NOKIA

NSP
Network Services Platform

Network Resource Controller - Flow (NRC-F)
Network Resource Controller - Packet (NRC-P)
Network Resource Controller - Transport (NRC-T)
Network Resource Controller - Cross domain (NRC-X)
Network Services Director
Release 17.9

Planning Guide

3HE-12074-AAAC-TQZZA

Issue 1

September 2017

Contents

List of tables

List of figures

About this document

Purpose

The *NSP NSD and NRC Planning Guide* consolidates all pre-installation information required to plan a successful deployment of the NSD and NRC modules of the Nokia NSP product.

Document support

Customer documentation and product support URLs:

Customer documentation welcome page

- https://infoproducts.alcatel-lucent.com/cgi-bin/doc_welc.pl

Technical support

- http://support.alcatel-lucent.com

How to comment

Documentation feedback

- Documentation Feedback

1 Product overview

1.1 NSP overview

1.1.1 Introduction

This chapter provides an overview of the Network Services Director (NSD) and Network Resource Controller (NRC) modules of the Network Services Platform (NSP).

1.1.2 NSP architecture

The NSP product consists of multiple interoperating network management modules for service provisioning, automation, optimization, and element management functions for IP and optical networks. The NSD and NRC modules provide the following functionality:

- Network Resource Controller – Flow (NRC-F) – Traffic flow management
- Network Resource Controller – Packet (NRC-P) – MPLS path computation
- Network Resource Controller – Transport (NRC-T) – Optical path computation
- Network Services Director (NSD) – service provisioning and activation
- NRC Cross Domain Coordination (NRC-X)

As part of the NSP architecture, the NSD and NRC modules work with the following element management systems:

- Network Functions Manager - Packet, or NFM-P (formerly 5620 SAM)
- Network Functions Manager - Transport, or NFM-T (formerly 1830 OMS)

1.1.3 NRC-F

The NRC-F is the flow controller module of the NSP. It uses flow-based protocols to perform intelligent traffic steering, and to automate policy-based redirection. The NRC-F monitors NEs discovered and statistics collected by the NFM-P. A vCPAA must be integrated with the NFM-P where the NRC-F monitors an AS.

In an NRC-F deployment, the VSR-NRC serves as an OpenFlow controller. The VSR-NRC pushes flow management information to OpenFlow switches as directed by the NRC-F.

1.1.4 NRC-P

The NRC-P manages the creation of LSPs across IP network elements (NEs). The NRC-P maintains a network topology and current path database synchronized with the NEs. A VSR-NRC is deployed as the NRC-P Path Computation Element (PCE) for CSPF computations for IS-IS and OSPF routing protocols. The NRC-P discovers the IGP network topology using the VSR-NRC.

This release supports the migration of networks discovered by CPAM in previous NSP releases to PCE SROS-based topology.

The VSR-NRC/PCE and VSR-NRC/OFC can be deployed on virtual machine instances, but these functions cannot reside on the same instance. For details about platform requirements, see the *Virtualized Service Router Installation and Setup Guide*.

1.1.5 NRC-T

The NRC-T manages transport path connections by maintaining an optical network topology and current path database that is synchronized with NEs. The NRC-T interoperates with the NFM-T element manager, which provides the optical network topology required for path computations.

1.1.6 NRC-X

The NRC-X optimizes network resources across different layers and domains of IP/MPLS and optical networks. The NRC-X is installed on a separate platform from the NSD and NRC modules. For the NSP Release 17.9, the NRC-X is deployed only in lab trials. In addition, the NRC-X does not support redundancy and does not work with redundant NSD and NRC-P/T systems in this release. Contact your Nokia representative for more details.

1.1.7 NSD

The NSD is the network service fulfillment module of the NSP. It provisions services using operator-defined policies across multi-domain networks. The NSD works with other NSP modules to perform service provisioning to specific elements.

1.1.8 nspOS

The nspOS is a set of platform services used by all NSP modules. The nspOS enables system-wide functions, including Single Sign On and operator access to the NSP Launchpad. The nspOS also contains common components and services that other NSP modules require.

The nspOS is installed with the NSD and NRC modules. In a multi-module deployment, each module uses the nspOS instance on the NSD and NRC host.

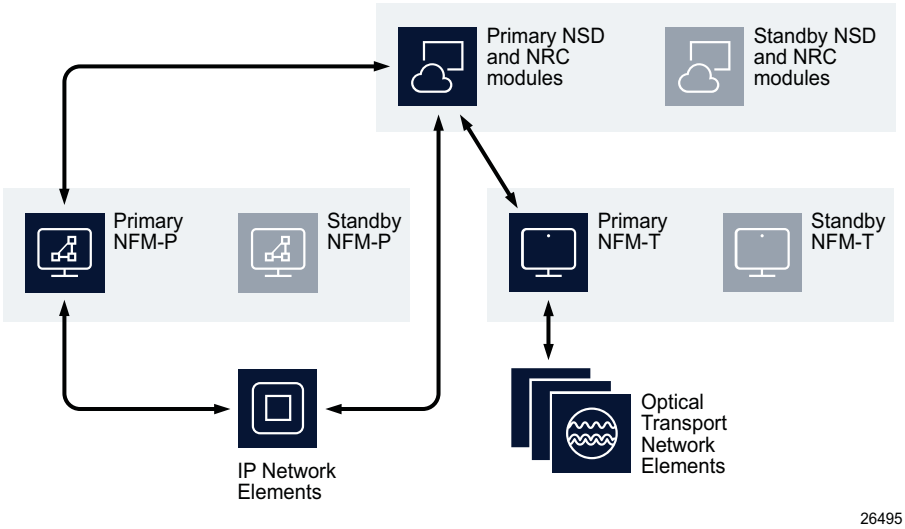
See the *NSP Deployment Overview* for details about the NSP modules and their deployment options.

1.1.9 NSD and NRC deployment overview

The NSD and NRC modules can be deployed as a standalone system or as an active/standby redundant pair. The modules are deployed with other applications, including the NFM-P and/or the NFM-T. Both the NFM-P and the NFM-T can be deployed in standalone or redundant configurations. The deployed configuration of an NSD and NRC system is not dependent on the redundancy mode of the NFM-P or the NFM-T. The NSD and NRC modules operate independently of the NFM-P and the NFM-T and will automatically reconnect to the primary server if an activity switch of the NFM-P or the NFM-T takes place.

The following figure shows a fully redundant deployment of all NSP modules:

Figure 1 Redundant deployment of NSP modules



The NSD and NRC modules can be installed on a bare metal, or a virtualized server. The NSD and NRC modules only support IPv4 connectivity with other components in the NSP architecture.

The NSD and NRC software is distributed in a tar file. An installation script will install multiple rpm packages for the NSD and NRC modules. See the *NSP NSD and NRC Installation and Upgrade Guide* for full installation instructions. The *NSP Release Notice* defines compatible software releases for other applications that can be deployed with the NSD and NRC modules.

1.2 NSD and NRC key technologies

1.2.1 Java virtual machine

The NSD and NRC modules use Java technology. The installation package contains a Java Virtual Machine which is installed with the software. This is a dedicated Java Virtual Machine and does not conflict with other JVMs which may be installed on the same workstation. The NSD and NRC modules use OpenJDK 8.

1.2.2 Databases

Embedded within the NSD and NRC host server is a Neo4j database (version 3.1) for network topology information and a PostgreSQL database (version 9.6.3) for policy management.

The Neo4j database contains a graphical representation of the network topology and its elements in a multi-layer graph. The installation of the Neo4j database is customized for, and must be dedicated to, the NSD and NRC modules. Nokia will not support any configuration that deviates from the NSD and NRC installation procedure.

The PostgreSQL database contains non-topological NSD and NRC information, including policies and templates. PostgreSQL is an open source database application. Nokia will not support any PostgreSQL database configuration that deviates from the NSD and NRC installation procedure.

Note: Nokia does not support direct customer access to the Neo4j and PostgreSQL databases.

1.2.3 Browser applications

The NSD and NRC modules provide functionality using browser-based applications. The NSD and NRC modules use standard REST security mechanisms for authentication and authorization. All NSD and NRC module applications are HTML-5 based and are supported on the latest desktop version of Google Chrome. The browser applications require that WebGL be enabled.

1.2.4 API

The NSD and NRC modules provide a northbound REST API with Swagger-compliant documentation. The northbound API supports queries, service creation requests, and other functions. Refer to the *NSP API Programmer Guide* for more information.

1.2.5 Network mediation

The NSD and NRC modules have southbound interfaces that consist of plug-ins that interact with the NFM-P and the NFM-T, as well as standard communication protocols to interface directly with network elements. The NSD and NRC modules will communicate with the NFM-P using CPROTO and HTTP protocols secured with TLS, and with the NFM-T using REST over TLS-secured HTTPS.

For NRC-P, a VSR-NRC PCE-configured element communicates with the PCC network elements via PCEP, IGP, and BGP-LS. For NRC-F, the OpenFlow Controller communicates to OpenFlow Switches using OpenFlow protocol.

The nspOS module hosts the Telemetry application, which communicates directly with NEs using GPRC.

The NFM-P manages IP network elements using SNMP, and the NFM-T uses TL-1 and SNMP to manage optical transport network elements.

2 Operating system specifications

2.1 Red Hat Enterprise Linux (RHEL)

2.1.1 Introduction

This chapter defines the operating system requirements for the NSD and NRC modules.

2.1.2 RHEL description and recommendations

The NSD and NRC modules are supported on Red Hat Enterprise Linux Server Edition 7.3 (x86-64). Previous releases, or other variants of Red Hat, and other Linux variants are not supported.

The NSD and NRC modules do not necessarily support all functionality provided in RHEL. SELinux, iptables, and Network Manager are not supported in NSD and NRC configurations. The NSD and NRC modules should use a time synchronization mechanism, such as NTP, to ensure accurate time. The NSD and NRC modules also require that the server hostname is configured in the */etc/hosts* file. RHEL must be installed in 64 bit mode where the NSD and NRC modules will be installed.

Customers are expected to purchase RHEL software and support for all platforms running RHEL Server with the NSD and NRC modules. It is strongly recommended to purchase a support package from Red Hat that provides 24x7 support.

Nokia recommends the installation of any OS, driver, or firmware updates that the hardware vendor advises for RHEL.

With the exception of documented Operating System parameter changes for NSD and NRC, all other settings must be left at the RHEL default configuration.

The *NSP NSD and NRC Installation and Upgrade Guide* provides detailed instructions for the RHEL OS installation.

2.1.3 Third-party applications

Applications that are not sanctioned by Nokia must not be running on any bare metal workstation or virtual instance running the NSD and NRC modules. Nokia reserves the right to remove any applications that are suspected of causing issues from workstations running NSD and NRC modules.

3 Platform requirements

3.1 Introduction

3.1.1 Overview

This chapter defines the platform requirements for successfully running the NSD and NRC modules. Follow these guidelines to ensure the modules perform adequately.

3.2 Hardware platform requirements

3.2.1 Overview

The NSD and NRC modules may be installed on bare metal, or virtual servers. For bare metal installations, x86-64 based workstations running RHEL must be used.

For optimal disk I/O performance, read and write caches must be enabled for each disk. Specific HBA controllers may be required for certain platforms to ensure that the read and write caches can be enabled. The server vendor should be consulted to determine the correct HBA controller and provide the procedure to enable the read and write caches. RAID 1 is recommended for a production system.

3.3 Hardware platform and resource requirements using virtualization

3.3.1 Overview

Virtualization is supported using both VMWare vSphere ESXi and RHEL KVM, including Openstack.

For NSD and NRC module installations on a Guest Operating System of a virtualized installation, the guest OS must be an NSD and NRC supported version of RHEL 7.3 Server x86-64.

Virtualized installations of NSD and NRC are server- and vendor-agnostic, but must meet any defined hardware criteria and performance targets to be used with the NSD and NRC modules. Server class hardware must be used, not desktops. Processors must be x86-64 based with a minimum core speed of 2.4GHz.

Defined CPU and Memory resources for a virtual machine must be reserved and dedicated to that guest OS, and cannot be shared or oversubscribed. Disk and network resources should be managed appropriately to ensure that other guest OSs on the same physical server do not negatively impact the operation of the NSD and NRC modules.

Provisioned CPU resources must be based upon CPU cores and not threads. If threaded CPUs are used, the number of vCPUs required should be multiplied by the number of threads per physical CPU core and assigned to the Virtual Machine.

Nokia support personnel must be provided with the details of the provisioned Virtual Machine. These details can either be provided through read-only access to the hypervisor or must be available to Nokia support when requested. Failure to provide these details could impact support of the NSD and NRC modules.

3.4 VMware Virtualization

3.4.1 Overview

The NSD and NRC modules support using VMware vSphere ESXi 6.0 or above, on x86 based servers natively supported by ESXi. VMware's Hardware Compatibility List (HCL) should be consulted to determine specific hardware support.

Not all features offered by ESXi are supported when using the NSD and NRC modules. For example, Fault Tolerant, High Availability (HA), Memory Compression, and Distributed Resource Scheduler (DRS) features are not supported. Nokia should be contacted to determine if a specific ESXi feature is supported with an NSD and NRC installation.

Virtual Machine Version 11 or above must be used. The disk must be "Thick Provisioned" with "Eager Zero" set. The SCSI controller must be set to "VMware Paravirtual" and the Disk Provisioning must be "Thick Provision Eager Zero". The Network Adapter must be "VMXNET 3". See the following table for additional Virtual Machine setting requirements:

Table 1 Additional Virtual Machine setting requirements

Resource type	Parameter	Setting
CPU	Shares	Set to High
	Reservation	Must be set to half the number of vCPUs * the CPU frequency. For example, on a 2.4 GHz 8 vCPU configuration, the reservation must be set to (1/2*8*2400) = 9600 MHz.
	Limit	Check box checked for unlimited
Advanced CPU	Hyperthreaded Core Sharing Mod	Set to None
Memory	Shares	Set to High
	Reservation	Slider set to the size of the memory allocated to the VM
	Limit	Check box checked for unlimited
Advanced Memory	NUMA Memory Affinity	No affinity
Disk	Shares	Set to High
	Limit — IOPs	Set to Unlimited

3.5 KVM virtualization

3.5.1 Overview

The NSD and NRC modules support using RHEL 6.3 through 6.7 KVM using QEMU version 0.12.1.2 and RHEL 7.2 KVM using QEMU version 1.5.3 and 2.3.0 only, on x86 based servers natively supported by KVM. Consult the RHEL's Hardware Compatibility List (HCL) to determine specific hardware support.

Not all features offered by KVM are supported when using the NSD and NRC modules. For example, Live Migration, Snapshots, or High Availability are not supported. Contact Nokia to determine if a specific KVM feature is supported with an installation of NSD and NRC modules.

3.5.2 Configuration

When you configure the KVM, set the parameters listed in the following table to the required values.

Table 2 KVM configuration parameters

Parameter	Value
Disk Controller type	virtio
Storage format	raw
Cache mode	none
I/O mode	native
I/O scheduler	deadline
NIC device model	virtio
Hypervisor type	kvm

3.6 Minimum hardware platform requirements

3.6.1 Overview

The hardware requirements of an NSD/NRC and NRC-X system depends on the following factors:

- Number of managed LSPs and services
- Number of managed elements
- Number of simultaneous user and API sessions
- Expected number of flows, monitored routers, number of ASes, number of ports with real-time statistics collection

The following tables list the minimum hardware platform requirements for the deployment of a lab RHEL x86-64 operating system for NSD and NRC, and NRC-X.

Lab NSD and NRC standalone	
CPU cores	4 (minimum 2.4 GHz)
Memory	recommended 32 GB, minimum 24 GB
Disk	1 SAS 10K RPM drive, 146 GB or more

Lab NRC-X	
CPU cores	4 (minimum 2.4 GHz)
Memory	minimum 32 GB
Disk	1 SAS 10K RPM drive, 160 GB or more

The following table lists the minimum hardware platform requirements for the deployment of an NSD and NRC production RHEL x86-64 operating system.

Production NSD and NRC system (standalone or redundant configuration)	
CPU cores	12 (minimum 2.4 GHz)
Memory	recommended 64 GB, minimum 42 GB
Disk	2 SAS 10K RPM drive, 270 GB or more

See the *NSP NSD and NRC Installation and Upgrade Guide* for disk partition recommendations.

3.7 Hostname requirements

3.7.1 Overview

The hostname of an NSD and NRC server must meet the following criteria:

- contains only ASCII alphanumeric characters
- cannot contain a hyphen
- cannot end with a period followed by a digit
- if the hostname is an FQDN, period characters delimit the FQDN components
- the FQDN of the hostname cannot exceed 63 characters

4 Network requirements

4.1 Overview

4.1.1 Introduction

This chapter describes the network requirements for an NSD and NRC system and the connectivity with other applications.

4.2 NSD and NRC to OSS clients

4.2.1 Bandwidth requirements

The bandwidth requirements depend on the number of concurrent connections and on the type of transactions that are performed. For a single provisioning thread, Nokia recommends to provide 50 kbps of bandwidth from the OSS client to the NSD and NRC server. An OSS client that performs frequent query operations (for example, port or service inventory) must be provided additional bandwidth.

4.3 NSD and NRC to GUI clients

4.3.1 Bandwidth requirements

The network size drives the primary bandwidth requirement for NSD and NRC to GUI clients. More NEs and services result in more data being sent from the NSD and NRC modules to GUI clients. Optimal GUI performance is achieved with 10 Mbps of bandwidth with minimal network latency. Nokia recommends to provide a minimum of 2.5 Mbps of bandwidth.

High network latency between the NSD and NRC modules and GUI clients slows GUI performance. Nokia recommends to limit the round-trip network latency time to 100 ms.

4.4 NSD and NRC to NFM-P

4.4.1 Bandwidth requirements

The bandwidth requirements depend on the following factors:

- the number of NEs, LSPs, and services configured on the NFM-P
- the frequency of NE updates to the NSD and NRC modules

When an NSD and NRC system re-synchronizes with the NFM-P, optimal performance is achieved with 50 Mbps of bandwidth between the NSD and NRC modules and the NFM-P. Nokia recommends to provide a minimum of 25 Mbps of bandwidth.

Network latency impacts the time it takes for the NSD and NRC modules to re-synchronize a large amount of data from the NFM-P. Nokia recommends to limit the round-trip network latency time to 100 ms.

4.5 NSD and NRC to NFM-T

4.5.1 Bandwidth requirements

The bandwidth requirements between the NSD and NRC modules and the NFM-T depend on the number of optical NEs and services configured in the network. Nokia recommends to provide 10 Mbps of bandwidth between the NSD and NRC modules and the NFM-T. High round-trip network latency affects GUI performance and must be limited to 100 ms.

4.6 Redundancy considerations

4.6.1 Overview

The network requirements between active/standby NSD and NRC servers depend on the network size (number of NEs and configured services) and the rate of service provisioning activities. The peak bandwidth requirement between redundant servers is 50 Mbps, with sustained bandwidth of 25 Mbps. Round-trip network latency between the redundant pair must be limited to 100ms.

5 Security

5.1 Introduction

5.1.1 Overview

This chapter provides general information about platform security for the NSD and NRC modules.

5.2 Securing the NSD and NRC modules

5.2.1 Overview

Nokia recommends you to perform the following steps to achieve workstation security for the NSD and NRC modules:

- Install the latest recommended patch cluster from Red Hat
- Implement firewall rules to control access to ports on NSD and NRC sytems, as detailed below

5.3 Operating system security for NSD and NRC workstationss

5.3.1 RHEL patches

Nokia supports customers applying RHEL patches provided by Red Hat which will include security fixes as well as functional fixes. If a patch is found to be incompatible with the NSD and NRC modules, the patch may need to be removed until a solution to the incompatibility is provided by Red Hat or Nokia. See the *NSP NSD and NRC Release Notice* for up-to-date information about the recommended RHEL maintenance update and patch levels.

5.3.2 Platform hardening

Additional efforts to secure the system could impact NSD and NRC operation or future upgrades of the product. Customers must perform some level of basic testing to validate additional platform hardening does not impact the operation of the NSD and NRC modules. The NSP Product Group makes no commitment to make the NSD and NRC modules compatible with a customer's hardening requirements.

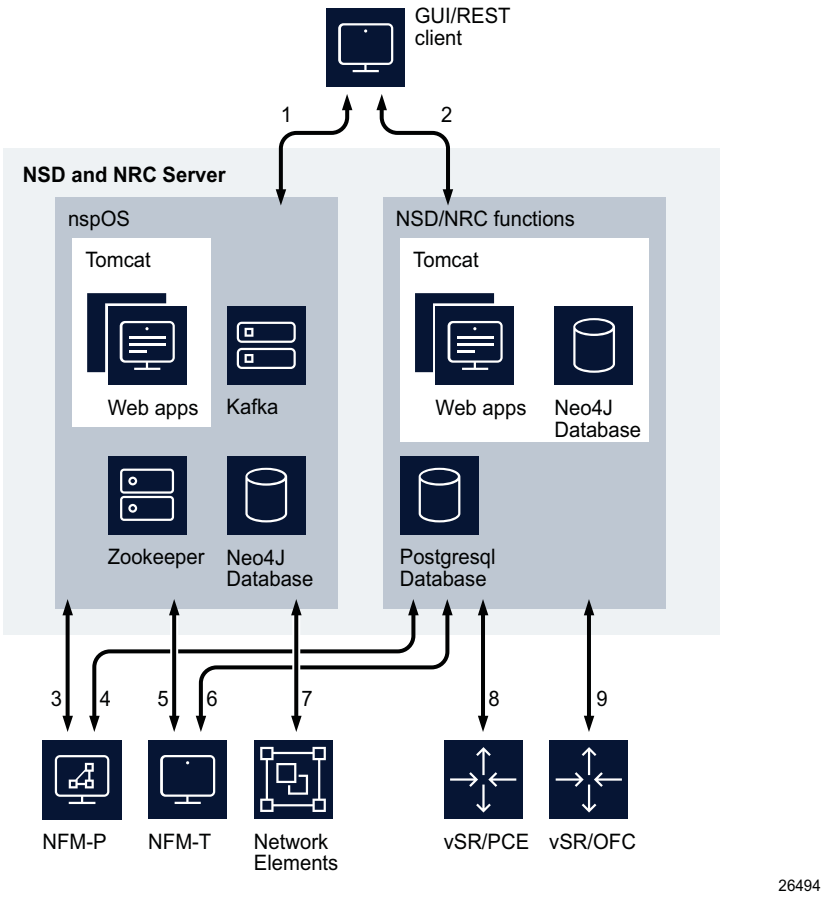
5.4 Communication between the NSD and NRC modules and external systems

5.4.1 Overview

The following diagrams illustrate the various components of the NSD and NRC modules and their internal communications, as well as communications with external systems.

The following figure shows a standalone NSD and NRC deployment and its communications with external systems.

Figure 2 Standalone NSD and NRC deployment



Connection	Usage
1,2	Web Client/REST API client connections. REST over HTTPS secured with TLS
3	SSO authentication (secure), zookeeper registration (non-secure), neo4j database (non-secure), kafka (non-secure)
4	Data connection - CPROTO protocol secured with TLS
5	SSO authentication (secure), zookeeper registration (non-secure)

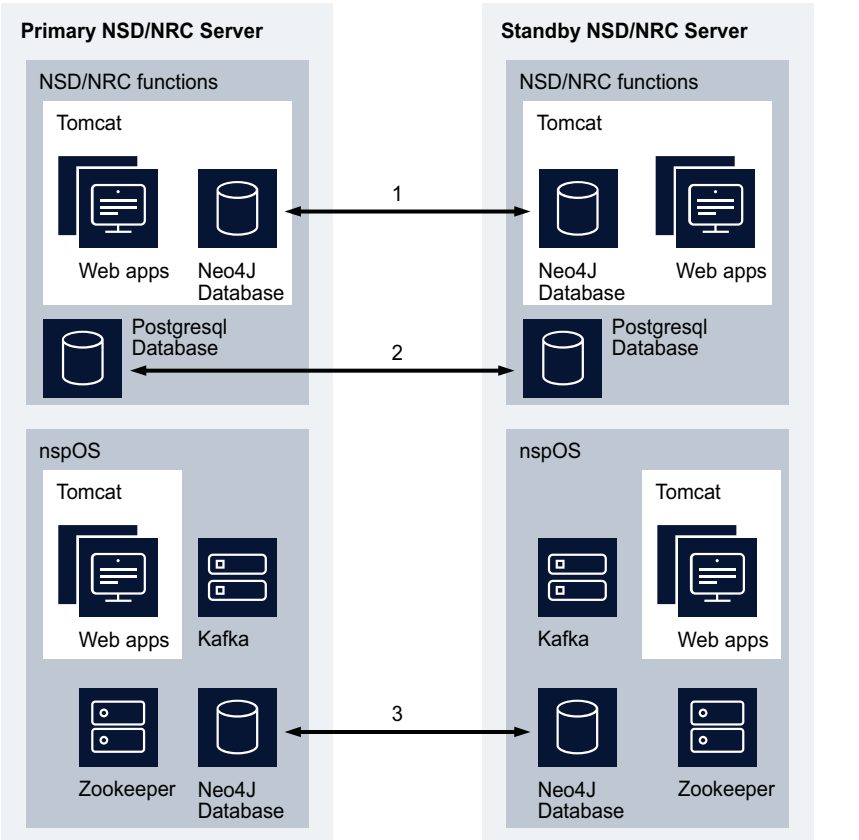
Connection	Usage
6	Data connection - REST over HTTPS secured with TLS
7	GPRC (for Telemetry) – secured with TLS NPN
8	Data connection - not secured
9	Data connection - not secured

5.5 Communication between redundant NSD and NRC server

5.5.1 Overview

The following figure shows the internal communications between redundant NSD and NRC servers:

Figure 3 Internal communications between redundant NSD and NRC servers



Connection	Usage
1	Neo4j data replication, not secured
2	Postgresql data replication, not secured
3	Neo4j data replication, not secured

5.6 NSD and NRC firewalls

5.6.1 Overview

A firewall can be deployed in an NSP topology to protect the NSD and NRC modules from different networks and applications.

The NSD and NRC modules do not support use of Network Address Translation (NAT) between its components or between itself and external applications (NFM-P/NFM-T/PCE/OFC).

Some NSD and NRC operations require idle TCP ports to remain open for long periods of time. Therefore, a customer firewall that closes idle TCP connections should adjust OS TCP keep-alives to ensure that the firewall will not close sockets that are in use by the NSD and NRC modules.

5.6.2 Firewall port requirements for NSD and NRC deployments

The following tables identify which ports need to be accessible in an NSD and NRC deployment within an NSP topology. The tables identify only the ports used between the NSD and NRC modules and other applications. See the respective product documentation for a complete list of firewall ports for other NSP modules.

Table 3 Listening ports for all communications with NSD/NRC

Application	Default port(s)	Type	Encryption	Description	NSD and NRC deployment
All	22	TCP	Dynamic Encryption	SSH/SCP/ SFTP Used for remote access and secure file transfer	Standalone and redundant

Table 3 Listening ports for all communications with NSD/NRC (continued)

Application	Default port(s)	Type	Encryption	Description	NSD and NRC deployment
NSD and NRC	5001	TCP	None	Neo4j database	Standalone and redundant
	5002	TCP	None	Neo4j database	Redundant only
	6017	TCP	None	Neo4j database	Standalone and redundant
	6018	TCP	None	Neo4j database	Redundant only
	8105	TCP	None	Java Tomcat	Standalone and redundant
	8223	TCP	None	Java Tomcat	Redundant only
	8543	TCP	Dynamic, SSL/TLS	Java Tomcat, secure HTTPS port for GUI and REST API	Standalone and redundant
	11211	TCP	None	Java Tomcat	Standalone and redundant
	47100 - 47199	TCP	None	Java Tomcat	Standalone and redundant
	47500 - 47599	TCP	None	Java Tomcat	Standalone and redundant

Table 3 Listening ports for all communications with NSD/NRC (continued)

Application	Default port(s)	Type	Encryption	Description	NSD and NRC deployment
nspOS	80	TCP	None	HTTP port for nspOS common applications, redirect to 443	Standalone and redundant
	443	TCP	Dynamic, SSL/TLS	Secure HTTPS port for nspOS common applications	Standalone and redundant
	2181	TCP	None	Zookeeper	Standalone and redundant
	2390	TCP	Dynamic, SSL/TLS	nspdctl	Standalone and redundant
	5007	TCP	None	Neo4j database	Standalone and redundant
	6007	TCP	None	Neo4j database	Standalone and redundant
	6432	TCP	None	PostgreSQL database	Standalone and redundant
	7473	TCP	Dynamic SSL/TLS	Neo4j database	Standalone and redundant
	7687	TCP	None	Neo4j database	Standalone and redundant
	9092	TCP	None	Kafka server	Standalone and redundant
VSR-NRC	4199	TCP	None	CPROTO	N/A

Table 3 Listening ports for all communications with NSD/NRC (continued)

Application	Default port(s)	Type	Encryption	Description	NSD and NRC deployment
NFM-P	7879	TCP	SSL/TLS	CPROTO	N/A
	8087	TCP	SSL/TLS	Web applications communications	N/A
	8543	TCP	SSL/TLS	Web applications communications	N/A
NFM-T	80	TCP	None	Used for redirect only	N/A
	8443	TCP	SSL/TLS	HTTPS-based communication	N/A

The following table lists the ports used in communication between the NSD and NRC modules and NFM-T:

Table 4 Ports used in communication between the NSD and NRC and NFM-T

Protocol	From port	From module	To port	To module
TCP	80	NFM-T presentation server	>32768	NSD/NRC
TCP	>32768	NSD/NRC	80	NFM-T presentation server
TCP	443	NSD/NRC	>15000	NFM-T
TCP	>15000	NFM-T	443	NSD/NRC
TCP	2181	NSD/NRC	>15000	NFM-T
TCP	>15000	NFM-T	2181	NSD/NRC
TCP	6432	NSD/NRC	>15000	NFM-T
TCP	>15000	NFM-T	6432	NSD/NRC
TCP	>32768	NSD/NRC	8443	NFM-T OTNE server

Table 4 Ports used in communication between the NSD and NRC and NFM-T (continued)

Protocol	From port	From module	To port	To module
TCP	8443	NFM-T OTNE server	>32768	NSD/NRC
TCP	9092	NSD/NRC	>15000	NFM-T
TCP	>15000	NFM-T	9092	NSD/NRC

The following table lists the ports used in communication between the NSD and NRC modules and VSR-NRC:

Table 5 Ports used in communication between the NSD and NRC modules and VSR-NRC

Protocol	From port	From module	To port	To module
TCP	>32768	NSD/NRC	4199	VSR-NRC
TCP	4199	VSR-NRC	>32768	NSD/NRC

The following table lists the ports used in communication between the NSD-NRC and NFM-P:

Table 6 Ports used in communication between the NSD-NRC and NFM-P

Protocol	From port	From module	To port	To module
TCP	2181	NSD/NRC	>15000	NFM-P
TCP	>15000	NFM-P	2181	NSD/NRC
TCP	>32768	NSD/NRC	7879	NFM-P
TCP	7879	NFM-P	>32768	NSD/NRC
TCP	>32768	NSD/NRC	8087	NFM-P
TCP	8087	NFM-P	>32768	NSD/NRC
TCP	7687	NSD/NRC	>15000	NFM-P
TCP	>15000	NFM-P	7687	NSD/NRC
TCP	9092	NSD/NRC	>15000	NFM-P
TCP	>15000	NFM-P	9092	NSD/NRC
TCP	>15000	NFM-P	7473	NSD/NRC
TCP	7473	NSD/NRC	>15000	NFM-P
TCP	>15000	NFM-P	443	NSD/NRC
TCP	443	NSD/NRC	>15000	NFM-P
TCP	>32768	NSD/NRC	8543	NFM-P

Table 6 Ports used in communication between the NSD-NRC and NFM-P (continued)

Protocol	From port	From module	To port	To module
TCP	8543	NFM-P	>32768	NSD/NRC
TCP	>15000	NFM-P	6432	NSD/NRC
TCP	6432	NSD/NRC	>15000	NFM-P

The following table lists the ports used in communication between the NSD and NRC modules and NEs:

Table 7 Ports used in communication between the NSD and NRC modules and NEs

Protocol	From port	From module	To port	To module
TCP	>32768	NSD/NRC	57400	NE
TCP	57400	NE	>32768	NSD/NRC

The following table lists the ports used in communication between the active and standby NSD-NRC in a redundant deployment:

Table 8 Ports used in communication between the active and standby NSD-NRC in a redundant deployment

Protocol	From port	To port
TCP	>32768	22
TCP	22	>32768
TCP	>32768	2390
TCP	2390	>32768
TCP	>32768	5001
TCP	5001	>32768
TCP	>32768	5002
TCP	5002	>32768
TCP	>32768	5007
TCP	5007	>32768
TCP	>32768	6007
TCP	6007	>32768
TCP	>32768	6017
TCP	6017	>32768
TCP	>32768	6018

Table 8 Ports used in communication between the active and standby NSD-NRC in a redundant deployment (continued)

Protocol	From port	To port
TCP	6018	>32768
TCP	>32768	6432
TCP	6432	>32768

The following table lists the ports used in communication between NSD-NRC and client (GUI/REST) applications:

Table 9 Ports used in communication between NSD-NRC and client (GUI/REST) applications

Protocol	To port	To module	Purpose
TCP	80	NSD and NRC / nspOS	for Launchpad redirect
TCP	443	NSD and NRC / nspOS	for Launchpad
TCP	8543	NSD and NRC	for NSD and NRC GUI, REST
TCP	8543	NFM-P	NFM-P web applications / REST
TCP	8443	NFM-T	NFM-T GUI
TCP	9092	NSD and NRC / nspOS	External notifications (messaging)