modified deployment, for example, if component IP addresses change.

When you convert a standalone NSP or NFM-P system that includes one or more NSP analytics servers to a redundant system, you must perform 17.5 “To enable redundancy support on an NSP analytics server” (p. 244).

17.2 To convert a standalone NSD and NRC system to a redundant NSD and NRC system

17.2.1 Purpose

Use this procedure to convert a previously-installed standalone NSD and NRC system to an NSD and NRC system with 1+1 redundancy.

Note: Upon converting to a redundant NSD and NRC system, TLS communication configurations must be updated so that the IP addresses of both the active and standby NSD and NRC servers are included in the SAN entries.

Note: If this NSD and NRC system will be deployed alongside an NFM-P system, that system must also be deployed in a redundant configuration. See the *NSP NFM-P Installation and Upgrade Guide* for more information.

17.2.2 Steps

1

Open the *NSP_installer_directory*/hosts file with a plain-text editor such as vi, where *NSP_installer_directory* is the directory where the NSP installer package was extracted.

2

Modify the entries for each component that the NSP servers will host to use the 1+1 redundancy values. See 13.2.1 “Description” (p. 101) for more information.

3

Copy the required license files to the *NSP_installer_directory*/license directory.

4

In the config.yml file, configure the auto_start parameter with a value of false.

5

Shut down all the active processes on the active, standalone NSP server. Execute:

```
nspdctl --host <nspServer_IP_address> stop ↲
```

```
systemctl stop nspos-nspd ↲
```

Where *nspServer_IP_address* is the IP address of the desired NSP server.

6

Start the NSP PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 12.8 “To configure and enable an NSP PKI server” (p. 91).

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

7

Install the NSP servers. Execute the following commands on one of the servers:

```
cd bin ↲
```

```
./install.sh ↲
```

The NSP servers are automatically deployed to both servers.

8

On what was previously the active, standalone NSP server, execute:

```
systemctl start nspos-nspd ↲
```

```
nspdctl --host <nspServer_IP_address> start ↲
```

Where *nspServer_IP_address* is the IP address of the desired NSP server.

9

On the standby NSP server, execute:

```
systemctl start nspos-nspd ↲
```

nspdctl --host <nspServer_IP_address> start ↵

Where *nspServer_IP_address* is the IP address of the desired NSP server.

10

If no other components are to be deployed, stop the NSP PKI server by entering CTRL+C in the console window.

11

Close the open console windows.

END OF STEPS

17.3 To convert redundant NSP servers to HA NSP servers with redundancy

17.3.1 Purpose

Use this procedure to convert existing, redundant NSP servers to HA NSP servers with redundancy.

Note: Upon converting to HA NSP servers with redundancy, TLS communication configurations must be updated so that the IP addresses of the additional servers in each cluster are included in the SAN entries.

Note: You must reconfigure the NFM-P and NFM-T systems that interact with the redundant NSP servers to include the IP addresses of the six servers in the new active and standby clusters.

17.3.2 Steps

1

Open the *NSP_installer_directory*/hosts file with a plain-text editor such as vi, where *NSP_installer_directory* is the directory where the NSP installer package was extracted.

2

Modify the entries for each component that the NSP servers will host to use the 1+1 redundancy values. See 13.2.1 “Description” (p. 101) for more information.

3

Copy the required license files to the *NSP_installer_directory*/license directory.

4

In the config.yml file, configure the auto_start parameter with a value of false.

5

Shut down all the active processes on the standby NSP server in the redundant deployment. Execute:

```
nspdctl --host <nspServer_IP_address> stop ↲
```

```
systemctl stop nspos-nspd ↲
```

Where *nspServer_IP_address* is the IP address of the desired NSP server.

6

Repeat Step 5 on the primary NSP server in the redundant NSD and NRC system.

7

Start the NSP PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 12.8 “To configure and enable an NSP PKI server” (p. 91).

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

8

Install the NSP servers. Execute the following commands on one of the servers:

```
cd bin ↲
```

```
./install.sh ↲
```

The intended components are automatically deployed to all NSP servers.

9

On what was previously the primary NSP server in the redundant deployment (now the first server in the primary datacenter), execute:

```
systemctl start nspos-nspd ↲
```

```
nspdctl --host <nspServer_IP_address> start ↲
```

Where *nspServer_IP_address* is the IP address of the desired NSP server.

10

Repeat Step 9 on the remaining two servers in the primary datacenter.

11

On what was previously the standby NSP server in the redundant deployment (now the first server in the standby datacenter), execute:

```
systemctl start nspos-nspd ↲
```

```
nspdctl --host <nspServer_IP_address> start ↲
```

Where *nspServer_IP_address* is the IP address of the desired NSP server.

12

Repeat Step 11 for the remaining two servers in the second datacenter.

13

If no other components are to be deployed, stop the NSP PKI server by entering CTRL+C in the console window.

14

Close the open console windows.

END OF STEPS

17.4 To convert an NSP system from IPv4 to IPv6

17.4.1 Purpose

CAUTION

Network management outage

Converting NSP system communication from IPv4 to IPv6 requires a shutdown of the entire NSP system and integrated products.

You must perform the procedure only with the assistance of technical support, and only during a maintenance window of sufficient duration.

Perform this procedure to convert the internal communication among all modules and components of an NSP system from IPv4 to IPv6.

Note: IPv6 support varies by product and deployment type; see the product *Planning Guide* for information.

Note: All NSP modules and components must be converted from IPv4 to IPv6 in one operation. The concurrent use of IPv4 and IPv6 among NSP modules and components is not supported.

Note: NSP communication with the managed network using IPv4 and IPv6 is supported, regardless of the protocol used for communication among NSP modules and components.

Note: To reduce the network outage duration, it is recommended that you plumb the required IPv6 addresses on each station in advance of performing the procedure.

17.4.2 Steps

1

Stop all NRC-X components; perform the following steps on each station that hosts the NRC-X module.

Note: In a redundant NRC-X deployment, you must perform the steps on the standby NRC-X station first.

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following commands in sequence:

   # **systemctl stop nspos-nspd** ↵

   # **nspdctl --host *address* stop** ↵

   where *address* is the IP address of the NRC-X host station

   The NRC-X server stops.

2

Stop all MDM components; perform the following steps on each MDM station.

Note: In a redundant MDM deployment, you must perform the steps on the standby MDM station first.

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following commands in sequence:

systemctl stop nsp-mediation.service ↵

The MDM server stops.

3

Stop each NFM-P component, in the following order:

- main servers, standby first in a redundant deployment
- main databases, standby first in a redundant deployment
- reserved auxiliary servers
- preferred auxiliary servers

See the *NSP NFM-P Administrator Guide* for information about stopping an NFM-P component.

4

Stop each NSD-NRC server; perform the following steps on each station that hosts the NSD-NRC.

Note: In a redundant NSD-NRC deployment, you must perform the steps on the standby NSD-NRC station first.

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following commands in sequence:

   # **systemctl stop nspos-nspd** ↵

   # **nspdctl --host *address* stop** ↵

   where *address* is the IP address of the NSD-NRC host station

   The NSD-NRC server stops.

5

If the IPv6 addresses for NSP communication are not plumbed, plumb each required IPv6 address on each station, and optionally, remove any IPv4 addresses that are no longer required.

6

Update the /etc/hosts on each NSP station by replacing each NSP IPv4 address with the required IPv6 address.

7

If you are using an NSP PKI server for TLS certificate generation, perform the following steps.

1. Start the PKI server, as described in 12.8 “To configure and enable an NSP PKI server” (p. 91).
2. Ensure that the PKI server is running and reachable over IPv6 by each NSP station.

8

Update the NSP installer hosts and configuration files by replacing each IPv4 address with the required IPv6 address.

9

Run the NSP installer to update the configuration for NSD, MDM, and NRC-X.

10

If the auto_start parameter in the relevant configuration file is set to false, start each NSD, MDM, and NRC-X manually:

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following commands in sequence:

   # **systemctl stop *service*** ↵

   # **nspdctl --host *address* start** ↵

   where:

   - *service* is **nspos-nspd** for an NSD-NRC or NRC-X host station, or **nsp-mediation.service** for an MDM server

- *address* is the IP address of the NSD-NRC host station, if applicable

11

Perform the IPv6 conversion procedure for a standalone or redundant NFM-P system, as required, in the *NSP NFM-P Installation and Upgrade Guide*.

12

If no other components are to be deployed, stop the NSP PKI server by entering CTRL+C in the console window.

13

Close the open console windows.

END OF STEPS

17.5 To enable redundancy support on an NSP analytics server

17.5.1 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.

17.5.2 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 NSP PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 12.8 “To configure and enable an NSP PKI server” (p. 91).

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

For information about a parameter, see Table 14-1, “NSP analytics server parameters” (p. 135).

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 NSP PKI server by entering CTRL+C in the console window.

11

Close the open console windows.

12

Close the console window.

END OF STEPS

17.6 To add MDM servers

17.6.1 Purpose

Perform this procedure to convert a standalone MDM server to an HA MDM cluster, or to add MDM servers to an MDM cluster.

The `fault_tolerance` parameter in the configuration file indicates the number of standby servers in the MDM cluster. The number of standby servers cannot exceed the number of active servers. See 13.3 “NSP configuration file” (p. 108) for more information about the configuration file.

This procedure can be performed on a running system unless you need to change the number of standby servers, that is, unless you need to change the `fault_tolerance` parameter.

17.6.2 Steps

1

Log in to the NSP server station as the root user.

2

Open a console window.

3

Add the IP addresses of the new servers to the `[mdm]` list in the NSP hosts file.

See 13.2 “NSP hosts file” (p. 101) for information about the hosts file.

4

Start the NSP PKI server, regardless of whether you are using the automated or manual TLS configuration method; perform 12.8 “To configure and enable an NSP PKI server” (p. 91).

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

5

If all the servers you are adding will be active servers, go to Step 8.

Add standby servers

6

Enter the following to stop the NSP server:

nspdctl--host *nspServer_IP_address* stop ↵

systemctl stop nspos-nspd ↵

where *nspServer_IP_address* is the IP address of the NSP server

7

Update the fault_tolerance parameter in the config.yml file.

8

Enter the following:

#**cd NSD_NRC_R_r/bin** ↵

Enter the following to install the MDM server software on the NSP server station:

#**./install.sh** ↵

The MDM server software is installed.

9

If the auto_start parameter in the config.yml is set to false, enter the following to start the NSP server:

systemctl start nspos-nspd ↵

nspdctl--host *nspServer_IP_address* start ↵

where *nspServer_IP_address* is the IP address of the NSP server

10

Optionally, perform the following to rebalance the cluster load:

POST https://{{*nspos_host*}}:
8545/mdm-necontrol-rest-api-app/api/v1/restconf/operations/rebalanceLoad

{

"rebalance-load" = [null]

}

where *nspos_host* is the IP address of the NSP server.

11

If no other components are to be deployed, stop the NSP PKI server by entering CTRL+C in the console window.

12

Close the open console windows.

END OF STEPS

18 NSP uninstallation

18.1 Introduction

18.1.1 Description

The procedures in this chapter describe how to uninstall the following NSP components:

- modules hosted on NSP server stations, such as MDM or the NSD and NRC
- NSP Flow Collectors
- NSP Flow Collector Controllers
- NSP analytics servers

For information about NFM-P uninstallation, see the *NSP NFM-P Installation and Upgrade Guide*.

For information about NFM-T uninstallation, see the *NFM-T Installation Guide*.

18.2 To uninstall the NSP server software

18.2.1 Purpose

The following steps describe how to remove the installed NSP software from one or more NSP server stations.

Note: You require the following user privileges:

- on the station that hosts the NSP installer software—root
- on each NSP server station—root

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

18.2.2 Steps

1

Log in as the root user on a station that has the downloaded and extracted NSP installer package.

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 path of the NSP installer package

R_r is the NSP software release, in the form *MAJOR_minor*

4

Perform one of the following.

a. Edit the hosts file in the directory to list only the addresses of the NSP servers to uninstall.

b. Create a new hosts file in the directory that lists only the addresses of the NSP servers to uninstall.

Note: The *NSP_installer_directory*/examples directory has an example hosts file. It is strongly recommended that you use a copy of the file, and not the original.

Note: The uninstaller uses the same root password on each NSP server in the list; ensure that you specify only servers that have the same root password.

5

Enter the following:

```
# ./bin/uninstall.sh ↵
```

You are prompted for the common root password of the NSP servers.

6

Enter the password.

The NSP software is removed from each server listed in the hosts file.

7

Close the console window.

END OF STEPS

18.3 To uninstall NSP Flow Collectors

18.3.1 Purpose

The following steps describe how 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.

18.3.2 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 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 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

18.4 To uninstall NSP Flow Collector Controllers

18.4.1 Purpose

The following steps describe how 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.

18.4.2 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 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 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

18.5 To uninstall an NSP analytics server

18.5.1 Purpose

The following steps describe how 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

18.5.2 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:

```
# su - ↵
```

6

Enter the following:

```
# yum erase nsp-analytics-server nspos-tomcat nspos-jre ↵
```

The yum utility resolves any package dependencies, and displays the following prompt:

```
Remove 3 Packages
Installed size: n.n G
Is this ok [y/N]:
```

7

Enter y ↵. The following and other progress messages are displayed:

```
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
```

When the removal of all packages is complete, the following is displayed:

```
Complete!
```

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

A Obtaining NSP software and documentation

A.1 Software

A.1.1 Software download

As a registered customer, you can download NSP software from the Nokia support portal. If you are a new customer and require access, contact your sales or support representative for registration information.

The NSP software on the Electronic Delivery→Downloads portal, also called ALED, is organized by release. You navigate through the hierarchy to select and download the packages you are licensed to use according to your purchase agreement.

NFM-T and NRC-T deliver software under their own product hierarchies in the portal.

After you select items for download and click Next, you must choose a download method. Click Help for information about the available download methods.

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

A.2 Documentation

A.2.1 Documentation architecture

NSP documentation consists of:

- application help
- product-level guides
- component-level guides
- component-specific tools

Application help

Each NSP application has application help to guide operators in the use of the interface. Help for applications is delivered in the NSP Help Center, which can be opened from a ? button on the NSP Launchpad or the application banner bar.

Product-level guides

Information about NSP in general, as well as about shared-mode compatibility and deployments, is communicated in product-level documentation.

The following documents apply to the entire NSP product:

- *NSP Deployment and Installation Guide* (this document)
- *NSP Lab Installer Reference**
- *NSP Planning Guide*
- *NSP Release Notice**
- *NSP System Administrator Guide*
- *NSP System Architecture Guide*

With the exception of the guides marked with an asterisk (*), these product-level guides are included in the on-product NSP Help Center.

Component-level guides

The NSP functions delivered by individual components are described in the component documentation. There are user documents and Release Notices for the following individually deployable components or component combinations:

- NFM-P
- NSD and NRCs

Component-level documentation is included in the on-product NSP Help Center.

Component-specific tools

NFM-P-specific developer tools and search tools for NFM-P alarms, statistics, and parameters continue to be delivered with NFM-P and are accessible under Help→Developer Tools in the NFM-P client GUI main menu. The content of these tools is not available in the NSP Help Center:

Developer tools in NFM-P:

- IPDR Reference
- JMS Example Code
- MV Metadata Navigator
- Schema Reference
- SDK Navigator
- Template Development Information
- XML API Reference

Search tools in NFM-P:

- Alarm Search Tool
- Parameter Search Tool
- Statistics Search Tool

A.2.2 NSP Help Center

Starting with NSP Release 19.6, NSP user documentation is delivered in an on-product application called the NSP Help Center. During NSP installation, the NSP Help Center loads the information content associated with each application and product component in your NSP deployment, providing you with end-to-end search capability across the user documentation, uncluttered by information irrelevant to your deployment.

The Help Center can be opened from a ? button available in every NSP application banner bar, as well as the NSP Launchpad. You can also open the Help Center from the Help menu in the NFM-P client GUI. You can browse the documentation from menus on the Help Center home page, or use the searching and filtering capabilities to isolate information quickly.

Searching

The Help Center application is centered on its robust search capabilities. Searches conducted from the home page search across documentation for all installed NSP components. As shown in the tooltip on the search bar, the boolean operators AND/OR/NOT are supported, as are the wildcard characters * (any string) and ? (any character). Exact-phrase search strings enclosed in quotation marks are also supported.

Note: Common, non-technical terms such as “the,” “and,” “on,” and others are ignored in all searches, including exact-string searches.

Search history is tracked as follows:

- The Recent Searches list on the home page is per-user, and the Popular Searches list shows the trend across all users of the system.
- When a search result link is clicked on the search results page, it is captured in the Recent Searches list and considered for forming the Popular Search list. Navigating to a page in any other way (for example, by browsing from the browse menu or following links within a browsed document) does not make the page eligible for capture in the Recent/Popular Searches list.

You can use the browser search to search within a page of content, or execute a new search from the search bar in the top right of your result page without having to return to the home page.

Filtering

You can filter your search results using filters in the left panel of the search results page.

You can filter by either or both of these facets:

- Application and Module Guides

  Select one or more applications or component-level documentation sets to narrow your search results to those areas.
- Content Type

  Select one or more content types to narrow your search results to hits that match the content type. For example, if your search term is “LSP” and you only want to see procedural information, select “Procedure” as the content type.

The content types for filtering are:

- Article - use-case-based material showcasing product or feature functionality

- Description - explanatory content
- Procedure - step-by-step instructions to complete a task
- Reference - brief look-up data, such as glossary terms
- Tool - content found in a developer toolset
- Workflow - a sequence of procedures to complete an objective

Browsing

From the home page, you can browse application help under APPLICATION GUIDES, or browse product-level and component-level guides under MODULE GUIDES. Once you have selected a guide or search result, you can browse within a guide using the table of contents tree in the left navigation panel.

Use the breadcrumbs in the search path to return to search results or the home page. Use the browser back button to return to any previously visited page.

A.2.3 Documentation delivery online

The documentation delivered on product in the NSP Help Center is also available online in PDF on the Nokia Documentation Center. If you are a new user and require access to the service, contact your support representative.

As a registered user, you can use the following link for direct access to the NSP product documentation: NSP user documentation

From the NSP product documentation page in the Documentation Center, you can:

- filter by release, model, category, content type, and format
- sort the results by title, document number, most accessed, or issue date
- search for documents
- search inside documents
- create a downloadable collection of your filtered documents

User documentation is filed under the “Manuals and Guides” content type; Release Notices and Release Descriptions are filed under “Release Information.”

Documentation alerts

To receive an e-mail when new or reissued NSP customer documents are available, subscribe to the notification service on the Documentation Alerts Subscription page.

B NSP RHEL OS compliance with CIS benchmarks

B.1 Overview

B.1.1 Purpose

Appendix B, “NSP RHEL OS compliance with CIS benchmarks”describes the NSP compliance with the Center for Internet Security, or CIS, security benchmarks for the RHEL OS.

B.1.2 Contents

B.2 RHEL 7 CIS benchmarks and NSP compliance

B.2.1 Description

Table B-1, “RHEL 7 CIS benchmarks and NSP compliance” (p. 261) lists the CIS v2.1.0 benchmarks for RHEL 7, and describes the NSP compliance with each.

The compliance applies to the RHEL 7 OS on stations in the following NSP modules:

- NSD+NRC
- NFM-P

Note: The compliance is for the Level 2 - Server profile.

Compliance indicators

The following compliance indicators are used:

- Supported—The product is fully compliant with the recommendation.
- No expected impact—The product team has not explicitly tested using the recommended configuration, but foresees no effect on system functions.

  It is recommended that you test such a configuration to ensure that system operation is unaffected; no commitment is offered to ensure product compatibility with a specific requirement.
- Partially supported—The product is conditionally compliant with the recommendation, as described in the Notes column.
- Not supported—The product does not support the recommended configuration.

Table B-1 RHEL 7 CIS benchmarks and NSP compliance

Section	Recommendation	Compliance	Notes
1.1	**Filesystem Configuration**		

Table B-1 RHEL 7 CIS benchmarks and NSP compliance (continued)

Section	Recommendation	Compliance	Notes
1.1.1	Disable unused filesystems		
1.1.1.1	Ensure mounting of cramfs filesystems is disabled (Scored)	Supported	—
1.1.1.2	Ensure mounting of freevxfs filesystems is disabled (Scored)	Supported	—
1.1.1.3	Ensure mounting of jffs2 filesystems is disabled (Scored)	Supported	—
1.1.1.4	Ensure mounting of hfs filesystems is disabled (Scored)	Supported	—
1.1.1.5	Ensure mounting of hfsplus filesystems is disabled (Scored)	Supported	—
1.1.1.6	Ensure mounting of squashfs filesystems is disabled (Scored)	Supported	—
1.1.1.7	Ensure mounting of udf filesystems is disabled (Scored)	Supported	—
1.1.1.8	Ensure mounting of FAT filesystems is disabled (Scored)	Supported	—
1.1.2	Ensure separate partition exists for /tmp (Scored)	Supported	Customer determines appropriate partition size; disk space cannot be taken from partitions defined in NSP module installation guide
1.1.3	Ensure nodev option set on /tmp partition (Scored)	Supported	—
1.1.4	Ensure nosuid option set on /tmp partition (Scored)	Supported	—
1.1.5	Ensure noexec option set on /tmp partition (Scored)	Not supported	noexec option cannot be set on /tmp, which is required for product installation and configuration
1.1.6	Ensure separate partition exists for /var (Scored)	Supported	Customer determines appropriate partition size; disk space cannot be taken from partitions defined in NSP module installation guide

Table B-1 RHEL 7 CIS benchmarks and NSP compliance (continued)

Section	Recommendation	Compliance	Notes
1.1.7	Ensure separate partition exists for /var/tmp (Scored)	Supported	Customer determines appropriate partition size; disk space cannot be taken from partitions defined in NSP module installation guide
1.1.8	Ensure nodev option set on /var/tmp partition (Scored)	Supported	—
1.1.9	Ensure nosuid option set on /var/tmp partition (Scored)	Supported	—
1.1.10	Ensure noexec option set on /var/tmp partition (Scored)	Not supported	noexec option cannot be set on /var/tmp, which is required for product installation and configuration
1.1.11	Ensure separate partition exists for /var/log (Scored)	Supported	Customer determines appropriate partition size; disk space cannot be taken from partitions defined in NSP module installation guide
1.1.12	Ensure separate partition exists for /var/log/audit (Scored)	Supported	Customer determines appropriate partition size; disk space cannot be taken from partitions defined in NSP module installation guide
1.1.13	Ensure separate partition exists for /home (Scored)	Supported	Customer determines appropriate partition size; disk space cannot be taken from partitions defined in NSP module installation guide
1.1.14	Ensure nodev option set on /home partition (Scored)	Supported	—
1.1.15	Ensure nodev option set on /dev/shm partition (Scored)	Supported	—
1.1.16	Ensure nosuid option set on /dev/shm partition (Scored)	Not supported	Not supported by Oracle
1.1.17	Ensure noexec option set on /dev/shm partition (Scored)	Not supported	Not supported by Oracle
1.1.18	Ensure nodev option set on removable media partitions (Not Scored)	Supported	Supported, but may affect ability to install NSP or patches from DVD drive or USB device

Table B-1 RHEL 7 CIS benchmarks and NSP compliance (continued)

Section	Recommendation	Compliance	Notes
1.1.19	Ensure nosuid option set on removable media partitions (Not Scored)	Supported	Supported, but may affect ability to install module or patches from DVD drive or USB device
1.1.20	Ensure noexec option set on removable media partitions (Not Scored)	Supported	Supported, but may affect ability to install module or patches from DVD drive or USB device
1.1.21	Ensure sticky bit is set on all world-writable directories (Scored)	Supported	—
1.1.22	Disable Automounting (Scored)	Supported	—
1.2	**Configure Software Updates**		
1.2.1	Ensure package manager repositories are configured (Not Scored)	Supported	—
1.2.2	Ensure gpgcheck is globally activated (Scored)	Supported	—
1.2.3	Ensure GPG keys are configured (Not Scored)	Supported	—
1.2.4	Ensure Red Hat Network or Subscription Manager connection is configured (Not Scored)	Supported	—
1.2.5	Disable the rhnsd Daemon (Not Scored)	Supported	—
1.3	**Filesystem Integrity Checking**		
1.3.1	Ensure AIDE is installed (Scored)	Not supported	May affect system performance
1.3.2	Ensure filesystem integrity is regularly checked (Scored)	Not supported	Requires AIDE
1.4	**Secure Boot Settings**		
1.4.1	Ensure permissions on bootloader config are configured (Scored)	Supported	—
1.4.2	Ensure bootloader password is set (Scored)	No expected impact	—
1.4.3	Ensure authentication required for single user mode (Not Scored)	No expected impact	—
1.5	**Additional Process Hardening**		

Table B-1 RHEL 7 CIS benchmarks and NSP compliance (continued)

Section	Recommendation	Compliance	Notes
1.5.1	Ensure core dumps are restricted (Scored)	Not supported	Core files required for customer software support
1.5.2	Ensure XD/NX support is enabled (Not Scored)	Supported	—
1.5.3	Ensure address space layout randomization (ASLR) is enabled (Scored)	Supported	—
1.5.4	Ensure prelink is disabled (Scored)	Supported	—
1.6	**Mandatory Access Control**		
1.6.1	Configure SELinux		
1.6.1.1	Ensure SELinux is not disabled in bootloader configuration (Scored)	Not supported	SELinux is not supported.
1.6.1.2	Ensure the SELinux state is enforcing (Scored)	Not supported	SELinux is not supported.
1.6.1.3	Ensure SELinux policy is configured (Scored)	Not supported	SELinux is not supported.
1.6.1.4	Ensure SETroubleshoot is not installed (Scored)	Not supported	SELinux is not supported.
1.6.1.5	Ensure the MCS Translation Service (mcstrans) is not installed (Scored)	Not supported	SELinux is not supported.
1.6.1.6	Ensure no unconfined daemons exist (Scored)	Not supported	SELinux is not supported.
1.6.2	Ensure SELinux is installed (Scored)	Not supported	SELinux is not supported.
1.7	**Warning Banners**		
1.7.1	Command Line Warning Banners		
1.7.1.1	Ensure message of the day is configured properly (Scored)	Supported	—
1.7.1.2	Ensure local login warning banner is configured properly (Not Scored)	Supported	—
1.7.1.3	Ensure remote login warning banner is configured properly (Not Scored)	Supported	—
1.7.1.4	Ensure permissions on /etc/motd are configured (Not Scored)	Supported	—

Table B-1 RHEL 7 CIS benchmarks and NSP compliance (continued)

Section	Recommendation	Compliance	Notes
1.7.1.5	Ensure permissions on /etc/issue are configured (Scored)	Supported	—
1.7.1.6	Ensure permissions on /etc/issue.net are configured (Not Scored)	Supported	—
1.7.2	Ensure GDM login banner is configured (Scored)	Supported	—
1.8	**Ensure updates, patches, and additional security software are installed (Not Scored)**	Partially supported	Applying RHEL patches is supported, but compatibility issues require backing out RHEL updates until a fix is available. Nokia does not recommend installing any additional software on the OS that hosts the NSP because it may affect NSP operation. Any non-sanctioned software must be removed if the software is suspected of causing NSP issues.
2	**Services**		
2.1	**inetd Services**		
2.1.1	Ensure chargen services are not enabled (Scored)	Supported	—
2.1.2	Ensure daytime services are not enabled (Scored)	Supported	—
2.1.3	Ensure discard services are not enabled (Scored)	Supported	—
2.1.4	Ensure echo services are not enabled (Scored)	Supported	—
2.1.5	Ensure time services are not enabled (Scored)	Supported	—
2.1.6	Ensure tftp server is not enabled (Scored)	Supported	Supported, but TFTP may be required for management of some NE types
2.1.7	Ensure xinetd is not enabled (Scored)	Supported	—
2.2	**Special Purpose Services**		

Table B-1 RHEL 7 CIS benchmarks and NSP compliance (continued)

Section	Recommendation	Compliance	Notes
2.2.1	Time Synchronization		
2.2.1.1	Ensure time synchronization is in use (Not Scored)	Supported	—
2.2.1.2	Ensure ntp is configured (Scored)	Supported	—
2.2.1.3	Ensure chrony is configured (Scored)	Supported	—
2.2.2	Ensure X Window System is not installed (Scored)	Supported	Supported, but may affect ability to run local GUI client on server
2.2.3	Ensure Avahi Server is not enabled (Scored)	Supported	—
2.2.4	Ensure CUPS is not enabled (Scored)	Supported	—
2.2.5	Ensure DHCP Server is not enabled (Scored)	Supported	—
2.2.6	Ensure LDAP server is not enabled (Scored)	Supported	—
2.2.7	Ensure NFS and RPC are not enabled (Scored)	Supported	—
2.2.8	Ensure DNS Server is not enabled (Scored)	Supported	—
2.2.9	Ensure FTP Server is not enabled (Scored)	Supported	—
2.2.10	Ensure HTTP server is not enabled (Scored)	Supported	—
2.2.11	Ensure IMAP and POP3 server is not enabled (Scored)	Supported	—
2.2.12	Ensure Samba is not enabled (Scored)	Supported	—
2.2.13	Ensure HTTP Proxy Server is not enabled (Scored)	Supported	—
2.2.14	Ensure SNMP Server is not enabled (Scored)	Supported	—
2.2.15	Ensure mail transfer agent is configured for local-only mode (Scored)	Supported	—
2.2.16	Ensure NIS Server is not enabled (Scored)	Supported	—

Table B-1 RHEL 7 CIS benchmarks and NSP compliance (continued)

Section	Recommendation	Compliance	Notes
2.2.17	Ensure rsh server is not enabled (Scored)	Supported	—
2.2.18	Ensure talk server is not enabled (Scored)	Supported	—
2.2.19	Ensure telnet server is not enabled (Scored)	Supported	—
2.2.20	Ensure tftp server is not enabled (Scored)	Supported	Supported, but TFTP may be required for management of some NE types
2.2.21	Ensure rsync service is not enabled (Scored)	Supported	—
2.3	**Service Clients**		
2.3.1	Ensure NIS Client is not installed (Scored)	Supported	—
2.3.2	Ensure rsh client is not installed (Scored)	Supported	—
2.3.3	Ensure talk client is not installed (Scored)	Supported	—
2.3.4	Ensure telnet client is not installed (Scored)	Supported	—
2.3.5	Ensure LDAP client is not installed (Scored)	Supported	—
3	**Network Configuration**		
3.1	**Network Parameters (Host Only)**		
3.1.1	Ensure IP forwarding is disabled (Scored)	Supported	—
3.1.2	Ensure packet redirect sending is disabled (Scored)	Supported	—
3.2	**Network Parameters (Host and Router)**		
3.2.1	Ensure source routed packets are not accepted (Scored)	Supported	—
3.2.2	Ensure ICMP redirects are not accepted (Scored)	Supported	—
3.2.3	Ensure secure ICMP redirects are not accepted (Scored)	Supported	—

Table B-1 RHEL 7 CIS benchmarks and NSP compliance (continued)

Section	Recommendation	Compliance	Notes
3.2.4	Ensure suspicious packets are logged (Scored)	Supported	Supported, but may affect system performance
3.2.5	Ensure broadcast ICMP requests are ignored (Scored)	Supported	—
3.2.6	Ensure bogus ICMP responses are ignored (Scored)	Supported	—
3.2.7	Ensure Reverse Path Filtering is enabled (Scored)	Supported	—
3.2.8	Ensure TCP SYN Cookies is enabled (Scored)	Supported	—
3.3	**IPv6**		
3.3.1	Ensure IPv6 router advertisements are not accepted (Scored)	Supported	—
3.3.2	Ensure IPv6 redirects are not accepted (Scored)	Supported	—
3.3.3	Ensure IPv6 is disabled (Not Scored)	Supported	—
3.4	**TCP Wrappers**		
3.4.1	Ensure TCP Wrappers is installed (Scored)	Supported	—
3.4.2	Ensure /etc/hosts.allow is configured (Scored)	Supported	—
3.4.3	Ensure /etc/hosts.deny is configured (Scored)	Supported	—
3.4.4	Ensure permissions on /etc/hosts.allow are configured (Scored)	Supported	—
3.4.5	Ensure permissions on /etc/hosts.deny are 644 (Scored)	Supported	—
3.5	**Uncommon Network Protocols**		
3.5.1	Ensure DCCP is disabled (Not Scored)	Supported	—
3.5.2	Ensure SCTP is disabled (Not Scored)	Supported	—
3.5.3	Ensure RDS is disabled (Not Scored)	Supported	—
3.5.4	Ensure TIPC is disabled (Not Scored)	Supported	—
3.6	**Firewall Configuration**		

Table B-1 RHEL 7 CIS benchmarks and NSP compliance (continued)

Section	Recommendation	Compliance	Notes
3.6.1	Ensure iptables is installed (Scored)	Supported	—
3.6.2	Ensure default deny firewall policy (Scored)	Supported	—
3.6.3	Ensure loopback traffic is configured (Scored)	Supported	—
3.6.4	Ensure outbound and established connections are configured (Not Scored)	Supported	See the NSP firewall requirements in the Security section of the module Planning Guide.
3.6.5	Ensure firewall rules exist for all open ports (Scored)	Supported	See the NSP firewall requirements in the Security section of the module Planning Guide.
3.7	**Ensure wireless interfaces are disabled (Not Scored)**	Supported	—
4	**Logging and Auditing**		
4.1	**Configure System Accounting (auditd)**		
4.1.1	Configure Data Retention		
4.1.1.1	Ensure audit log storage size is configured (Not Scored)	Supported	Default size of 6 Mbytes recommended
4.1.1.2	Ensure system is disabled when audit logs are full (Scored)	Supported	Supported, but not recommended
4.1.1.3	Ensure audit logs are not automatically deleted (Scored)	Supported	—
4.1.2	Ensure auditd service is enabled (Scored)	Supported	—
4.1.3	Ensure auditing for processes that start prior to auditd is enabled (Scored)	No expected impact	—
4.1.4	Ensure events that modify date and time information are collected (Scored)	Supported	—
4.1.5	Ensure events that modify user/group information are collected (Scored)	Supported	—
4.1.6	Ensure events that modify the system's network environment are collected (Scored)	Supported	—

Table B-1 RHEL 7 CIS benchmarks and NSP compliance (continued)

Section	Recommendation	Compliance	Notes
4.1.7	Ensure events that modify the system's Mandatory Access Controls are collected (Scored)	Not supported	SELinux is not supported.
4.1.8	Ensure login and logout events are collected (Scored)	Supported	—
4.1.9	Ensure session initiation information is collected (Scored)	Supported	—
4.1.10	Ensure discretionary access control permission modification events are collected (Scored)	Supported	—
4.1.11	Ensure unsuccessful unauthorized file access attempts are collected (Scored)	Supported	—
4.1.12	Ensure use of privileged commands is collected (Scored)	No expected impact	—
4.1.13	Ensure successful file system mounts are collected (Scored)	Supported	—
4.1.14	Ensure file deletion events by users are collected (Scored)	Supported	Supported, but may affect system performance
4.1.15	Ensure changes to system administration scope (sudoers) is collected (Scored)	Supported	—
4.1.16	Ensure system administrator actions (sudolog) are collected (Scored)	Supported	—
4.1.17	Ensure kernel module loading and unloading is collected (Scored)	Supported	—
4.1.18	Ensure the audit configuration is immutable (Scored)	Supported	—
4.2	**Configure Logging**		
4.2.1	Configure rsyslog		
4.2.1.1	Ensure rsyslog Service is enabled (Scored)	Supported	—
4.2.1.2	Ensure logging is configured (Not Scored)	No expected impact	—
4.2.1.3	Ensure rsyslog default file permissions configured (Scored)	Supported	—

Table B-1 RHEL 7 CIS benchmarks and NSP compliance (continued)

Section	Recommendation	Compliance	Notes
4.2.1.4	Ensure rsyslog is configured to send logs to a remote log host (Scored)	No expected impact	—
4.2.1.5	Ensure remote rsyslog messages are only accepted on designated log hosts. (Not Scored)	Supported	An NSP server must not be configured as a log host.
4.2.2	Configure syslog-ng		
4.2.2.1	Ensure syslog-ng service is enabled (Scored)	Supported	—
4.2.2.2	Ensure logging is configured (Not Scored)	No expected impact	—
4.2.2.3	Ensure syslog-ng default file permissions configured (Scored)	Supported	—
4.2.2.4	Ensure syslog-ng is configured to send logs to a remote log host (Not Scored)	No expected impact	—
4.2.2.5	Ensure remote syslog-ng messages are only accepted on designated log hosts (Not Scored)	Supported	An NSP server must not be configured as a log host.
4.2.3	Ensure rsyslog or syslog-ng is installed (Scored)	Supported	—
4.2.4	Ensure permissions on all logfiles are configured (Scored)	No expected impact	—
4.3	**Ensure logrotate is configured (Not Scored)**	Supported	Supported, but troubleshooting may be affected if log files unavailable.
5	**Access, Authentication and Authorization**		
5.1	**Configure cron**		
5.1.1	Ensure cron daemon is enabled (Scored)	Supported	—
5.1.2	Ensure permissions on /etc/crontab are configured (Scored)	Supported	—
5.1.3	Ensure permissions on /etc/cron.hourly are configured (Scored)	Supported	—
5.1.4	Ensure permissions on /etc/cron.daily are configured (Scored)	Supported	—
5.1.5	Ensure permissions on /etc/cron.weekly are configured (Scored)	Supported	—

Table B-1 RHEL 7 CIS benchmarks and NSP compliance (continued)

Section	Recommendation	Compliance	Notes
5.1.6	Ensure permissions on /etc/cron.monthly are configured (Scored)	Supported	—
5.1.7	Ensure permissions on /etc/cron.d are configured (Scored)	Supported	—
5.1.8	Ensure at/cron is restricted to authorized users (Scored)	Supported	—
5.2	**SSH Server Configuration**		
5.2.1	Ensure permissions on /etc/ssh/sshd_ config are configured (Scored)	Supported	—
5.2.2	Ensure SSH Protocol is set to 2 (Scored)	Supported	—
5.2.3	Ensure SSH LogLevel is set to INFO (Scored)	Supported	—
5.2.4	Ensure SSH X11 forwarding is disabled (Scored)	Supported	Supported, but affects NSP client operation if client uses SSH X11 forwarding
5.2.5	Ensure SSH MaxAuthTries is set to 4 or less (Scored)	Supported	—
5.2.6	Ensure SSH IgnoreRhosts is enabled (Scored)	Supported	—
5.2.7	Ensure SSH HostbasedAuthentication is disabled (Scored)	Supported	—
5.2.8	Ensure SSH root login is disabled (Scored)	Not supported	Required for product installation
5.2.9	Ensure SSH PermitEmptyPasswords is disabled (Scored)	Supported	—
5.2.10	Ensure SSH PermitUserEnvironment is disabled (Scored)	Supported	—
5.2.11	Ensure only approved ciphers are used (Scored)	Supported	—
5.2.12	Ensure only approved MAC algorithms are used (Scored)	Supported	**NOTE:** If eNodeB NEs are managed, hmac-sha1 must be included.
5.2.13	Ensure SSH Idle Timeout Interval is configured (Scored)	Not supported	May affect OSS client operation

Table B-1 RHEL 7 CIS benchmarks and NSP compliance (continued)

Section	Recommendation	Compliance	Notes
5.2.14	Ensure SSH LoginGraceTime is set to one minute or less (Scored)	Supported	—
5.2.15	Ensure SSH access is limited (Scored)	No expected impact	—
5.2.16	Ensure SSH warning banner is configured (Scored)	Supported	—
5.3	**Configure PAM**		
5.3.1	Ensure password creation requirements are configured (Scored)	No expected impact	—
5.3.2	Ensure lockout for failed password attempts is configured (Scored)	Supported	—
5.3.3	Ensure password reuse is limited (Scored)	Supported	—
5.3.4	Ensure password hashing algorithm is SHA-512 (Scored)	Supported	—
5.4	**User Accounts and Environment**		
5.4.1	Set Shadow Password Suite Parameters		
5.4.1.1	Ensure password expiration is 90 days or less (Scored)	Partially supported	**NOTE:** The password expiration period for NSP Linux users must not be altered.
5.4.1.2	Ensure minimum days between password changes is 7 or more (Scored)	No expected impact	—
5.4.1.3	Ensure password expiration warning days is 7 or more (Scored)	Supported	—
5.4.1.4	Ensure inactive password lock is 30 days or less (Scored)	Partially supported	**NOTE:** The password expiration period for NSP Linux users must not be altered.
5.4.2	Ensure system accounts are non-login (Scored)	Supported	—
5.4.3	Ensure default group for the root account is GID 0 (Scored)	Supported	—
5.4.4	Ensure default user umask is 027 or more restrictive (Scored)	Not supported	—

Table B-1 RHEL 7 CIS benchmarks and NSP compliance (continued)

Section	Recommendation	Compliance	Notes
5.5	**Ensure root login is restricted to system console (Not Scored)**	Partially supported	May cause operational challenges during module installation, upgrade, or maintenance
5.6	**Ensure access to the su command is restricted (Scored)**	Not supported	—
6	**System Maintenance**		
6.1	**System File Permissions**		
6.1.1	Audit system file permissions (Not Scored)	Not supported	—
6.1.2	Ensure permissions on /etc/passwd are configured (Scored)	Supported	—
6.1.3	Ensure permissions on /etc/shadow are configured (Scored)	Supported	—
6.1.4	Ensure permissions on /etc/group are configured (Scored)	Supported	—
6.1.5	Ensure permissions on /etc/gshadow are configured (Scored)	Supported	—
6.1.6	Ensure permissions on /etc/passwd- are configured (Scored)	Supported	—
6.1.7	Ensure permissions on /etc/shadow- are configured (Scored)	Supported	—
6.1.8	Ensure permissions on /etc/group- are configured (Scored)	Supported	—
6.1.9	Ensure permissions on /etc/gshadow- are configured (Scored)	Supported	—
6.1.10	Ensure no world writable files exist (Scored)	Supported	—
6.1.11	Ensure no unowned files or directories exist (Scored)	Supported	—
6.1.12	Ensure no ungrouped files or directories exist (Scored)	Supported	—
6.1.13	Audit SUID executables (Not Scored)	Supported	—
6.1.14	Audit SGID executables (Not Scored)	Supported	—
6.2	**User and Group Settings**		

Table B-1 RHEL 7 CIS benchmarks and NSP compliance (continued)

Section	Recommendation	Compliance	Notes
6.2.1	Ensure password fields are not empty (Scored)	Supported	—
6.2.2	Ensure no legacy “+” entries exist in /etc/passwd (Scored)	Supported	—
6.2.3	Ensure no legacy “+” entries exist in /etc/shadow (Scored)	Supported	—
6.2.4	Ensure no legacy “+” entries exist in /etc/group (Scored)	Supported	—
6.2.5	Ensure root is the only UID 0 account (Scored)	Supported	—
6.2.6	Ensure root PATH Integrity (Scored)	Supported	—
6.2.7	Ensure all users' home directories exist (Scored)	Supported	—
6.2.8	Ensure users' home directories permissions are 750 or more restrictive (Scored)	Partially supported	Not supported for NSP users
6.2.9	Ensure users own their home directories (Scored)	Supported	—
6.2.10	Ensure users' dot files are not group or world writable (Scored)	Supported	—
6.2.11	Ensure no users have .forward files (Scored)	Supported	—
6.2.12	Ensure no users have .netrc files (Scored)	Supported	—
6.2.13	Ensure users' .netrc Files are not group or world accessible (Scored)	Supported	—
6.2.14	Ensure no users have .rhosts files (Scored)	Supported	—
6.2.15	Ensure all groups in /etc/passwd exist in /etc/group (Scored)	Supported	—
6.2.16	Ensure no duplicate UIDs exist (Scored)	Supported	—
6.2.17	Ensure no duplicate GIDs exist (Scored)	Supported	—
6.2.18	Ensure no duplicate user names exist (Scored)	Supported	—

Table B-1 RHEL 7 CIS benchmarks and NSP compliance (continued)

Section	Recommendation	Compliance	Notes
6.2.19	Ensure no duplicate group names exist (Scored)	Supported	—