



# **NSP Network Services Platform**

Release 19.11

## **System Administrator Guide**

**3HE-15382-AAAD-TQZZA**

**Issue 1**

**November 2019**

---

**Legal notice**

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

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

© 2019 Nokia.

# Contents

<b>About this document</b> .....	<b>5</b>
<b>1 NSP system administration overview</b> .....	<b>7</b>
1.1 Introduction .....	7
<b>2 NSP security administration</b> .....	<b>9</b>
2.1 NSP security administration overview .....	9
2.2 User password policies .....	9
2.3 NSP TLS administration .....	10
2.4 NSP security administration procedures .....	12
2.5 To change the nsp system user password .....	13
2.6 To update the supported NSP TLS versions and ciphers.....	14
2.7 To whitelist a system .....	18
<b>3 NSP application administration</b> .....	<b>21</b>
3.1 NSP application administration overview .....	21
3.2 NSP application access and browser support.....	21
3.3 To configure global NSP application settings .....	24
3.4 To configure the NSP alarm-severity colors .....	25
3.5 To configure NSP linked URLs .....	26
3.6 To activate or deactivate NSP applications .....	26
3.7 To configure event logging .....	28
3.8 To configure an e-mail server for alarm notifications.....	28
<b>4 NSP component administration</b> .....	<b>31</b>
<b>NSP server administration procedures</b> .....	<b>31</b>
4.1 NSP server administration overview .....	31
4.2 To start or stop an NSP server .....	31
4.3 To display the NSP server status .....	32
4.4 To apply an NSD and NRC license .....	33
4.5 To enable single-address geo-redundant NSP system access .....	34
4.6 To disable NSD and NRC websocket event notifications.....	35
4.7 To enable additional NRC-P functions.....	36
<b>NSP analytics server administration procedures</b> .....	<b>39</b>
4.8 NSP analytics server administration overview .....	39
4.9 To start or stop an NSP analytics server .....	39
4.10 To manage images on an analytics server .....	40

---

4.11	To enable and manage analytics server logging .....	41
4.12	To collect analytics-server log files .....	43
	<b>NSP Flow Collector administration procedures</b> .....	<b>46</b>
4.13	NSP Flow Collector administration overview .....	46
4.14	To start or stop an NSP Flow Collector .....	46
4.15	To display the NSP Flow Collector status or release level .....	47
4.16	To open the NSP Flow Collector web UI .....	48
4.17	To configure NSP Flow Collector statistics aggregation .....	49
	<b>NSP Flow Collector Controller administration procedures</b> .....	<b>51</b>
4.18	NSP Flow Collector Controller administration overview .....	51
4.19	To start or stop an NSP Flow Collector Controller .....	51
4.20	To display the NSP Flow Collector Controller status or release level .....	52
4.21	To open the NSP Flow Collector Controller web UI .....	53
4.22	To force an NSP Flow Collector Controller to extract a network data snapshot .....	53
	<b>MDM administration procedures</b> .....	<b>55</b>
4.23	MDM server administration overview .....	55
4.24	To start or stop an MDM server .....	55
4.25	Workflow for commissioning a device for model-driven management .....	56
	<b>NFM-T server administration procedures</b> .....	<b>57</b>
4.26	To rollback integration between an NSP or NFM-P server and a standalone NFM-T system .....	57
4.27	To rollback integration between an NSP or NFM-P server and a classic HA NFM-T system .....	59
4.28	To rollback integration between an NSP or NFM-P server and a hot HA NFM-T system .....	63
<b>5</b>	<b>NSP database administration</b> .....	<b>67</b>
5.1	NSP database administration overview .....	67
5.2	NSP database administration procedures .....	67
5.3	To manually back up the NSP databases .....	67
5.4	To manually restore the NSP databases .....	69
<b>6</b>	<b>NSP system redundancy</b> .....	<b>75</b>
6.1	NSP redundancy models .....	75
6.2	NSP redundancy failure scenarios and recovery mechanisms .....	77

---

# About this document

## Purpose

The *NSP System Administrator Guide* describes Network Services Platform system management, maintenance, and redundancy functions for operators who have NSP system administrator privileges.

## 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](#)



---

# 1 NSP system administration overview

## 1.1 Introduction

### 1.1.1 Guide description

The *NSP System Administrator Guide* describes how to perform various NSP system management operations as requirements arise, or as directed by technical support.

The guide is written for an NSP operator who has the NSP administrator role assigned to their NSP user group. For information about NSP role-based user management, see [Chapter 2, “NSP security administration”](#).

### 1.1.2 NSP administrator responsibilities

An NSP system administrator can manage all NSP functional areas, and is primarily responsible for the following:

- system security, such as TLS configuration and user management, as described in [Chapter 2, “NSP security administration”](#)
- application setup, as described in [Chapter 3, “NSP application administration”](#); application usage is described in the online application help
- starting, stopping, and configuring system components, as described in [Chapter 4, “NSP component administration”](#)
- database management, such as restoration after a failure, as described in [Chapter 5, “NSP database administration”](#)
- understanding NSP fault-tolerance mechanisms based on component redundancy, as described in [Chapter 6, “NSP system redundancy”](#)

**i** **Note:** It is strongly recommended that you perform an administrative procedure in this guide only under the guidance of technical support.





---

## 2 NSP security administration

### 2.1 NSP security administration overview

#### 2.1.1 Introduction

This chapter describes the following NSP security topics:

- TLS administration, such as version support and certificate expiry; see [2.3 “NSP TLS administration” \(p. 10\)](#)
- system security management; see [2.4 “NSP security administration procedures” \(p. 12\)](#)

User access control, session management, and activity logging are documented in the *NSP User Manager Application Help*.

### 2.2 User password policies

#### 2.2.1 Overview

When an operator attempts to log in to the NSP Launchpad and a password change is required, the new password must conform to the password policy of the authenticating agent, as described below.

Application	Requirement
<b>NFM-P</b>	When an NFM-P-authenticated user is prompted to change their password during an NSP login attempt, the new password must conform to the NFM-P password requirements. See the <i>NSP NFM-P Administrator Guide</i> for the NFM-P password requirements and expiration policy.
<b>NFM-T</b>	When an NFM-T-authenticated user is prompted to change their password during an NSP login attempt, the password must conform to the NFM-T password requirements, which are described in the Common Functions section of the <i>NFM-T Administration Guide</i> .
<b>LDAP, RADIUS and TACACS+</b>	A password-change policy is not applied during an NSP user login attempt. If a password change is required, the user must contact the system administrator for information about the LDAP, RADIUS, or TACACS+ password requirements.

---

## 2.3 NSP TLS administration

### 2.3.1 Overview

The NSP uses TLS to secure the external interfaces between NSP components. Additionally, if all NSP system components are at Release 19.6 or later, you can enable TLS on some internal nspOS subsystems and services.

The supported TLS versions and cipher list are configurable; see [2.6 “To update the supported NSP TLS versions and ciphers” \(p. 14\)](#).

**i** **Note:** The NSD and NRC uses TLS 1.2; TLS 2.0 is not supported.

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

#### Internal NSP TLS certificates

An internal NSP TLS certificate is used for securing internal processes. For maximum security, an NSP Public Key Infrastructure server, or PKI server, uses an internally generated private CA to create the internal certificate. Consequently, no certificate from any external CA is trusted for access to the processes.

A PKI server generates an internal certificate automatically during initialization. During NSP installation, or an upgrade from a Release earlier than 19.6, the PKI server must be running in order for each component to request and receive the internal certificate, as described in the *NSP Deployment and Installation Guide*.

**i** **Note:** To reduce complexity, each upgrade procedure instructs you to start the PKI server, regardless of the upgrade conditions.

#### External NSP TLS certificates

An external NSP TLS certificate secures the interfaces between NSP components. The NSP automates the deployment of external certificates to components using an NSP PKI server.

An NSP PKI server can use the following to secure an NSP system:

- custom certificate, which is a signed certificate that you provide
- PKI-server certificate, which the PKI server generates; the certificate is signed by an internally generated private root CA

See the *NSP Deployment and Installation Guide* for more information about NSP TLS deployment using a PKI server.

### 2.3.2 Replacing NSP TLS certificates

NSP TLS certificate replacement may be required when:

- a component is added to the NSP system
- a component IP address or hostname changes
- a TLS certificate nears or reaches expiry

---

See [2.3.3 “TLS certificate expiry notifications” \(p. 12\)](#) for information about how the NSP monitors and responds to TLS certificate expiry.

### Internal TLS certificate management

When you add a new component to an NSP system, the component installation procedure instructs you to start the PKI server. During component initialization, the PKI server automatically distributes the required internal TLS artifacts to the component.

When the TLS certificate used by the internal processes requires replacement because of expiry, or because of a system configuration update, for example, a component addition or address change, or because you enable nspOS security, the following actions may be required.

1. Start the PKI server.
2. Enable certificate regeneration in the **tls** section of the NSP configuration file; see “NSP component parameters” in the *NSP Deployment and Upgrade Guide*.
3. Stop each component.
4. If the NSP system includes an NSP analytics server:
  - a. If you are enabling nspOS security, use the “AnalyticsAdmin.sh updateConfig” command on the analytics server to enable and configure nspOS security.
  - b. Enable certificate regeneration using the “AnalyticsAdmin.sh genCertificate” command. See “To install an NSP analytics server” in the *NSP Deployment and Installation Guide* for configuration information.
5. Run the NSP installer.
6. Start each component.

### External TLS certificate management

When you add a new component to an NSP system, the component installation procedure instructs you to start the PKI server. During component initialization, the PKI server automatically distributes the required external TLS artifacts to the component.

When you need to replace an external certificate because of expiry, or because of a system change such as component addition or address change, the replacement method depends on the TLS deployment method:

- Manual—The certificate replacement process is the same as the manual TLS deployment process described in the *NSP Deployment and Installation Guide*.
- Automated—The following options are available.
  - Provide a custom CA-signed certificate to the PKI server for TLS distribution to components.
  - Let the PKI server generate a certificate that is signed by the PKI server private root CA service.

If you use the automated method, you must perform the following sequence of actions to update the TLS configuration in the NSP system.

1. Remove the TLS artifacts for the current certificate from the PKI server.
2. Start the PKI server.
3. If you have a custom certificate, specify the certificate location in the **tls** section of the NSP configuration file; see “NSP component parameters” in the *NSP Deployment and Installation Guide*.

4. Enable certificate regeneration in the **tls** section of the NSP configuration file; see “NSP component parameters” in the *NSP Deployment and Installation Guide*.
5. If the NSP system includes an NSP analytics server, enable certificate regeneration in the analytics-server configuration using the “AnalyticsAdmin.sh genCertificate” command.
6. Stop each component.
7. Run the NSP installer.
8. Start each component.

**i** **Note:** If you do not provide a custom certificate, enabling certificate regeneration in the NSP configuration file causes the PKI server to generate an internal and an external certificate; if you provide a custom certificate, only an internal certificate is generated, and the existing external certificate remains in service.

### 2.3.3 TLS certificate expiry notifications

An NSP server checks the expiry date of each TLS certificate in the local keystore during installation, and every 24 hours thereafter. If a certificate is expired or approaching expiry, the NSP raises one of the following alarms that are viewable in the Fault Management application:

- Warning, if the certificate is to expire within 30 days of the current time
- Critical, if the certificate is to expire within 7 days of the current time
- Critical, if the certificate is expired

**i** **Note:** The NSP raises one alarm per certificate.

**i** **Note:** NSP TLS certificate-expiry alarms are not self-clearing.

When a TLS certificate is expired, the NSP server continues to operate normally, but some application functions that depend on secure communication may be inoperable.

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

## 2.4 NSP security administration procedures

### 2.4.1 Description

The following procedures describe NSP security administration operations.

**i** **Note:** NSP PKI server operation is described in the *NSP Deployment and Installation Guide*.

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

- # —root user
- bash\$ —nsp user

---

## 2.5 To change the nsp system user password

### 2.5.1 Purpose

Perform this procedure to change the password of the RHEL nsp user in a standalone or redundant NSP system.

### 2.5.2 Steps

1 \_\_\_\_\_

Log in to the NSP station as the root user.

2 \_\_\_\_\_

Open a console window.

3 \_\_\_\_\_

Enter the following:

```
# passwd nsp ↵
```

The following prompt is displayed:

```
New Password:
```

4 \_\_\_\_\_

Enter the new password and press ↵.

The following prompt is displayed:

```
Confirm New Password:
```

5 \_\_\_\_\_

Enter the new password again and press ↵. The password is changed.

6 \_\_\_\_\_

Record the new password and store it in a secure location.

7 \_\_\_\_\_

Close the console window.

8 \_\_\_\_\_

Log out of the component station.

**END OF STEPS** \_\_\_\_\_

---

## 2.6 To update the supported NSP TLS versions and ciphers

### 2.6.1 Purpose



#### CAUTION

##### Service Disruption

*This procedure involves a complete shutdown and restart of the NSP system.*

*It is strongly recommended that you perform this procedure only during a scheduled maintenance period.*



#### CAUTION

##### Potential Service Outage

*Using this procedure to disable the TLSv1 protocol may prevent NSP system access for clients that use Java 7; Java 8 and later clients are unaffected.*

*If you use the procedure to disable TLSv1, the following conditions apply to Java 7 clients:*

- A client that uses Java 7, update 94 or earlier, cannot connect to the NSP.
- A client that uses Java 7, update 95 or later, can connect to the NSP only if you enable TLSv1.1 or TLSv1.2, as required, on the client station.

To enable TLSv1.1 or TLSv1.2 for a client, you must add the protocol to the list of supported protocols defined by the `jdk.tls.client.protocols` Java system property on the client station, for example:

```
jdk.tls.client.protocols=TLSv1.2
```



**Note:** The NSD and NRC uses TLS 1.2; TLS 2.0 is not supported.

Outdated TLS versions or ciphers may present a security risk. Perform this procedure to update the lists of supported TLS versions and ciphers in an NSP system.

### 2.6.2 Steps

#### Prepare new cipher and TLS versions files

- 1 \_\_\_\_\_  
Log in to the standalone or primary NSP server station as the `nsp` user.
- 2 \_\_\_\_\_  
Enter the following:  

```
bash$ cd /opt/nsp/scripts/security ↵
```
- 3 \_\_\_\_\_  
Enter the following to create the default cipher list file:

---

```
bash$ ./ciphers_and_tls_update.bash create -cdc default-ciphers-file ↵
```

4

Enter the following to create the default TLS list file:

```
bash$ ./ciphers_and_tls_update.bash create -cdt default-tls-file ↵
```

5

Enter the following to copy the default ciphers file to a new file:

```
bash$ cp default-ciphers-file new_ciphers_file ↵
```

where *new\_ciphers\_file* is the name to assign to the new ciphers file

6

Open *new\_ciphers\_file* using a plain-text editor such as vi.

7

Remove the ciphers that are not to be supported.

8

Save and close the file.

9

Enter the following to copy the default TLS versions file to a new file:

```
bash$ cp default-tls-file new_tls_file ↵
```

where *new\_tls\_file* is the name to assign to the new TLS versions file

10

Open *new\_tls\_file* using a plain-text editor such as vi.

11

Remove the TLS versions that are not to be supported.



**Note:** TLSv1.2 is mandatory and must not be removed.

12

Save and close the file.

## Distribute files to system components

13

If the NSP system is redundant, distribute the required files to the standby NSP server station.

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

2. Enter the following:  

```
# cd /opt/nsp/scripts/security ↵
```
3. Copy the following files from the primary NSP server station to the current directory:
  - /opt/nsp/scripts/security/new\_ciphers\_file
  - /opt/nsp/scripts/security/new\_tls\_file

---

## 14

If the NSP system includes NSP Flow Collectors, NSP Flow Collector Controllers, or NSP analytics servers, distribute the required files to each NSP Flow Collector, NSP Flow Collector Controller, and NSP analytics server station.

1. Log in to the station as the nsp user.
2. Enter the following:  

```
bash$ mkdir /opt/nsp/cipher_update ↵
```
3. Enter the following to switch to the root user:  

```
bash$ su ↵
```
4. Copy the following files from the standalone or primary NSP server station to the /opt/nsp/cipher\_update directory:
  - /opt/nsp/scripts/security/ciphers\_and\_tls\_update.bash
  - /opt/nsp/scripts/security/new\_ciphers\_file
  - /opt/nsp/scripts/security/new\_TLS\_file
5. Enter the following:  

```
# chmod a+x /opt/nsp/cipher_update/ciphers_and_tls_update.bash ↵
```

## Stop NSP system

---

## 15

If the NSP system is redundant, stop the standby NSP server, as described in [4.2 “To start or stop an NSP server”](#) (p. 31).

---

## 16

If the system includes one or more NSP analytics servers, stop each analytics server, as described in [4.9 “To start or stop an NSP analytics server”](#) (p. 39).

---

## 17

If the system includes one or more NSP Flow Collectors, stop each NSP Flow Collector, as described in [4.14 “To start or stop an NSP Flow Collector”](#) (p. 46).

---

## 18

If the system includes one or more NSP Flow Collector Controllers, stop each NSP Flow Collector Controller, as described in [4.19 “To start or stop an NSP Flow Collector Controller”](#) (p. 51).



---

19

Stop the standalone or primary NSP server, as described in 4.2 “To start or stop an NSP server” (p. 31).

## Apply new cipher and TLS lists

---

20

Perform the following steps on each NSP server station to apply the new TLS configuration.

1. Log in as the nsp user.
2. Open a console window.
3. Enter the following:

```
bash$ cd /opt/nsp/scripts/security ↵
```

4. Enter the following:

**Note:** The `-fo` parameter is optional, and sets the cipher priority according to the order in the specified file. If the parameter is not included, the cipher priority is set to the default order.

```
bash$ ./ciphers_and_tls_update.bash apply -c new_ciphers_file -t new_tls_file -fo ↵
```

where

*new\_ciphers\_file* is the updated ciphers file

*new\_tls\_file* is the updated TLS versions file

The script applies the new configuration, and backs up the previous configuration in the following file:

```
ciphers_and_tls_backup.timestamp.tar.gz
```

---

21

If the system includes one or more NSP Flow Collectors, NSP Flow Collector Controllers, or NSP analytics servers, perform the following steps on each NSP Flow Collector, NSP Flow Collector Controller, and NSP analytics server station to apply the new TLS configuration.

1. Log in as the nsp user.
2. Enter the following:

```
bash$ cd /opt/nsp/cipher_update ↵
```

3. Enter the following:

**Note:** The `-fo` parameter is optional, and sets the cipher priority according to the order in the specified file. If the parameter is not included, the cipher priority is set to the default order.

```
bash$ ./ciphers_and_tls_update.bash apply -c new_ciphers_file -t new_tls_file -fo ↵
```

where

*new\_ciphers\_file* is the updated ciphers file

---

*new\_tls\_file* is the updated TLS versions file

The script applies the new configuration, and backs up the previous configuration in the following file:

`ciphers_and_tls_backup.timestamp.tar.gz`

---

22

Close the open console windows.

## Start NSP system

---

23

Start the standalone or primary NSP server, as described in [4.2 “To start or stop an NSP server”](#) (p. 31).

---

24

If the NSP system is redundant, start the standby NSP server, as described in [4.2 “To start or stop an NSP server”](#) (p. 31).

---

25

If the system includes one or more NSP Flow Collector Controllers, start each NSP Flow Collector Controller, as described in [4.19 “To start or stop an NSP Flow Collector Controller”](#) (p. 51).

---

26

If the system includes one or more NSP Flow Collectors, start each NSP Flow Collector, as described in [4.14 “To start or stop an NSP Flow Collector”](#) (p. 46).

---

27

If the system includes one or more NSP analytics servers, start each analytics server, as described in [4.9 “To start or stop an NSP analytics server”](#) (p. 39).

---

28

Close the open console windows.

---

END OF STEPS

## 2.7 To whitelist a system

### 2.7.1 Purpose

When an OSS embeds reports from the Analytics application in its own OSS web application, requests to retrieve these reports may be identified as cross-origin requests. Such requests are blocked by the NSP CORS policy, as only the hosts in the whitelist are accepted as NSP components. Perform this procedure to disable the blocking of report retrieval by an OSS.

---

Similarly, when an NSP deployment includes an NSP Analytics server and an NFM-P at a release earlier than 18.12, the CORS filtering may result in a 401 error. Performing the procedure resolves this issue also.

## 2.7.2 Steps

1 \_\_\_\_\_  
Log in as the nsp user on the NSP server station that hosts the active nspOS instance.

2 \_\_\_\_\_  
Open a console window.

3 \_\_\_\_\_  
Enter the following to acquire an access token from the REST API Gateway:

```
bash$ curl --insecure -X POST https://server/rest-gateway/rest/api/v1/auth/token -H 'authorization: Basic credentials' -H 'cache-control: no-cache' -H 'content-type: application/x-www-form-urlencoded' -d grant_type=client_credentials ↵
```

where

*server* is the IP address or hostname of the server that hosts the active nspOS instance

*credentials* is the base64-encoded credentials, expressed as *username:password*

The REST API Gateway returns an access token.

4 \_\_\_\_\_  
Enter the following once for each NSP analytics server to add the server as a whitelist target:



**Note:** You must add each NSP analytics server in the deployment to the whitelist.

```
bash$ curl -kv https://server/session-manager/api/v1/whitelist/allowedHosts -H 'Content-Type: application/json' -H "Authorization: Bearer access_token" --data '{"host":"whitelist_target"}' -X POST ↵
```

where

*server* is the IP address or hostname of the server that hosts the active nspOS instance

*access\_token* is the access token returned in [Step 3](#)

*whitelist\_target* is the hostname or IP address of the NSP analytics server station

The NSP analytics server is added to the whitelist.

5 \_\_\_\_\_  
Close the console window.

END OF STEPS \_\_\_\_\_



---

## 3 NSP application administration

### 3.1 NSP application administration overview

#### 3.1.1 Introduction

This chapter describes NSP application access requirements, general application configuration settings, and best practices for application access.

### 3.2 NSP application access and browser support

#### 3.2.1 Licensing

You can obtain the following NSP license types:

- Standard
- Premium

A Premium NSP license enables all applications on the NSP Launchpad. When a Standard NSP license is in use, applications that require a Premium NSP license are identified by a badge.

Contact your sales representative for comprehensive licensing information.

#### 3.2.2 Browser access to redundant NSP servers

If you open a browser to the primary NSP server URL in a redundant deployment, the primary NSP server login page opens.

If you open a browser to the standby NSP server URL, the browser is redirected to the primary NSP server URL if the standby server is operational; otherwise, the browser shows the standby server URL as unreachable.

##### **Single-address access to geo-redundant NSP system**

To reduce the number of IP addresses that an NSP operator requires for access to the servers in a geographically redundant NSP deployment, you can use a reverse-proxy server to set one IP address for NSP access, regardless of which NSP cluster or server is active.

See [4.5 “To enable single-address geo-redundant NSP system access” \(p. 34\)](#) for proxy-server configuration information.

#### 3.2.3 Disabling unused applications

To improve the NSP startup time, an NSP administrator can disable unused applications. The NSP does not load a disabled application during system initialization or display the application icon on the NSP Launchpad. See [3.6 “To activate or deactivate NSP applications” \(p. 26\)](#) for information.

### 3.2.4 OSS access

Applications that use REST APIs publish a set of URLs for managed application resources or web services. Each domain application documents the URLs that are available to users. The API URLs are accessible through a browser to authorized users, including OSS applications, which can use the URLs for cross-launching.

See the [Nokia Network Developer Portal](#) for more information about OSS access to the NSP using a REST API.

### 3.2.5 Browser support

All NSP applications are supported on the latest version of Google Chrome. For information about additional supported browsers for NSP applications, see the NSP NFM-P Planning Guide.

**i** **Note:** In order for the Apple Safari web browser to open the Analytics application, you must ensure that the following Safari privacy settings are configured, if present in your browser version:

- Safari Preferences page, Cookies And Website Data—Always Allow
- Prevent cross-site tracking—disabled

**i** **Note:** If you are using Chrome or Firefox on Windows 8.1 or Windows Server 2012, it is recommended that you enable ClearType Text for optimal viewing of fonts:  
In the Windows Control Panel, open the Display settings, and enable the Turn on ClearType parameter under the Adjust ClearType text settings.

**i** **Note:** You cannot switch browsers between clients or applications. You must always use the system default browser.

**i** **Note:** It is recommended to use the NSP Launchpad for access to NSP applications, as user-created links to individual applications may be broken by a server activity switch or software upgrade.

### 3.2.6 Application help and user documentation

You can open the NSP Help Center from each NSP application user interface by clicking on the ? icon. The Help Center provides application-specific help, as well as access to other NSP documentation.

### 3.2.7 Application-server connection loss

NSP application sessions that are terminated by a server connection loss may require up to two minutes to reset after the server connection is restored. In the interim, the application GUI may seem to function, but executing a GUI command results in a Server Not Found browser error. The condition persists until an automated system function clears the former application session.

### 3.2.8 Best practices for application access

Some HTTP errors or stalled user sessions can be avoided by adhering to the following best practices:

- Although other browser types are supported, Chrome is the preferred browser.
- Enable cookies in your browser.
- Sign in to the NSP Launchpad before opening additional NSP applications in other tabs.
- Before signing in as a different user, close all other NSP tabs and sign out of the last tab.
- If multiple NSP applications are open in one browser, close all other NSP tabs before signing out of the last NSP tab; do not just close the browser.
- Avoid pausing a polling application for more than ten minutes.
- In the event of an NSP server activity switch or shutdown, close all browser tabs; you can sign in again when the server returns to service.

### 3.2.9 Keyboard-based navigation

You can use the keyboard to navigate and interact with most NSP applications. Keyboard navigation allows you to highlight and select interactive components in the application using keystrokes instead of a pointing device.

The following table lists the accessibility options.

Keystroke	Action
Tab	Advance to next element
Shift + Tab	Return to previous element
Alt + down arrow Option/ALT + down arrow in Apple/OSX	Open pop-up or drop-down menu
Shift + F10 Shift + Fn + F10 in Apple/OSX	Open contextual menu
Ctrl + c Command + c in Apple/OSX	Copy
Ctrl + v Command + v in Apple/OSX	Paste
Enter	Open folder or expandable object such as tile Invoke action on button or menu item
F8 Fn + F8 in Apple/OSX	Move over larger components or to next page
F5 Shift + Fn + F5 in Apple/OSX	Refresh

Keystroke	Action
Shift + F1 Shift + Fn + F1 in Apple/OSX	Open tool tip
Esc	Close tool tip or menu
Arrow	After tile selected using Tab key, navigate across tiles in matrix such as Fault Management Top Unhealthy NEs view or Service Supervision matrix view Up and down arrows for navigation through items in open contextual or pop-up menu Up and down arrows for navigation between table rows Left and right arrows for navigation across table column headers
Shift + right or left arrow	Reorder data-table columns in selected header

### 3.3 To configure global NSP application settings

#### 3.3.1 Purpose

Use this procedure to specify the default operating parameters of NSP applications.

#### 3.3.2 Steps

- 1 \_\_\_\_\_  
Sign in to the NSP as an administrator.
- 2 \_\_\_\_\_  
From the NSP Launchpad, click More, Settings.
- 3 \_\_\_\_\_  
Click System Settings.
- 4 \_\_\_\_\_  
Set the application polling time.
- 5 \_\_\_\_\_  
Choose a Language from the drop-down menu.



- 
- 6 \_\_\_\_\_  
Type a security statement in the text field, and then select the check box to enable the security statement.
  - 7 \_\_\_\_\_  
Select the Color row with severity in IP and Wireless applications parameter, if required.
  - 8 \_\_\_\_\_  
Configure settings for physical maps in the Network Supervision and Supervision Management applications, if required:
    - Background Map Layer URL—link to a map available under an open license, in the following format:  
`https://tile_server/path/file.png`
    - Background Map Layer Attribution—optional free-form text field for crediting an open license provider for legal purposes
  - 9 \_\_\_\_\_  
Click Save.

END OF STEPS \_\_\_\_\_

## 3.4 To configure the NSP alarm-severity colors

### 3.4.1 Purpose

Use this procedure to specify the display colors for alarm severity levels.

### 3.4.2 Steps

- 1 \_\_\_\_\_  
Sign in to the NSP as an administrator.
- 2 \_\_\_\_\_  
Choose More, Settings from the NSP Launchpad.
- 3 \_\_\_\_\_  
Click System Colors.
- 4 \_\_\_\_\_  
Under Alarms, click on an alarm severity category and then click on the color you want to associate with the alarm severity category.  
Repeat this step to set custom colors for other alarm severity categories, as required.

---

5 \_\_\_\_\_  
Select a text color.

6 \_\_\_\_\_  
Click Save.

END OF STEPS \_\_\_\_\_

## 3.5 To configure NSP linked URLs

### 3.5.1 Purpose

Use this procedure to link up to 20 external URLs that application users can open in a new browser tab from the More menu on the NSP Launchpad.

### 3.5.2 Steps

1 \_\_\_\_\_  
Sign in to the NSP as an administrator.

2 \_\_\_\_\_  
Choose More, Settings from the NSP Launchpad.

3 \_\_\_\_\_  
Click Linked URLs.

4 \_\_\_\_\_  
Configure the Display Name and URL parameters.

5 \_\_\_\_\_  
Click Add.

6 \_\_\_\_\_  
To remove a linked URL, hover over the URL item in the list and click the Delete button at the end of the row.

END OF STEPS \_\_\_\_\_


## 3.6 To activate or deactivate NSP applications

### 3.6.1 Purpose

Use this procedure to specify which NSP applications are available to operators from the NSP Launchpad.

---

 **Note:** Deactivating unused NSP applications decreases the NSP startup time.

 **Note:** Deactivating and reactivating an NSP application may cause the NFM-P web server to restart unexpectedly. To avoid this behavior, you must restart the NFM-P web server between application deactivation and reactivation.



### CAUTION

#### Service Disruption

*This procedure involves a restart of each NSD and NRC server.*

*It is strongly recommended that you perform this procedure only during a scheduled maintenance period.*

## 3.6.2 Steps

1 \_\_\_\_\_

Sign in to the NSP Launchpad as an administrator.

2 \_\_\_\_\_

Choose More, Settings.

3 \_\_\_\_\_

Click App Deployment Control.

4 \_\_\_\_\_


Expand an application category, and then select or deselect the required check boxes to activate or deactivate applications in the category.

5 \_\_\_\_\_

Select the check box to indicate that you understand the implications of the change.

6 \_\_\_\_\_

Click Save.

 **Note:** If you are reactivating an application, there may be a brief delay before the Launchpad displays the application icon.

7 \_\_\_\_\_

If you are deactivating any application, restart the NSP; see [4.2 "To start or stop an NSP server" \(p. 31\)](#) for information about how to perform the actions in the following steps.

1. If the NSP system is redundant, stop the standby NSD and NRC server.
2. Stop the primary or standalone NSD and NRC server.
3. Start the primary or standalone NSD and NRC server.

- 
4. If the NSP system is redundant, start the standby NSD and NRC server.

END OF STEPS

---

## 3.7 To configure event logging

### 3.7.1 Purpose

Use this procedure to configure the recording of assurance events, or to purge all event records from the database.

**i** **Note:** Events can be retained for up to 30 days.

### 3.7.2 Steps

- 1 \_\_\_\_\_  
Sign in to the NSP as an administrator.
- 2 \_\_\_\_\_  
Choose More, Settings from the NSP Launchpad.
- 3 \_\_\_\_\_  
Click Event Logging Policy.
- 4 \_\_\_\_\_  
To enable event logging, select the Enable Event Logging parameter.
- 5 \_\_\_\_\_  
To specify how long event records are retained, configure the Retention Time parameter.
- 6 \_\_\_\_\_  
To delete all event records from the database, click Purge Event Records.
- 7 \_\_\_\_\_  
Click Save.

END OF STEPS

---

## 3.8 To configure an e-mail server for alarm notifications

### 3.8.1 Purpose

Use this procedure to configure connection information to an e-mail server for use with Fault Management alarm e-mail policies.

---

### 3.8.2 Steps

1 \_\_\_\_\_  
Sign in to the NSP as an administrator.

2 \_\_\_\_\_  
Choose More, Settings from the NSP Launchpad.

3 \_\_\_\_\_  
Click E-mail Server Settings.

4 \_\_\_\_\_  
Specify the address of an e-mail server, and the user name and credentials of an administrative user.

5 \_\_\_\_\_  
Click Save.

**END OF STEPS** \_\_\_\_\_



---


## 4 NSP component administration

### NSP server administration procedures

#### 4.1 NSP server administration overview

##### 4.1.1 Description

The following procedures describe NSP server administration operations.

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

- # —root user
- bash\$ —nsp user

#### 4.2 To start or stop an NSP server

##### 4.2.1 Purpose

Perform this procedure to start or stop the NSP software on an NSP server station.



#### CAUTION

##### Service disruption

*Stopping an NSP server may create a network-management outage, and starting an NSP server out of sequence in a redundant deployment may initiate a server activity switch that is potentially disruptive to network management.*

*Perform the procedure only under the guidance of technical support during a scheduled maintenance period.*

##### 4.2.2 Steps

1 \_\_\_\_\_

Log on to an nsp server station as the root user.

2 \_\_\_\_\_

Open a console window.

3 \_\_\_\_\_

To start an NSP server, enter the following:

```
# nspdctl --host server start ↵
```

where server is the IP address or hostname of the NSP server that you intend to start

---

The NSP server starts.

4

---

To stop an NSP server, enter the following:

```
# nspdctl --host server stop ↵
```

where server is the IP address or hostname of the NSP server that you intend to start

The NSP server stops.

5

---

Close the console window.

END OF STEPS

---

## 4.3 To display the NSP server status

### 4.3.1 Steps

1

---

Log on to the nsp server station as the root user.

2

---

Open a console window.

3

---

Perform one of the following.

a. To display the status of the local nsp server, enter the following:

```
# nspdctl status ↵
```

b. To display the status of a remote nsp server, enter the following:

```
# nspdctl --host server status ↵
```

where server is the NSP server IP address or hostname

The NSP server operational information is displayed.

The server is operational if the State value is “running” and the required services are shown as “active”.



**Note:** The nsp-sdn-replication service is shown as active only in a redundant deployment.

4

---

Close the console window.

END OF STEPS

---



---

## 4.4 To apply an NSD and NRC license

### 4.4.1 Purpose

Use this procedure to apply a new or updated license to an NSD and NRC server.

### 4.4.2 Steps

1

Copy the required license files to the *NSP\_installer\_directory/license* directory, where *NSP\_installer\_directory* is the directory contains the extracted NSP software package.

2

Log in to the NSD and NRC station as the nsp user.

3

Open a console window.

4

Enter the following:

```
bash$ cd NSP_installer_directory/bin ↵
```

5

Enter the following to apply the license:

```
bash$ ./install.sh ↵
```

The license is distributed to each NSD and NRC server.

6

Enter the following to switch to the root user:

```
bash$ su ↵
```

7

Enter the following to restart the web server and activate the new license:



**Note:** If the NSD and NRC deployment is redundant, you must perform the step on each NSD and NRC server.

```
# systemctl restart nsp-tomcat ↵
```

The web server restarts, and the license is applied.

8

Close the console window.

END OF STEPS

---

---

## 4.5 To enable single-address geo-redundant NSP system access

### 4.5.1 Purpose

Use this procedure to reduce the number of IP addresses a user requires for access to the servers in a geographically redundant NSP system.

You can implement a reverse proxy that presents only one IP address for system access. A reverse proxy maps the IP address to the appropriate server or server cluster.

**i** **Note:** The procedure describes using the `mod_proxy` Apache HTTP module. Using a different proxy agent or `mod_proxy` configuration is supported but not described. Also, `mod_proxy` installation is not described. Reverse proxy implementation is specific to a network; the network administrator can best determine which implementation is best suited to the management network.

### 4.5.2 Steps

1 \_\_\_\_\_

Log in as the root user on the station that is to host the reverse proxy.

2 \_\_\_\_\_

Open a console window.

3 \_\_\_\_\_

Open the `httpd.conf` file in the `mod_proxy` installation directory using a plain-text editor such as `vi`.

4 \_\_\_\_\_

Edit the file to include the following:

```
<VirtualHost *:*>
  <Proxy nspOS://dr>
    BalancerMember http://NSD_NRC_server1
    BalancerMember http://NSD_NRC_server2
  </Proxy>
  ProxyPreserveHost Off
  ProxyPass / nspOS://dr/
  ProxyPassReverse / nspOS://dr/
</VirtualHost>
```

where

`NSD_NRC_server1` and `NSD_NRC_server2` are the IP addresses or hostnames of the NSD and NRC servers

---

**i** **Note:** In a geographically redundant deployment with HA, the *NSD\_NRC\_server1* and *NSD\_NRC\_server2* addresses are the VIP IP addresses of the HA clusters.

5 \_\_\_\_\_  
Close the console window.

END OF STEPS \_\_\_\_\_

## 4.6 To disable NSD and NRC websocket event notifications

### 4.6.1 Purpose

Websocket-based events are used by the NSD and NRC applications. Perform this procedure to disable websocket event notifications, if required.

**i** **Note:** The websocket connection used by the NSD and NRC modules may not function if a browser or any client is behind a proxy. Websocket communication through an entity between the websocket client and server, for example, a proxy server, firewall, or load balancer, is dependent on the entity configuration.

### 4.6.2 Steps

1 \_\_\_\_\_  
Log in to the NSD and NRC station as the nsp user.

2 \_\_\_\_\_  
Open a console window.

3 \_\_\_\_\_  
Enter the following:  
`bash$ cd /opt/nsp/configure/config ↵`

4 \_\_\_\_\_  
Open the `wsc-security.conf` file using a plain-text editor such as `vi`.

5 \_\_\_\_\_  
Modify the following section to read:

```
websocket {  
  enableEvents=false  
}
```

6 \_\_\_\_\_  
Enter the following to restart the web server:

---

**i** **Note:** If the NSD and NRC deployment is redundant, you must perform the step on each NSD and NRC server.

```
# systemctl restart nsp-tomcat ↵
```

The web server restarts, and websocket event notifications are disabled.

7

Close the console window.

END OF STEPS

---

## 4.7 To enable additional NRC-P functions

### 4.7.1 Purpose

Use this procedure to enable NRC-P functions that are disabled by default.

**i** **Note:** You must perform the procedure on each NSD and NRC server in the NSP system.

### 4.7.2 Steps

**i** **Note:** You must edit a file in the procedure using only a plain-text editor such as vi.

1

Log in to the NSD and NRC server as the nsp user.

2

Enter the following to stop the server:

```
bash$ nspdctl --host server stop ↵
```

where *server* is the NSP server IP address

3

To enable BGP-LS topology learning; edit the `/opt/nsp/configure/config/arm-system.conf` file to read as follows:

```
nrcp {  
    bgpLS  
    {  
        isTopoSourceBgpLS=true
```

4

To enable threshold-crossing alarms, or TCAs for port utilization information; edit the `/opt/nsp/configure/config/nrcf.conf` file to read as follows:

```
nrc-f  
{
```

---

```
tca
{
    enable = true
```

**5**

To enable PCEP for PCC- and PCE-initiated LSP creation; edit the `/opt/nsp/configure/config/sros-vms.conf` file to read as follows:

```
sros-vms {
    enabled=false
    vms =[
        {
            .
            .
            .
            pcep=true
```

**6**

To manage the Cflowd caching of NRC-P flows; edit the `/opt/nsp/configure/config/nrcf.conf` file to read as follows, where `nn` is the cache timeout, in seconds:

```
cflowd
{
    # Cflowd cache timeout (Seconds)
    cache_timeout = nn
```

**7**

To enable BGP for NRC-P flow management for the Autonomous System Optimizer application, which obtains from the CPAM the BGP prefixes of each steered AS; configure the following parameters in the `/opt/nsp/configure/config/nrcf.conf` file:

```
bgp
{
    # BGP Autonomous system number of CPAA router
    cpaa_autonomous_system_number = 100
    # BGP prefix filter id used for fetching prefixes.
    prefix_filter_id = 65535
    # BGP prefix fetch timeout(milli seconds).
    prefix_fetch_timeout = 60000
    # BGP AS subnet info refresh timer(hours)
    as_subnet_refresh_timer = 24
```

---

8

To enable OpenFlow for NRC-P flow steering; edit the `/opt/nsp/configure/config/sros-vms.conf` file to read as follows:

```
sros-vms {  
    enabled=false  
    vms =[  
        {  
            .  
            .  
            .  
            openflow=true
```

---

9

Enter the following to start the NSP server:

```
bash$ nspctl --host server start ↵
```

where *server* is the NSP server IP address

The NSP server starts.

---

10

Close the console window.

---

END OF STEPS

---

## NSP analytics server administration procedures

### 4.8 NSP analytics server administration overview

#### 4.8.1 Description

The following procedures describe NSP analytics server administration operations.

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

- # —root user
- bash\$ —nsp user

### 4.9 To start or stop an NSP analytics server

#### 4.9.1 Purpose

Perform this procedure to start or stop the analytics server software on a station.

1 \_\_\_\_\_

Log in to the analytics server station as the nsp user.

2 \_\_\_\_\_

Open a console window.

3 \_\_\_\_\_

To start the NSP analytics server, enter the following:

```
bash$ /opt/nsp/analytics/bin/AnalyticsAdmin.sh start ↵
```

The following is displayed:

```
Starting Analytics Application
```

When the analytics server is started, the following is displayed.

```
Analytics Application successfully started!
```

4 \_\_\_\_\_

To stop the NSP analytics server, enter the following:

```
bash$ /opt/nsp/analytics/bin/AnalyticsAdmin.sh stop ↵
```

The following is displayed:

```
Stopping Analytics Application
```

When the analytics server is stopped, the following is displayed:

```
Analytics Application is not running
```

---

5 \_\_\_\_\_  
Close the console window.

END OF STEPS \_\_\_\_\_

## 4.10 To manage images on an analytics server

### 4.10.1 Purpose

Perform this procedure to upload logo images from an analytics server to the Images folder in the NSP Analytics application repository, or to update or remove existing images. You can use logo images for Analytics report branding.

Before you begin, the images must be saved to the analytics server in one of the following formats:

- JPEG
- JPG
- GIF
- PNG
- SVG
- BMP

An image name or filename can include only the following characters:

- alphanumerics
- underscore ( \_ )
- period ( . )

**i** **Note:** You can also manage images from the NSP Analytics application; see the application online help for information.

### 4.10.2 Steps

1 \_\_\_\_\_  
Log in to the NSP analytics server station as the nsp user.

2 \_\_\_\_\_  
Open a console window.

3 \_\_\_\_\_  
Create a text file that contains the information for each image that you want to deploy to the Analytics application; add one line for each image, in the following format:

```
image_name|path/image_filename  
where
```



---

*image\_name* is the name to assign to the Resource ID that a user must specify when adding the image to a report

*path* is the absolute path of the image file

*image\_filename* is the name of the image file, and is the name that the Analytics application applies to the image in the Repository folder

4

---

To remove an image from the application Repository folder, add the following line to the text file:

```
image_filename|delete
```

5

---

Enter the following to deploy the images:

```
bash$ /opt/nsp/analytics/bin/AnalyticsAdmin.sh deployImage text_file ↵
```

where *text\_file* is the absolute path of the text file created in [Step 3](#)

The analytics server deploys the images and displays progress messages.

6

---

When the image deployment is complete, close the console window.

END OF STEPS

---

## 4.11 To enable and manage analytics server logging

### 4.11.1 Purpose

Perform this procedure to enable, configure, or disable the logging of Analytics application events on an NSP analytics server, for example, when troubleshooting an application problem.

By default, an analytics server logs only error events.



#### CAUTION

##### System disruption

*Performing the procedure restarts the analytics server.*

*Also, the logging is verbose; the created log files may consume excessive disk space if logging is enabled for an extended period.*

*Perform the procedure only if required, and only for the period required to collect the log entries of interest. Contact technical support for assistance or more information.*



**Note:** The following RHEL CLI prompt in a command line denotes the nsp user, and is not to be included in a typed command:

- bash\$

---

**i** **Note:** If the analytics servers are redundant, you must perform the procedure on each analytics server to ensure that all log events are collected, for example, in the event that the Analytics application begins using a different analytics server, or if analytics load balancing is enabled.

#### 4.11.2 Steps

1 \_\_\_\_\_  
Log in to the 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 enableLog object ↵`  
where *object* is one of the following:

- ADHOC—generates logs during ad hoc report design
- SQL—logs the SQL commands that the analytics server generates during report execution
- ALL—enables all available log objects

The following message and prompt are displayed.  
`This Action requires Analytics Server restart.  
Please type 'YES' to continue.`

5 \_\_\_\_\_  
Enter YES.  
The following is displayed as the analytics server restarts and the logging begins.

```
Stopping Analytics Application
date time Starting Analytics Application
Waiting for Analytics Server to come up
date time Analytics Server is UP and Running
Analytics Server successfully started!
```

The log entries are stored in the following file:

- /opt/nsp/analytics/log/analytics.server.log

---

6

To change the logging level, perform the following steps:

**i** **Note:** You must use the `resetLog` option to disable any logging level that is enabled. For example, if ALL logging is enabled, and you want only SQL logging, you must disable ALL logging, and then enable SQL logging; using the `enableLog` option does not disable any previously enabled logging level.

1. Reset the logging level, as described in [Step 7](#).
2. Go to [Step 4](#).

---

7

To reset the logging function to the default of logging only error events, perform the following steps.

1. Enter the following:

```
bash$ AnalyticsAdmin.sh resetLog ↵
```

The following message and prompt are displayed.

```
This Action requires Analytics Server restart.
```

```
Please type 'YES' to continue.
```

2. Enter YES.

The following is displayed as the analytics server restarts and the logging is reset to the default level.

```
Stopping Analytics Application
```

```
date time Starting Analytics Application
```

```
Waiting for Analytics Server to come up
```

```
date time Analytics Server is UP and Running
```

```
Analytics Server successfully started!
```

---

8

Close the console window.

---

END OF STEPS

## 4.12 To collect analytics-server log files


### 4.12.1 Purpose

Use this procedure to collect the relevant log files for troubleshooting an NSP analytics server if requested by technical support.

---

## 4.12.2 Steps

- 1 \_\_\_\_\_  
Log in as the root user on the Analytics server station.
- 2 \_\_\_\_\_  
Open a console window.
- 3 \_\_\_\_\_  
Enter the following:  

```
# cd /opt/nsp/analytics/bin ↵
```
- 4 \_\_\_\_\_  
Enter the following:  
 **Note:** You cannot specify /tmp, or any directory below /tmp, as the output directory.  

```
# ./getDebugFilesAnalytics.bash output_dir days ↵
```

where

*output\_dir* is a local directory that is to contain the output files

*days* is the optional number of days for which to collect log files; if not specified, all logs are collected

Messages like the following are displayed as the logs are collected:

```
Please wait, capturing workstation information files. This may take a  
few minutes...  
Done capturing workstation information files.  
Please wait, capturing analytics server debug files. This may take  
several minutes...  
Done capturing analytics server debug files.  
Please wait, capturing nsp os log files. This may take several  
minutes...  
Done capturing nsp os log files.  
-----  
Please ftp the output_dir/filespec.tar files to the Nokia ftp server  
ftp to IP_address, login as anonymous  
Put the files in /pub/<CUSTOMER_NAME>/incoming  
Contact your Nokia support representative for assistance  
-----
```
- 5 \_\_\_\_\_  
Transfer the files as directed in the script output.

---

**6**

Close the console window.

**END OF STEPS**

---

---

## NSP Flow Collector administration procedures

### 4.13 NSP Flow Collector administration overview

#### 4.13.1 Description

The following procedures describe NSP Flow Collector administration operations.

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

- # —root user
- bash\$ —nsp user

### 4.14 To start or stop an NSP Flow Collector



#### CAUTION

##### System degradation

*On a station that has a collocated NSP Flow Collector and NSP Flow Collector Controller, starting or stopping the Flow Collector also starts or stops the Flow Collector Controller, and affects all Flow Collectors associated with the Controller.*

*Before you stop an NSP Flow Collector that is collocated with a Flow Collector Controller, ensure that you understand the implications of the action.*

#### 4.14.1 Steps

1 \_\_\_\_\_

Log in to the NSP Flow Collector station as the nsp user.

2 \_\_\_\_\_

Open a console window.

3 \_\_\_\_\_

Enter the following:

```
bash$ cd /opt/nsp/flow ↵
```

4 \_\_\_\_\_

To stop the NSP Flow Collector, perform one of the following:

- a. If the NSP Flow Collector is collocated on the station with an NSP Flow Collector Controller, enter the following:

```
bash$ ./fcc/bin/flowCollectorController.bash stop ↵
```

The NSP Flow Collector and NSP Flow Collector Controller stop.

- 
- b. If the NSP Flow Collector is on a dedicated station, enter the following:

```
bash$ ./fc/bin/flowCollector.bash stop ↵
```

The NSP Flow Collector stops.

---

**5**

To start the NSP Flow Collector, perform one of the following:

- a. If the NSP Flow Collector is collocated on the station with an NSP Flow Collector Controller, enter the following:

```
bash$ ./fcc/bin/flowCollectorController.bash start ↵
```

The NSP Flow Collector and NSP Flow Collector Controller start.

- b. If the NSP Flow Collector is on a dedicated station, enter the following:

```
bash$ ./fc/bin/flowCollector.bash start ↵
```

The NSP Flow Collector starts.

---

**6**

Close the console window.

---

END OF STEPS

## 4.15 To display the NSP Flow Collector status or release level

### 4.15.1 Steps

---

**1**

Log in to the NSP Flow Collector station as the nsp user.

---

**2**

Open a console window.

---

**3**

Enter the following:

```
bash$ cd /opt/nsp/flow ↵
```

---

**4**

To display the NSP Flow Collector status, perform one of the following:

- a. If the NSP Flow Collector is collocated on the station with an NSP Flow Collector Controller, enter the following:

```
bash$ ./fcc/bin/flowCollectorController.bash status ↵
```

The NSP Flow Collector Controller and Flow Collector status information is displayed.

- b. If the NSP Flow Collector is on a dedicated station, enter the following:

---

```
bash$ ./fc/bin/flowCollector.bash status ↵
```

The NSP Flow Collector status is displayed.

If the NSP Flow Collector is running, the line that begins with flow-collector includes Started.

If the NSP Flow Collector is not running, the following is displayed:

```
nspos-karaf.service is not running
```

---

## 5

To display the NSP Flow Collector release level, perform one of the following.

- a. If the NSP Flow Collector is collocated on the station with an NSP Flow Collector Controller, enter the following:

```
bash$ ./fcc/bin/flowCollectorController.bash version ↵
```

The NSP Flow Collector Controller and Flow Collector release level is displayed.

- b. If the NSP Flow Collector is on a dedicated station, enter the following:

```
bash$ ./fc/bin/flowCollector.bash version ↵
```

The NSP Flow Collector release level is displayed.

---

## 6

Close the console window.

END OF STEPS

---

## 4.16 To open the NSP Flow Collector web UI

### 4.16.1 Purpose

Use this procedure to open the NSP Flow Collector web UI for Flow Collector configuration.

### 4.16.2 Steps

---

#### 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

---

#### 2

Enter the required user credentials and click OK. The NSP Flow Collector web UI opens.

END OF STEPS

---



---

## 4.17 To configure NSP Flow Collector statistics aggregation

### 4.17.1 Steps

- 1 

---

Open the NSP Flow Collector web UI, as described in [4.16 “To open the NSP Flow Collector web UI” \(p. 48\)](#).

The Collection Policy tab is displayed.
- 2 

---

Click on the Aggregation Policy tab.
- 3 

---

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.
- 4 

---

Configure the aggregations.

**i** **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.

**i** **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.
- 5 

---

Configure the transfer of BB NAT records in CSV format to a file server, if required.

---

**i** **Note:** A minimum 1-Gbyte/s link is required between the NSP Flow Collector and the file server.

**i** **Note:** SFTP transfers are considerably slower than FTP transfers.

1. Click on the NAT Transfer tab.
2. Configure the parameters:
  - Enable Transfer—whether file transfers are enabled
  - Transfer Protocol—FTP or SFTP
  - IP Address / Host name—file server address
  - Port—file server port
  - Location—file server directory that is to contain the files
  - User—FTP or SFTP username
  - Password—FTP or SFTP password

**6** \_\_\_\_\_  
Click Save Configuration. The configuration is saved.

**7** \_\_\_\_\_  
Close the NSP Flow Collector web UI.

**END OF STEPS** \_\_\_\_\_

---

## NSP Flow Collector Controller administration procedures

### 4.18 NSP Flow Collector Controller administration overview

#### 4.18.1 Description

The following procedures describe NSP Flow Collector Controller administration operations.

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

- # —root user
- bash\$ —nsp user

### 4.19 To start or stop an NSP Flow Collector Controller



#### CAUTION

##### Data loss

*Stopping an NSP Flow Collector Controller may affect the statistics collection of the associated NSP Flow Collectors.*

*Perform the procedure only under the guidance of technical support during a scheduled maintenance period.*

#### 4.19.1 Steps

1 \_\_\_\_\_  
Log in to the NSP Flow Collector Controller station as the nsp user.

2 \_\_\_\_\_  
Open a console window.

3 \_\_\_\_\_  
Enter the following:

```
bash$ cd /opt/nsp/flow/fcc/bin ↵
```

4 \_\_\_\_\_  
To stop the NSP Flow Collector Controller, enter the following:



**Note:** If the NSP Flow Collector Controller is collocated on a station with an NSP Flow Collector, stopping the NSP Flow Collector Controller also stops the Flow Collector.

```
bash$ ./flowCollectorController.bash stop ↵
```

The NSP Flow Collector Controller stops.

---

5

To start the NSP Flow Collector Controller, enter the following:

**i** **Note:** If the NSP Flow Collector Controller is collocated on a station with an NSP Flow Collector, starting the NSP Flow Collector Controller also starts the Flow Collector.

```
bash$ ./flowCollectorController.bash start ↵
```

The NSP Flow Collector Controller starts.

---

6

Close the console window.

END OF STEPS

---

## 4.20 To display the NSP Flow Collector Controller status or release level

### 4.20.1 Steps

---

1

Log in to the NSP Flow Collector Controller station as the nsp user.

---

2

Open a console window.

---

3

Enter the following:

```
bash$ cd /opt/nsp/flow/fcc/bin ↵
```

---

4

To view the NSP Flow Collector Controller status, enter the following:

```
bash$ ./flowCollectorController.bash status ↵
```

The NSP Flow Collector Controller status is displayed.

If the NSP Flow Collector Controller is running, the line that begins with flow-collector-controller includes Started.

If the NSP Flow Collector Controller is not running, the following is displayed:

```
nspos-karaf.service is not running
```

---

5

To view the NSP Flow Collector Controller release level, enter the following:

```
bash$ ./flowCollectorController.bash version ↵
```

The NSP Flow Collector Controller release level is displayed

- 
- 6 \_\_\_\_\_  
Close the console window.

END OF STEPS \_\_\_\_\_

## 4.21 To open the NSP Flow Collector Controller web UI

### 4.21.1 Purpose

Use this procedure to open the NSP Flow Collector Controller web UI for Flow Collector Controller configuration.

### 4.21.2 Steps

- 1 \_\_\_\_\_  
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

- 2 \_\_\_\_\_  
Enter the required user credentials and click OK. The NSP Flow Collector Controller web UI opens.

END OF STEPS \_\_\_\_\_

## 4.22 To force an NSP Flow Collector Controller to extract a network data snapshot

### 4.22.1 Purpose

An NSP Flow Collector Controller requires an image, called a snapshot, of current NFM-P data that is subsequently distributed to each NSP Flow Collector that it controls. Perform this procedure to force an NSP Flow Collector Controller to extract the system Cflowd or AA Cflowd provisioned-object snapshot from the NFM-P.



#### CAUTION

#### Service Disruption

*Performing the procedure consumes NFM-P main server resources, and is typically required only when recommended by technical support.*

*Perform the procedure only if required, and only under the guidance of technical support during a period of low NFM-P system activity.*

---

## 4.22.2 Steps

- 1 \_\_\_\_\_  
Open the NSP Flow Collector Controller web UI, as described in [4.21 “To open the NSP Flow Collector Controller web UI” \(p. 53\)](#).  
The NFM-P Configuration tab is displayed.
- 2 \_\_\_\_\_  
Click on the Operations tab.
- 3 \_\_\_\_\_  
To force the snapshot extraction for AA Cflowd statistics collection, click Force AA Snapshot Extraction.  
The extraction begins.
- 4 \_\_\_\_\_  
To force the snapshot extraction for system Cflowd statistics collection, click Force SYS Snapshot Extraction.  
The extraction begins.
- 5 \_\_\_\_\_  
Close the NSP Flow Collector Controller web UI.

**END OF STEPS** \_\_\_\_\_

---

## MDM administration procedures

### 4.23 MDM server administration overview

#### 4.23.1 Description

The following procedures describe MDM server administration operations.

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

- # —root user
- bash\$ —nsp user

### 4.24 To start or stop an MDM server

#### 4.24.1 Purpose

Perform this procedure to start or stop an MDM server.

**i** **Note:** In a redundant MDM deployment, you must perform the steps on the standby MDM server station first.

#### 4.24.2 Steps

- 1 \_\_\_\_\_  
Log on to the MDM server station as the root user.
- 2 \_\_\_\_\_  
Open a console window.
- 3 \_\_\_\_\_  
To stop the MDM server, enter the following:  
`# systemctl stop nsp-mediation.service ↵`  
The MDM server stops.
- 4 \_\_\_\_\_  
To start the MDM server, enter the following:  
`# systemctl start nsp-mediation.service ↵`
- 5 \_\_\_\_\_  
Close the console window.

END OF STEPS \_\_\_\_\_

---

## 4.25 Workflow for commissioning a device for model-driven management

### 4.25.1 Purpose

Use this workflow as a high-level guide to prepare a device to be managed using MDM. For the NSP to manage an NE using MDM, it cannot be managed by the same NSP through NFM-P.

This procedure provides the generic steps for an SR OS NE. See the adaptor user guide for the specific CLI commands to execute as part of this workflow.

Other devices will have similar mandatory actions, such as configuring NE identification information and configuring management protocols, but the specific steps will be different.

### 4.25.2 Stages

- 1 

---

If the NE was managed by NFM-P, it must be unmanaged from NFM-P before it can be discovered through MDM. See the procedure to manage, unmanage, and delete devices in the *NSP NFM-P User Guide*.
- 2 

---

Open a console window on the device.
- 3 

---

Perform required pre-configuration on the device:

  - Device identification: defines the NE Name used for filtering, configuration and monitoring of the device in NSP
  - Management Interface protocol configuration: defines authentication, capabilities and behaviour of the management interface

See the adaptor documentation and the documentation for the NE for details.
- 4 

---

Use the Device Administrator application to discover the device and to verify that the device configuration allows management of the device. See the Device Administrator application help for information about device discovery.




---

## NFM-T server administration procedures


### 4.26 To rollback integration between an NSP or NFM-P server and a standalone NFM-T system

#### 4.26.1 Purpose

Use this procedure to rollback a previously-configured integration between an NSP or NFM-P server and an NFM-T system that was deployed in a standalone configuration.

 **Note:** The rollback may take up to 1 hour and 20 minutes to complete.

#### 4.26.2 Steps

- 1 \_\_\_\_\_  
Log in to the NFM-T host server Auto Installer (AI) Web-UI as admin user.
- 2 \_\_\_\_\_  
On the Regular Operations tab choose Manage configurations > Existing Configurations, then click on the Action link of the bench that needs to be rolled back.
- 3 \_\_\_\_\_  
On the "Action on bench <bench\_name>" GUI, click on the Install tab and execute "Update bench" with the following parameters:
  - Path to depot: /DEPOT/<NFM-T\_Current\_Load>/  
**NOTE:** This must be the same load path as the NFM-T.
  - Select upgrade operation type: Update ConfigurationClick Execute to rollback the site.  
 **Note:** This operation may take up to 1 hour and 15 minutes to complete.
- 4 \_\_\_\_\_  
When the Update Configuration finishes, the NFM-T GUI launch icon should no longer appear on the NSP Launchpad.
- 5 \_\_\_\_\_  
On the 'Action on bench <bench\_name>' GUI, click on the Certificates tab and Execute Update Certificates.
- 6 \_\_\_\_\_  
Launch the NFM-T GUI from the Web Client to make sure that the NFM-T GUI is accessible without using the NSP Launchpad.

7

Ensure all OTNE, Services, and managed objects are present on the NFM-T GUI.

8

Perform one of the following:

a. If the NFM-T system was integrated with an NSP server, perform the following steps:

1. Log in to the NSP server as root user and navigate to the NSP install directory.
2. Remove NFM-T credentials from the config.yml file.
3. Execute the following command to re-run the installer and update the NSP configuration:

```
# cd /<NSP_installer_path>/bin/install.sh
```

4. Restart all NSP applications, by executing the following command as root user:

**NOTE:** If the NSP was deployed with 1+1 redundancy, this command must be executed on both the primary and standby servers. If it was deployed in HA mode, the command must be executed on all clusters.

```
# nspctl <nspServer_IP_address> restart
```

b. If the NFM-T system was integrated with an NFM-P server, perform the following steps:

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$ nspctl --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:
  - a. As root user, execute:

```
# cd /opt/nsp/os/install/examples
```

- b. Copy the NFM-T integration configuration from the config.json file.
- c. Modify the config.json file in the /opt/nsp/os/install directory by adding the copied NFM-T integration configuration.
- d. 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.

9

When the restart has completed, execute the following script on all NSP servers to clear optical alarms, network elements, and services inherited from NFM-T server integration:

---

```
# cd /<NSP_installer_path>/tools/nfmt/  
  
# nfmt-rollback.py -ip <NSP IP> -user <username> -pass <password>
```

Where:

*NSP IP* is the IP address of the NSP server

*Username* is the NSP admin user name

*Password* is the NSP admin user password

---

10

Log in to the NSP GUI and make sure the inherited optical alarms, network elements, and services have been cleared.

END OF STEPS

---

## 4.27 To rollback integration between an NSP or NFM-P server and a classic HA NFM-T system

### 4.27.1 Purpose

Use this procedure to rollback a previously-configured integration between an NSP or NFM-P server and an NFM-T system that was deployed in a classic HA configuration.

**i** **Note:** This procedure assumes the active instance is on NOC and the standby instance is on DRC. If this is not the case, the procedure must be implemented in dual mode (DRC replaced with NOC, and vice versa).

The rollback may take up to 2 hours and 30 minutes to complete.

### 4.27.2 Before you begin

Before performing this rollback procedure, verify that replication has been enabled (NOC/DRC with data line up) via the NFM-T PMC GUI.

### 4.27.3 Steps

---

1

Log in to the active (NOC) NFM-T Web-UI and launch the Process Monitoring and Control (PMC) Java GUI Dashboard by choosing ADMINISTER > PMC.

---



2

From the PMC GUI, select Switch Mode > Action > To Manual Switch. This disables automatic switchover, if enabled.

---

3

Click on the Replication icon, choose Action > Replication Manager > Stop replication.

- 4 \_\_\_\_\_  
Log in to the NFM-T Host Server Auto Installer (AI) Web-UI as admin user.
  
- 5 \_\_\_\_\_  
From the Regular Operations tab of the AI Web-UI, select Manage configurations > Existing Configurations, then click on the Action link of the bench that needs to be rolled back.
  
- 6 \_\_\_\_\_  
On the "Action on bench <bench\_name>" GUI, click on the Install tab and execute "Update bench" for DRC with the following parameters:
  - Path to depot: /DEPOT/<NFM-T\_Current\_Load>/  
**NOTE:** This must be the same load path as the NFM-T.
  - Select the HA site to update: DRC
  - Select upgrade operation type: Update ConfigurationClick Execute to rollback the DRC site.  
 **Note:** This operation may take up to 1 hour and 15 minutes to complete.
  
- 7 \_\_\_\_\_  
When the DRC rollback has completed, return to the "Action on bench <bench\_name>" GUI and click on the Stop tab.
  
- 8 \_\_\_\_\_  
Click Stop Control on NOC site and then Stop processes on the NOC site.
  
- 9 \_\_\_\_\_  
From the Start tab of the AI Web-UI, start processes on the DRC site.
  
- 10 \_\_\_\_\_  
From the Install tab, execute "Update bench" for NOC with following parameters:
  - Path to depot: /DEPOT/<NFM-T\_Current\_Load>/  
**NOTE:** This must be the same load path as the NFM-T
  - Select the HA site to update: NOC
  - Select upgrade operation type: Update ConfigurationClick Execute to rollback the NOC site.  
 **Note:** This operation may take up to 1 hour and 15 minutes to complete.
  
- 11 \_\_\_\_\_  
When the NOC rollback has completed, return to the AI Web-UI menu and click on the Install tab.

- 
- 12 From the Install tab, execute “Integration”, specifying DRC as the affected site.
- 
- 13 From the Start tab, execute “Start HA” on NOC.
- 
- 14 Log in to the Web-UI and launch the PMC GUI. From the GUI, ensure all bench instances are up and running.
- 
- 15 On the AI Web-UI, click on the Start tab and execute “Start HA” on the DRC.
- 
- 16 When the Update Configuration finishes, the NFM-T GUI launch icon should no longer appear on the NSP Launchpad.
- 
- 17 Launch the NFM-T GUI from the Web Client to make sure that the NFM-T GUI is accessible without using the NSP Launchpad.
- 
- 18 Ensure all OTNE, Services, and managed objects are present on the NFM-T GUI.
- 
- 19 From the PMC GUI, start data replication.
- 
- 20 When data replication has completed, switch back activity from DRC to NOC.
- 
- 21 Perform one of the following:
- a. If the NFM-T system was integrated with an NSP server, perform the following steps:
    1. Log in to the NSP server as root user and navigate to the NSP install directory.
    2. Remove NFM-T credentials from the config.yml file.
    3. Execute the following command to re-run the installer and update the NSP configuration:

```
# cd /<NSP_installer_path>/bin/install.sh
```
    4. Restart all NSP applications, by executing the following command as root user:

**NOTE:** If the NSP was deployed with 1+1 redundancy, this command must be executed on both the primary and standby servers. If it was deployed in HA mode, the command must be executed on all clusters.

To rollback integration between an NSP or NFM-P server and a classic HA NFM-T system

---

```
# nspdctl <nspServer_IP_address> restart
```

- b. If the NFM-T system was integrated with an NFM-P server, perform the following steps:
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:
  - a. As root user, execute:

```
# cd /opt/nsp/os/install/examples
```
  - b. Copy the NFM-T integration configuration from the config.json file.
  - c. Modify the config.json file in the /opt/nsp/os/install directory by adding the copied NFM-T integration configuration.
  - d. 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.

---

## 22

When the restart has completed, execute the following script on all NSP servers to clear optical alarms, network elements, and services inherited from NFM-T server integration:

```
# cd /<NSP_installer_path>/tools/nfmt/
```

```
# nfmt-rollback.py -ip <NSP IP> -user <username> -pass <password>
```

Where:

*NSP IP* is the IP address of the NSP server

*Username* is the NSP admin user name

*Password* is the NSP admin user password

---

## 23

Log in to the NSP GUI and make sure the inherited optical alarms, network elements, and services have been cleared.

END OF STEPS

---

---

## 4.28 To rollback integration between an NSP or NFM-P server and a hot HA NFM-T system

### 4.28.1 Purpose

Use this procedure to rollback a previously-configured integration between an NSP or NFM-P server and an NFM-T system that was deployed in a hot HA configuration.

**i** **Note:** This procedure assumes the active instance is on NOC and the standby instance is on DRC. If this is not the case, the procedure must be implemented in dual mode (DRC replaced with NOC, and vice versa).

The rollback may take up to 2 hours and 30 minutes to complete.

### 4.28.2 Before you begin

Before performing this rollback procedure, verify that replication has been enabled (NOC/DRC with data line up) via the NFM-T PMC GUI.

### 4.28.3 Steps

- 1 \_\_\_\_\_  
Log in to the active (NOC) NFM-T Web-UI and launch the Process Monitoring and Control (PMC) Java GUI Dashboard by choosing ADMINISTER > PMC.
- 2 \_\_\_\_\_  
Disable automatic switchover, if enabled.
- 3 \_\_\_\_\_  
Right-click on each instance available in System Monitor and choose High Availability > Disable Hot Standby.
- 4 \_\_\_\_\_  
Log in to the NFM-T Host Server Auto Installer (AI) Web-UI as admin user.
- 5 \_\_\_\_\_  
From the Regular Operations tab of the AI Web-UI, select Manage configurations > Existing Configurations, then click on the Action link of the bench that needs to be rolled back.
- 6 \_\_\_\_\_  
On the "Action on bench <bench\_name>" GUI, click on the Install tab and execute "Update bench" for DRC with the following parameters:
  - Path to depot: /DEPOT/<NFM-T\_Current\_Load>/  
**NOTE:** This must be the same load path as the NFM-T.
  - Select the HA site to update: DRC
  - Select upgrade operation type: Update Configuration

---

Click Execute to rollback the DRC site.

**i** **Note:** This operation may take up to 1 hour and 15 minutes to complete.

---

7

When completed, ssh to the NOC (active) NFM-T VM and place it in Standby mode by executing the following command on the NOC cli:

```
/usr/Systems/<instance>_<instance_id>_Master/MWSVC/HA/script/HAClient  
tosby
```

---

8

Connect to the rolled back DRC VM Web-UI as an admin user.

---

9

To start monitoring the network, navigate to Dashboard > ADMINISTER > System Monitor on the DRC Web-UI, then right-click on each available instance and choose High Availability > To Active.

---

10

Go to the Install tab on the AI Web-UI and execute "Update bench" with following parameters:

- Path to depot: /DEPOT/<NFM-T\_Current\_Load>/  
**NOTE:** This must be the same load path as the NFM-T
- Select the HA site to update: NOC
- Select upgrade operation type: Update Configuration

Click Execute to rollback the NOC site.

**i** **Note:** This operation may take up to 1 hour and 15 minutes to complete.

---

11

From the DRC NFM-T System Monitor Web-UI, right-click on High Availability and select Companion To Standby.

---

12

Right-click on the High Availability and select Enable Hot Standby to activate Replication.

---

13

Right-click on the High Availability and select Switchover to switch activity back to the NOC Site.

---

14

When the Update Configuration finishes, the NFM-T GUI launch icon should no longer appear on the NSP Launchpad.



---

15

Launch the NFM-T GUI from the Web Client to make sure that the NFM-T GUI is accessible without using the NSP Launchpad.

---

16

Ensure all OTNE, Services, and managed objects are present on the NFM-T GUI.

---

17

Perform one of the following:

a. If the NFM-T system was integrated with an NSP server, perform the following steps:

1. Log in to the NSP server as root user and navigate to the NSP install directory.
2. Remove NFM-T credentials from the config.yml file.
3. Execute the following command to re-run the installer and update the NSP configuration:

```
# cd /<NSP_installer_path>/bin/install.sh
```

4. Restart all NSP applications, by executing the following command as root user:

**NOTE:** If the NSP was deployed with 1+1 redundancy, this command must be executed on both the primary and standby servers. If it was deployed in HA mode, the command must be executed on all clusters.

```
# nspctl <nspServer_IP_address> restart
```

b. If the NFM-T system was integrated with an NFM-P server, perform the following steps:

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$ nspctl --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:
  - a. As root user, execute:

```
# cd /opt/nsp/os/install/examples
```

- b. Copy the NFM-T integration configuration from the config.json file.
- c. Modify the config.json file in the /opt/nsp/os/install directory by adding the copied NFM-T integration configuration.
- d. 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.

**18** 

---

When the restart has completed, execute the following script on all NSP servers to clear optical alarms, network elements, and services inherited from NFM-T server integration:

```
# cd /<NSP_installer_path>/tools/nfmt/
```

```
# nfmt-rollback.py -ip <NSP IP> -user <username> -pass <password>
```

Where:

*NSP IP* is the IP address of the NSP server

*Username* is the NSP admin user name

*Password* is the NSP admin user password

**19** 

---

Log in to the NSP GUI and make sure the inherited optical alarms, network elements, and services have been cleared.

**END OF STEPS** 

---

---

## 5 NSP database administration

### 5.1 NSP database administration overview

#### 5.1.1 Introduction

This chapter describes the procedures that must be performed in order to preserve crucial NSP system data in the case of a system failure.

##### Shared-mode deployments

In a shared-mode NSP deployment, you must synchronize the backup and restore operations among the system components. See the specific module or product documentation, as required, for information about system backup and restore operations for other modules and products..

##### Database failure notifications

The NSP raises the following Fault Management system alarms in response to a suspected PostgreSQL database failure:

- Major—one or more follower databases are unresponsive
- Critical—the leader database is unresponsive

**i** **Note:** The alarms do not clear automatically when the problem is resolved, so must be cleared manually.

### 5.2 NSP database administration procedures

#### 5.2.1 Description

The following procedures describe NSP database administration operations.

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

- # —root user
- bash\$ —nsp user

### 5.3 To manually back up the NSP databases

#### 5.3.1 Purpose

Use this procedure to manually back up the contents of the NSP Neo4j, PostgreSQL, and Tomcat databases.

**i** **Note:** The Tomcat database is included only in an NSP system that includes the NRC-F.

**i** **Note:** The NSP performs scheduled daily database backups, which are stored in the following

---

directory for up to seven days:

/opt/nsp/backup/scheduled

A maximum of four backups can be saved for up to one month. The backup schedule is defined in the following file:

/opt/nsp/scripts/db/nsp-backup.conf

**i** **Note:** If the NSP servers are deployed in HA mode, you must perform the backup on the active member of each cluster.

### 5.3.2 Steps

1 \_\_\_\_\_

Log in to the primary NSP server as the nsp user.

2 \_\_\_\_\_

Open a console window.

3 \_\_\_\_\_

Enter the following:

```
bash$ nspdctl --host server backup -d backup_directory ↵
```

where

*server* is the NSP server IP address or hostname

*backup\_directory* is the name of a new directory that is to hold the database backup file set; if the directory already exists, the backup fails

The NSP backs up the databases.

4 \_\_\_\_\_

Enter the following to verify that the backup completed successfully.

```
bash$ nspdctl --host server backup status ↵
```

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

5 \_\_\_\_\_

As the nsp user, transfer the backup files from *backup\_directory* to a secure location for safekeeping.

6 \_\_\_\_\_

Close the console window.

END OF STEPS \_\_\_\_\_

---

## 5.4 To manually restore the NSP databases

### 5.4.1 Purpose

Use this procedure to restore the NSP Neo4j, PostgreSQL, and Tomcat databases from a backup set, for example, after a database failure. The databases are automatically backed up daily on an NSP server, and can be manually backed up using an NSP server CLI, as described in 5.3 “To manually back up the NSP databases” (p. 67), or using the NSP REST API.

**i** **Note:** The Tomcat database is included only in an NSP system that includes the NRC-F, and does not need to be restored otherwise.

**i** **Note:** All backup files must be from the same backup set, and must each be restored as part of one maintenance activity.

### 5.4.2 Steps

1 \_\_\_\_\_  
Copy the Neo4j, PostgreSQL, and Tomcat database backup files, as required, to an empty temporary directory on the standalone or primary NSP server station.

**i** **Note:** A Tomcat database backup file is present only if the NSP system includes the NRC-F, and is not required otherwise.

The location of an automated daily backup file set on an NSP server station is:

`/opt/nsp/backup/scheduled/timestamp-daily`  
where *timestamp* is the backup creation time

2 \_\_\_\_\_  
Log in as the root user on the standalone or primary NSP server station.

3 \_\_\_\_\_  
Open a console window.

4 \_\_\_\_\_  
Enter the following once for each NSP server to stop the server SDN and nspOS services:

**i** **Note:** In a redundant NSP deployment, you must specify the standby NSP server first.

```
bash$ nspdctl --host server_IP stop ↵
```

where *server\_IP* is the NSP server IP address

5 \_\_\_\_\_  
Enter the following to switch to the root user:

```
bash$ su - ↵
```

---

6

Enter the following:

```
# cd NSP_installer_directory/tools/database ↵
```

where *NSP\_installer\_directory* is the directory that contains the extracted NSP software package

---

7

Restore the Neo4j database on each NSP server.

**i** **Note:** You must perform this step for each NSP server in a redundant deployment. Use the `--target` parameter to specify the primary or standby NSP server, as required.

1. Enter the following:

```
# ./db-restore.sh --target server_IP ↵
```

where *server\_IP* is the primary or standby NSP server IP address in a redundant deployment

**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 ↵:

```
path/nspos-neo4j_backup_timestamp.tar.gz
```

where

*path* is the absolute path of the Neo4j backup file

*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:
```

```
path/nspos-neo4j_backup_timestamp.tar.gz? Press return to continue,  
or Ctrl+C to abort:
```

3. 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
```

4. If the `failed` value is greater than zero, a restore failure has occurred; contact technical support for assistance.

## 8

Restore the PostgreSQL database.



**Note:** You must perform this step for each NSP server in a redundant deployment. Use the `--target` parameter to specify the primary or standby NSP server, as required.

1. Enter the following:

```
# ./db-restore.sh --target server_IP ↵
```

where `server_IP` is the primary or standby NSP server IP address in a redundant deployment

**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 `↵`:

```
path/nspos-postgresql_backup_timestamp.tar.gz
```

where

`path` is the absolute path of the PostgreSQL backup file

`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:
path/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.

9

If the NSP system includes the NRC-F, restore the Tomcat database.

**i** **Note:** You must perform this step for each NSP server in a redundant deployment. Use the `--target` parameter to specify the primary or standby NSP server, as required.

1. Enter the following:

```
# ./db-restore.sh --target server_IP ↵
```

where `server_IP` is the primary or standby NSP server IP address in a redundant deployment

**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 ↵:

```
path/nsp-tomcat_backup_timestamp.tar.gz
```

where

`path` is the absolute path of the Tomcat backup file

`timestamp` is the backup creation time

The following messages and prompt are displayed:

```
PLAY [all] *****
[dbrestore : pause]
Do you want to restore the nsp Tomcat db from file:
path/nsp-tomcat_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.

**10**

---

Enter the following once for each NSP server to start the server SDN and nspOS services:

 **Note:** In a redundant NSP deployment, you must specify the primary NSP server first.

```
bash$ nspctl --host server_IP start ↵
```

where `server_IP` is the NSP server IP address

The NSP server starts.

**11**

---

Close the console window.

**END OF STEPS**

---



---

## 6 NSP system redundancy

### 6.1 NSP redundancy models

#### 6.1.1 Description

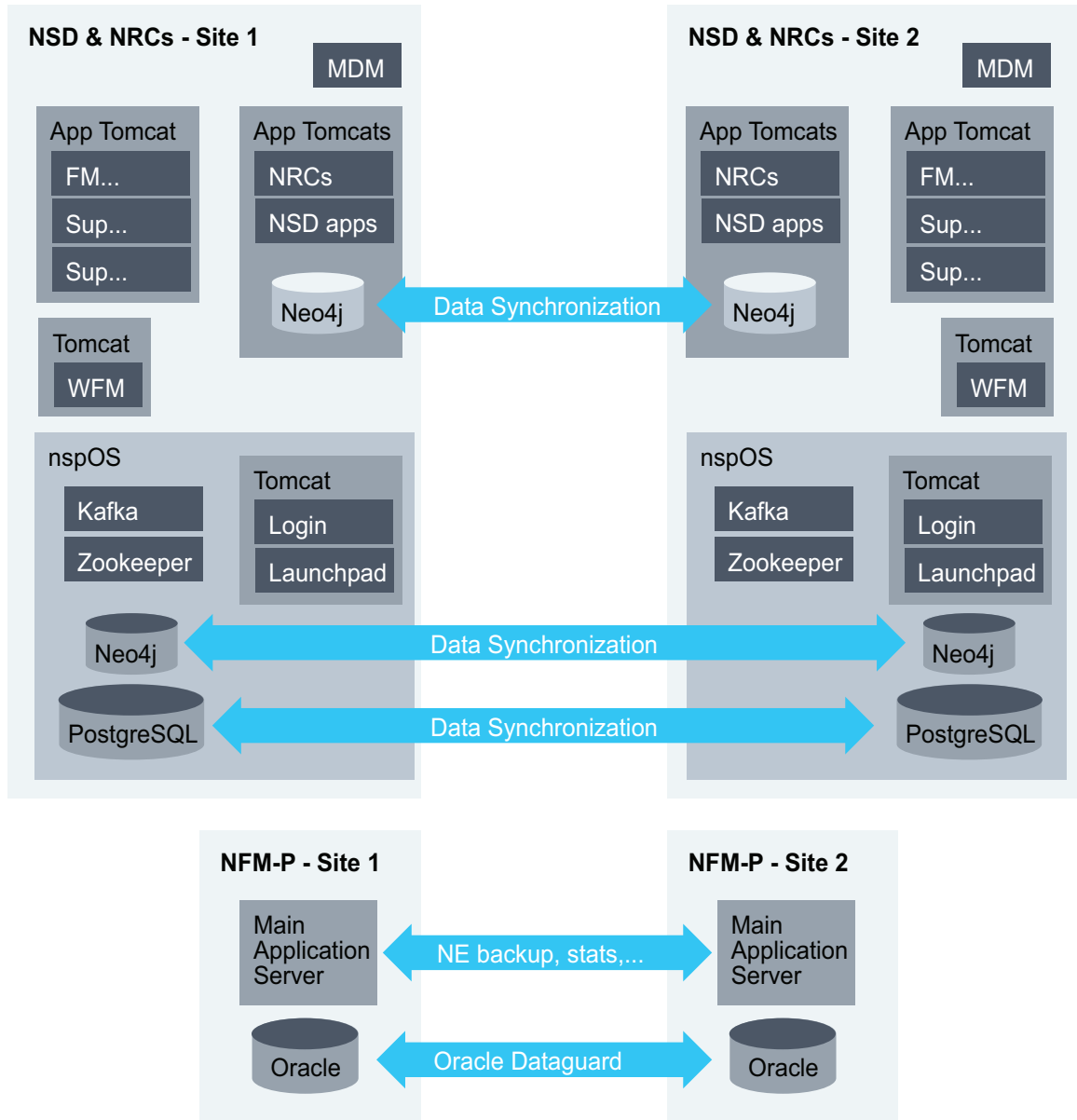
All NSP modules support a 1+1 redundancy model. In this scenario, each module has a group of active components, and a group of warm standby components; each component is a separate OS instance that hosts a module function. For example, the NFM-P has main server, main database, and optional auxiliary 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, or DR, 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 other system at the remote site is running in a warm standby mode. When redundant NSP systems are in geographically separate facilities, Nokia recommends for best performance to keep all active NSP modules on one site to minimize network latency between the modules. Aligning the active NSP modules in a shared-mode deployment is performed by an administrator.

To deploy the NSP in a redundant shared-mode configuration, each component in the deployment must be redundant. If a redundant NSP deployment includes the NFM-T, the NFM-T must be deployed as a 1+1, or classic HA, system. The NSD and NRC can be deployed as a 1+1 system, or as a 3+3 system, which is HA with DR.

The following figure shows the NSP deployed as a 1+1 system.

Figure 6-1 NSP modules deployed using 1+1 redundancy



28347

---

## 6.2 NSP redundancy failure scenarios and recovery mechanisms

### 6.2.1 Overview

The following topics describe NSP recovery actions in the event of a redundancy failure; a failure scenario may apply to multiple shared-mode configurations, depending on which components are deployed.

### 6.2.2 NSP disaster-recovery alarm behavior

The following are the alarms that the NSP raises in the Fault Management application against the NmsSystem object in response to a failure in a geographically redundant NSP system:

- PrimaryDatabaseDown—severity is Critical
- ActivitySwitch—severity is Major
- DatabaseRedundancyFailure—severity is Major

**i** **Note:** Before you manually clear an alarm, use the following command on an NSP server to check the DR site availability:

```
nspdctl system status
```

**i** **Note:** If you clear an alarm while the failure condition is still present, the NSP does not raise the alarm again.

The following failure scenario examples apply to a 1+1 DR deployment of redundant NSP sites at geographically remote facilities.

#### Scenario 1

1. The NSP at the standby site fails
2. A major DatabaseRedundancyFailure alarm is raised against the standby site.
3. The problem at the standby site is resolved, and the standby NSP returns to service after database replication begins, but the alarm does not automatically clear.
4. An administrator manually clears the alarm from the Fault Management application.

#### Scenario 2

1. The NSP at the standby site fails.
2. A major DatabaseRedundancyFailure alarm is raised against the standby site.
3. The problem at the standby site is resolved, and the standby NSP returns to service after database replication begins, but the alarm does not automatically clear.
4. The NSP at the standby site fails again; a second DatabaseRedundancyFailure alarm with a new timestamp is raised. Two DatabaseRedundancyFailure alarms are now present in the Fault Management application.
5. When the problem is resolved, an administrator manually clears both alarms from the Fault Management application.

#### Scenario 3

1. The NSP at the primary site fails.

- 
2. An activity switch occurs, and the standby site assumes the primary role.
  3. A critical PrimaryDatabaseDown alarm is raised against the new primary site.
  4. A major ActivitySwitch alarm is raised against the former primary site, which is now the standby site.
  5. The problem at the standby site is resolved, but the alarms do not automatically clear.
  6. When the problem is resolved, an administrator manually clears both alarms from the Fault Management application.

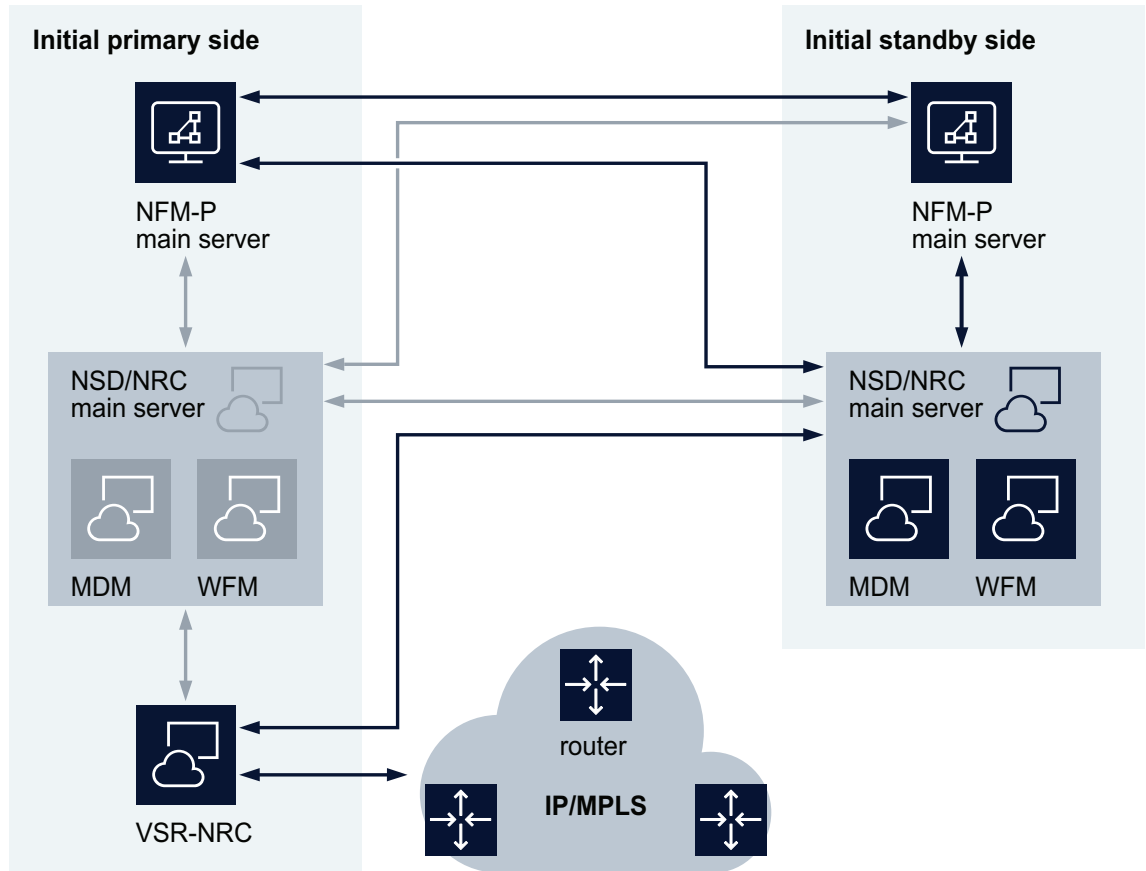
### 6.2.3 Primary NSD/NRC server failure

The nspd agents on each server exchange a heartbeat every 5 seconds. If the nspd agent on the standby server (or the leader of the standby cluster, in an HA deployment) does not receive a heartbeat within 60 seconds, the standby server (or standby cluster, in an HA deployment) is promoted to active. The new primary server (or cluster, in an HA deployment) will communicate with the primary database, the NFM-P, and the VSR-NRC. Primary server applications no longer running (nspdct status = inactive) could also trigger a switchover.



**Note:** When an NSD/NRC switchover occurs, an MDM switchover also occurs.

Figure 6-2 Primary NSD/NRC server failure

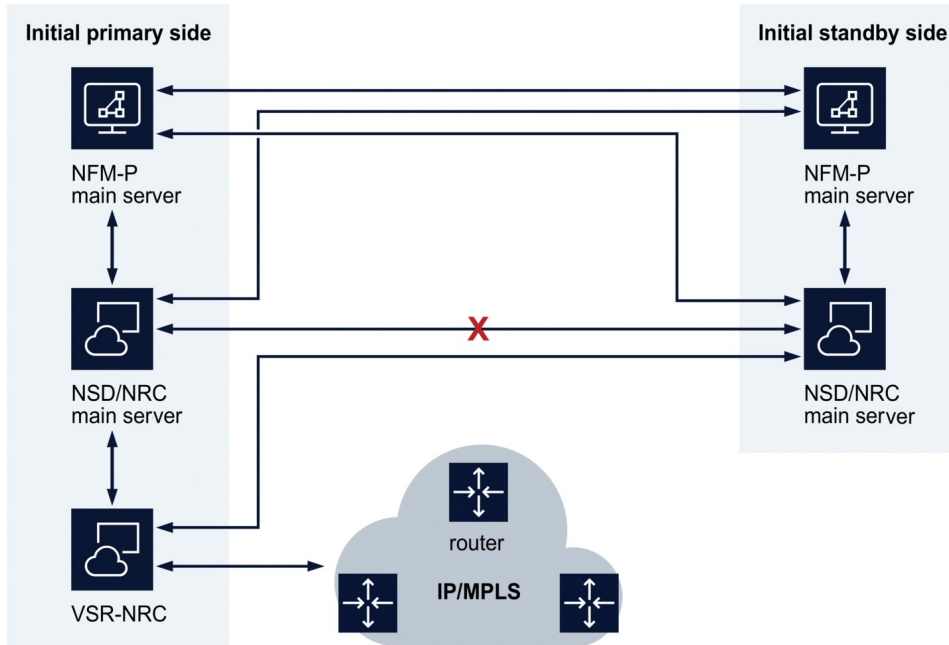


28344

#### 6.2.4 Primary and standby NSD/NRC server communication failure

When communication between NSD/NRC servers fails, both NSD/NRC servers are considered active, creating what is called a split-brain scenario. A thirty second loss of communication between the primary NSD/NRC server and the standby NSD/NRC server may trigger a switchover. When communication is restored, the NSD/NRC server with the higher uptime value is designated the primary server, and the other NSD/NRC server is designated the standby. If you want the server with the lower uptime value to be the primary server, you must shut down the server with the higher uptime value before you restore network connectivity.

Figure 6-3 Primary and standby NSD/NRC server communication failure



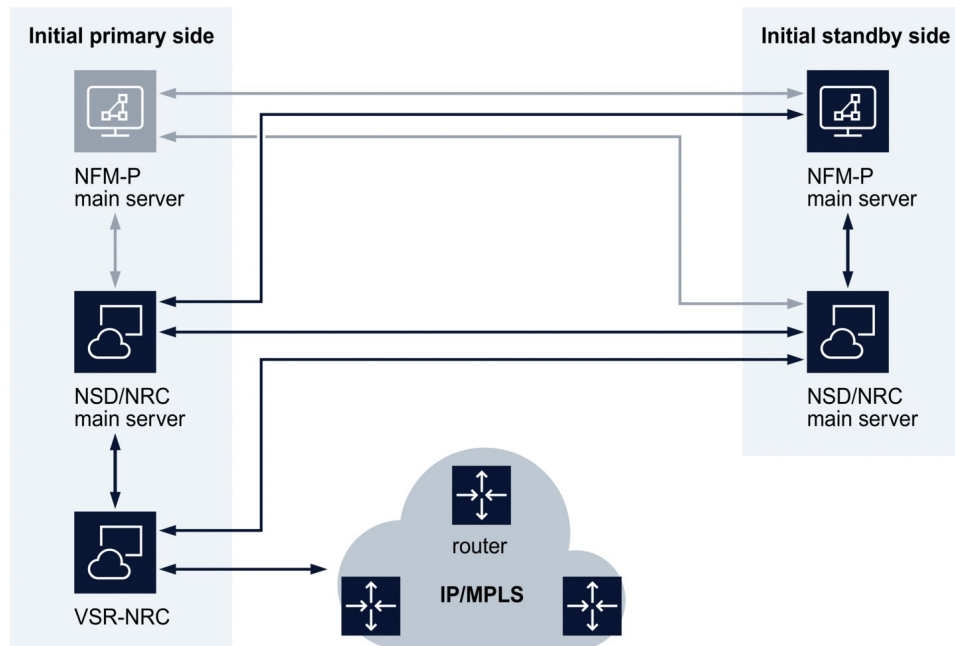
28343

### 6.2.5 NFM-P main server failure

When the primary NFM-P main server becomes unavailable, the standby main server automatically assumes the role of primary server. The NSD/NRC subsequently communicates with the new primary main server.



Figure 6-4 Primary NFM-P server goes down



28342

## 6.2.6 MDM failure

If the MDM server or cluster goes down, the administrator must perform a manual switch to the other site.

If the MDM HA cluster becomes degraded, the administrator must bring up new active MDM servers by doing one of the following:

- adding new servers to the NSP hosts file
- repairing failed MDM servers

A failed MDM server that is restored to service assumes the role of a standby MDM server.

**i** **Note:** When an NSD/NRC switchover occurs, an MDM switchover also occurs.

## 6.2.7 WFM failure

In a collocated WFM deployment, the WFM switches over when an NSD and NRC switchover occurs.

In a distributed WFM deployment, manual alignment of the WFM VMs is required. During installation, the administrator must verify that the WFM icon is displayed on the NSP Launchpad of the active NSD/NRC site. If not, the WFM may be active at the other site.

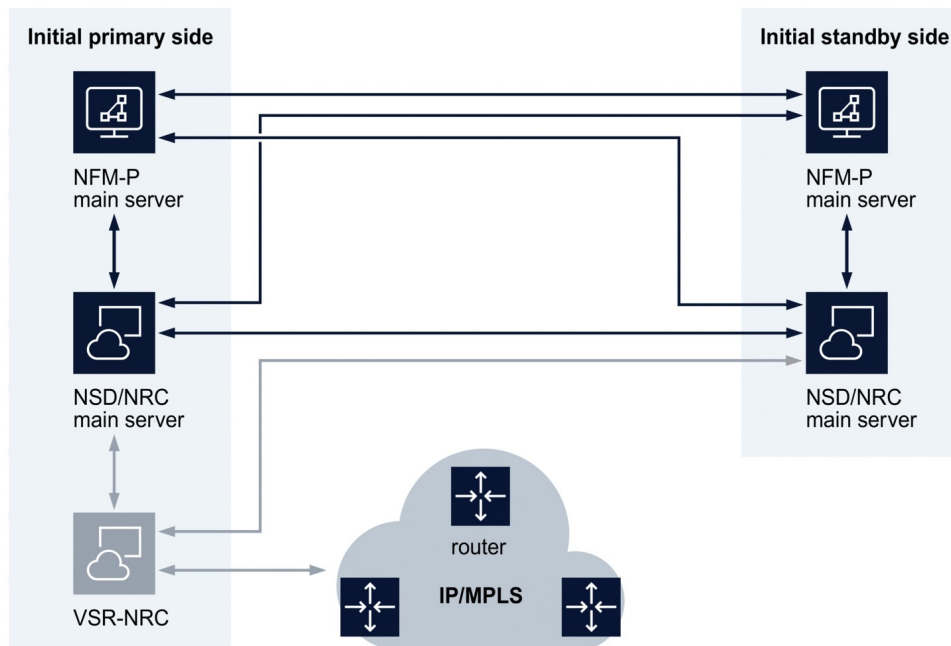
If the WFM fails, a switchover to the other WFM occurs in order to preserve the data. If the NSD/NRC remains operational at the initial primary site, the administrator must repair the failed WFM, or

install a new WFM, and then shut down the WFM at the initial standby site.

### 6.2.8 Standalone VSR-NRC failure

When a standalone VSR-NRC fails, it must be recovered. Such an action is required if the VSR-NRC IOM fails, or if both CPMs fail; if only the active CPM fails, the inactive CPM automatically becomes active.

Figure 6-5 Standalone VSR-NRC failure



28345

### 6.2.9 Primary VSR-NRC failure

The primary VSR-NRC communicates with the primary NSD/NRC server. When the primary VSR-NRC becomes unavailable, a manual NSD/NRC server switchover is required. The new primary NSD/NRC server then communicates with the VSR-NRC with which it is configured to communicate. Such an action is required if the VSR-NRC IOM fails, or if both of CPMs fail; if only the active CPM fails, the inactive CPM automatically becomes active.

After a manual NSD/NRC server switchover, LSP data is recovered only by reconfiguring any PCCs with originating PCC-initiated LSPs to communicate with the new active VSR-NRC. Alternatively, the primary VSR-NRC can be restored to service.

Figure 6-6 Primary VSR-NRC failure

