NSP
Network Services Platform Server

Gen11 RHEL 8.x User Guide

3HE-19466-AAAA-TQZZA
Issue 3
February 2025

Legal notice

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

Contents

About this document

Purpose

The *NSP Server Gen11 RHEL 8.x User Guide* describes Nokia NSP Server deployment and management activities such as system installation and upgrade, maintenance, security, and troubleshooting.

Intended audience

The audience is a deployment technician or system administrator who needs to deploy, manage, or troubleshoot the NSP Server.

Scope

The *NSP Server Gen11 RHEL 8.x User Guide* describes the NSP Server, and provides procedures for system deployment and server administration. The document scope is limited to the general management of the server platform and installed components; the document does not describe the operation, administration, or maintenance of the NSP (which is purchased separately).

Document support

Customer documentation and product support URLs:

- Documentation Center
- Technical support

How to comment

Please send your feedback to documentation.feedback@nokia.com.

Part I: Getting started

Overview

Purpose

This part of the *NSP Server Gen11 RHEL 8.x User Guide* provides information that is required in advance of deploying the server, such as platform specifications.

Contents

1 Before you begin

1.1 Product overview

1.1.1 Introduction

The NSP Server simplifies the process of sizing, purchasing, configuring and maintaining the server hardware, and the Red Hat® Enterprise Linux® (RHEL) operating system. It is a platform that can be used to support the purchase, download, and installation of the Network Services Platform (NSP) on RHEL KVM VMs.

1.1.2 Using the NSP Server

This guide principally describes deployment, upgrade, and operation, administration, and maintenance (OAM) functions that are specific to the NSP Server.

Some component functions may be available only after specific system configuration.

1.2 Deploying NSP Server

1.2.1 NSP components

NSP components, such as the NSP cluster, Deployer node, and NFM-P main server, can be downloaded and installed on the NSP Server. Refer to the *NSP Server Gen11 RHEL 8.x Release Notice* for the complete list of compatible NSP components and any restrictions to deployment.

1.2.2 Deployment options

NSP components can be deployed indirectly via one or more KVM VMs you create on the NSP Server using the NSP K8S Platform, NSP RHEL, NSP NFM-P, vCPAA, and VSR-NRC qcow2 images downloaded from the Nokia Support Portal.

Note: Bare metal deployment, that is deployment of NSP components directly on the NSP Server RHEL OS instance, is no longer supported.

1.2.3 Sizing requirements

Your official NSP Platform Sizing Response indicates whether the NSP Server can be used for your specific network, the size of each NSP component that may be deployed, and the number of NSP Servers required. An official NSP sizing recommendation is required for any deployments using the NSP Server.

Note: Any modification to the NSP Server, including hardware changes, RHEL RPM additions, and configuration changes are prohibited. Nokia provides a patch tool for updating the RHEL KVM hypervisor.

1.3 Reference documentation

1.3.1 Description

The following documents provide comprehensive information about NSP operation, administration, and maintenance:

- *NSP System Administrator Guide*
- *NSP User Guide*
- *NSP Administrator Guide*
- *NSP Classic Management User Guide*
- *NSP Planning Guide*
- *NSP Installation and Upgrade Guide*

For additional system or network management information, see the appropriate NSP, VSR-NRC, or vCPAA documentation.

2 Platform description

2.1 NSP Server hardware

2.1.1 Description

The NSP Server is delivered as a fully assembled unit that has all required hardware elements, which include the following:

- HPE DL380 Gen11 8SFF CTO Server
- 2x INT Xeon-G 5418Y CPU for HPE
- 12 x HPE 32GB 2Rx8 PC5-4800B-R Smart Kit
- HPE DL380 Gen11 8SFF U.3 Premium Kit
- 4x HPE 3.2TB NVMe MU SFF BC U.3ST MV SSD
- 2x HPE 600GB SAS 10K SFF BC MV HDD
- HPE MR416i-p Gen11 SPDM Storage Controller
- BCM 57416 10GbE 2p BASE-T Adaptor
- BCM 5719 1Gb 4p BASE-T Adaptor
- HPE 96W Smart Storage Li-ion Battery 145mm Kit
- HPE DL360 Gen11 Stg Control Enable Cable Kit
- BCM 5719 1Gb 4p BASE-T OCP Adaptor
- 2x HPE 1000W FS Titanium Hot Plug Power Supply Kit
- HPE DL3XX Gen11 CPU2/OCP2 x8 Enable Kit
- HPE DL380 Gen11 TM Y-Cable Kit
- HPE DL380/DL560 G11 2U High Performance Fan Kit
- 2x HPE DL380/DL560 G11 High Performance 2U HS Kit
- HPE DL3XX Gen11 Easy Install Rail 3 Kit

Table 2-1 Technical Specifications of the hardware

Technical Specifications	Description
Form Factor	2U rack
Chassis Type	HPE DL380 Gen11 8 SFF bay
Dimensions	8.75 x 44.8 x 72.7 cm / 3.44 x 17.64 x 28.62 in
Net Weight	29.03 kg / 64 lbs
Gross Weight	Air packed weight: 40.29 kg / 88.82 lbs
Rated Line Voltage (per power supply)	1000W (platform maximum): 100-240 VAC

Table 2-1 Technical Specifications of the hardware (continued)

Technical Specifications	Description
BTU Rating – Maximum	3039 BTU/hr (at 220V)
Temperature	10° to 35°C (50° to 95°F) at sea level
Humidity	8% to 90% - Relative humidity (Rh), 28°C maximum wet bulb temperature, non-condensing
Altitude	3050 m (10,000 ft)

Note: The included rail system is for a four post 19” cabinet. Consult Nokia for verifying specific rack mounting requirements.

2.2 Component connectivity

2.2.1 Server iLO port

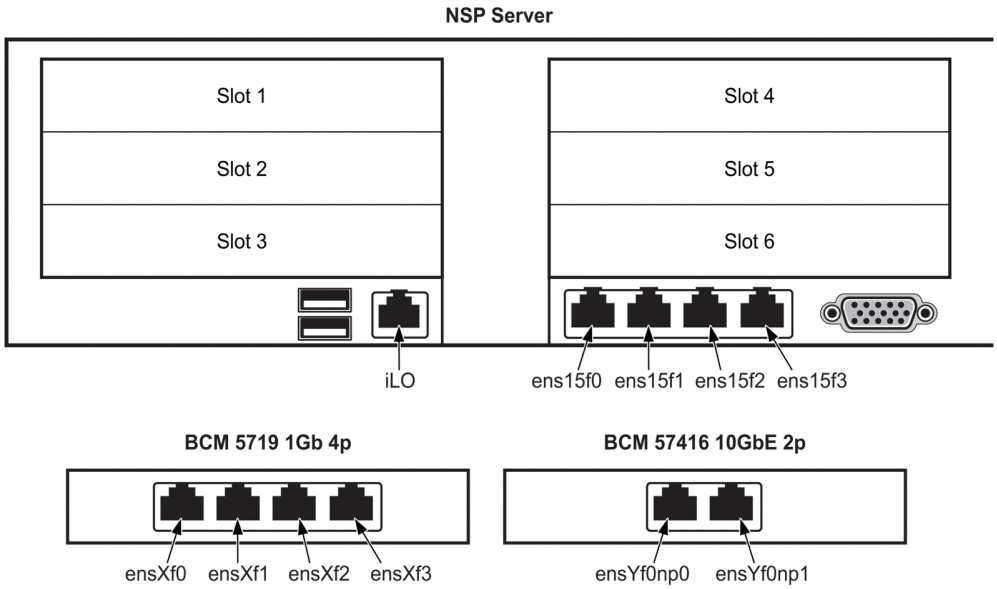
The physical iLO port on the NSP Server provides access to the HPE iLO 6 module, which is required for the management of physical host resources such as storage, devices, and network settings. The iLO 6 module also provides firmware, power, and thermal information, including event logs.

2.2.2 Server Ethernet ports

The NSP Server includes eight 1Gb and two 10Gb BASE-T Ethernet ports. The ports on the two network interface cards with four ports are 1GbE, and the ports on the network interface card with two ports are 10GbE. Due to factory integration changes, the BCM 5719 1Gb 4p and BCM 57416 10GbE 2p network interface cards, shown outside of the server in Figure 2-1, “NSP Server rear view” (p. 13), may be placed in any one of slots 1 through 3. Due to this, the physical port to OS interface mapping must be determined based upon the actual physical card slotting. The "X" and "Y" in the interface name, as shown in Figure 2-1, “NSP Server rear view” (p. 13), will match the physical slot that the interface card occupies. For example, if BCM 5719 1Gb 4p occupies slot two, the interface names will be ens2f0, ens2f1, ens2f2, and ens2f3.

During commissioning of the NSP Server, a physical connection to ens15f0 is required to access the hypervisor. Depending upon the physical connection requirements, other ports can be used for VM connectivity. Virtual bridges are preconfigured on all interfaces except for ens15f0. These bridges are created for convenience and can be deleted if required. When using multiple NSP Servers in a single deployment, it is recommended to use the 10Gb interfaces for internal NSP communication.

Figure 2-1 NSP Server rear view



2.2.3 NSP Support for RHEL IP Bonding

Nokia supports using the RHEL IP Bonding feature on the NSP Server. Some preconfigured virtual bridges will need to be deleted prior to configuring IP Bonding and then recreated manually afterwards. Support for IP Bonding is intended only to provide network interface redundancy configured in active-backup mode. All other modes of IP Bonding are not supported. See the RHEL documentation for information about configuring IP Bonding and virtual bridges.

3 Security

3.1 Hardware manufacturer recommendations

3.1.1 Description

The following recommendations from the *HPE iLO 6 User Guide* and *HPE iLO 6 Integrated Lights-Out Security Technology Brief* are implemented on the NSP Server during factory setup:

- Enforce password complexity—a user password must be at least 8 characters long and include three of the following character classes:
  - uppercase ASCII
  - lowercase ASCII
  - digits
  - special characters
- Configure host authentication and iLO 6 credentials for Smart Update Manager
- Disable iLO service port
- Set iLO security state to "High Security"
- Disable unused protocols
  - RIBCL
  - DHCPv6
  - IPMI
  - SNMP
- Configure iLO 6 Configuration Utility login
- Enable Global Component Security
- Enable Secure Boot

See the *HPE iLO 6 User Guide* and *HPE iLO 6 Integrated Lights-Out Security Technology Brief* for other security best practices regarding, for example, physical platform security, Internet security, and TLS.

3.2 iLO module access

3.2.1 Description

The following iLO module access methods are available:

- remote console—default port is 17990
- SSH—default port is 22
- SNMPv3, for receiving iLO alerts—default access port is 161; default port for receiving alerts is 162
- HTTPS web interface—default port is 443

Note: If using firewall, you need at least the remote console and HTTPS web interface ports for NSP Server installation.

Note: To use SNMPv3 with HPE SIM 7.2 or later, the SNMP Trap Port value in the iLO BIOS must be set to 50005.

See the *HPE iLO 6 User Guide and HPE iLO 6 Integrated Lights-Out Security Technology Brief* for more information.

3.3 Host OS

3.3.1 Description

Only hardening recommendations documented as supported may be applied to the RHEL operating system. The supported CIS hardening recommendations are documented Appendix A, “NSP Server RHEL OS compliance with CIS benchmarks”.

Part II: Deployment

Overview

Purpose

This part of the *NSP Server Gen11 RHEL 8.x User Guide* describes how to physically set up the server and perform subsequent NSP software installation.

Contents

4 NSP Server initial setup

4.1 Introduction

4.1.1 Description

Note: The system localization is U.S. English.

The system BIOS is factory-configured; in addition, the server is commissioned to include the following:

- Red Hat Enterprise Linux (RHEL) 8.8. Newer OS patches can be manually applied.

  Note: Even though the NSP Server RHEL ISO includes packages not installed on the NSP Server, only the packages installed are supported. The addition of other OS packages is not supported.
- HP iLO 6 management module

4.2 Workflow for initial NSP Server setup

4.2.1 Description

The following workflow describes the sequence of high-level actions to configure the required user accounts and network parameters for NSP Server deployment.

4.2.2 Stages

1

Physically mount the server chassis according to the manufacturer specifications; see the rack-mount installation instructions in the Operations chapter of the HPE User Guide for the server.

2

Make the required physical network connections; see 4.3 “To cable the server Ethernet ports” (p. 20).

3

Configure the BIOS and iLO 6 user accounts and network parameters; see 4.4 “To configure the BIOS and iLO 6” (p. 20).

4

Complete the RHEL 8 OS setup; see 4.6 “To finalize the NSP Server setup” (p. 25).

5

Download NSP software bundles and patches; see 4.7 “To download NSP Server software and RHEL patches” (p. 26)

6

Complete the NSP Server setup; see 4.8 “To finalize NSP Server setup” (p. 28).

4.3 To cable the server Ethernet ports

4.3.1 Purpose

Perform this procedure to establish the required Ethernet connections for the NSP Server.

4.3.2 Steps

1

Obtain separate Cat6 or better Ethernet cables of sufficient length to make connections from the NSP Server.

2

Connect the ports.

3

Apply power to the server by pressing the Power On/Standby LED on the front panel.

4

Monitor the LEDs on the front panel to ensure that the hardware initialization completes; see the appropriate HPE User Guide to obtain the LED status information.

5

A non-flashing green LED on a NIC indicates that an Ethernet link is established. Ensure that each connected port has an established Ethernet link.

END OF STEPS

4.4 To configure the BIOS and iLO 6

4.4.1 Purpose

Perform this procedure to secure the server BIOS and iLO 6 user accounts, and set the iLO 6 IP address.

4.4.2 Steps

Set BIOS administrator password

1

If the server is running, press and hold the power on/standby LED at the top right of the front panel until the server stops.

2

Start the server by pressing the power on/standby LED.

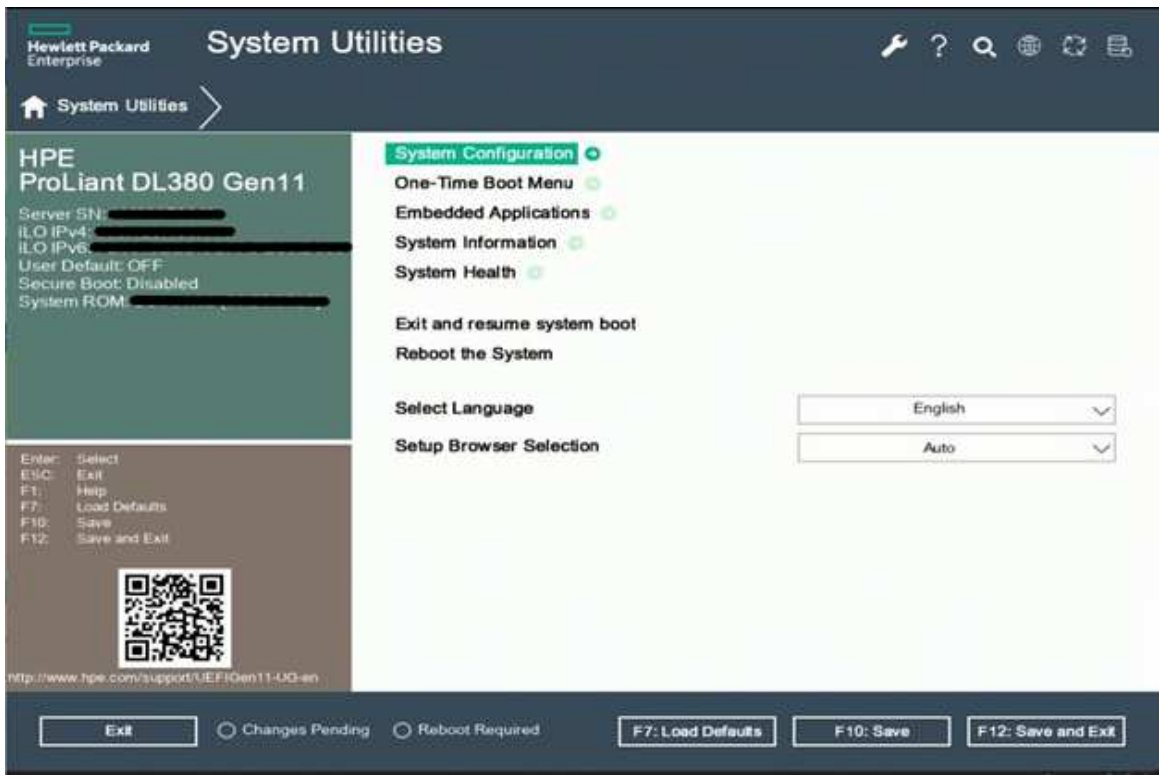
The LED lights, and the monitor displays an initialization screen before displaying the power-on self-test, or POST screen.

3

When the POST screen is displayed, press F9. The System Utilities menu opens, as shown in Figure 4-1, “BIOS System Utilities menu” (p. 20).

Menu navigation is performed using the up and down cursor keys. Pressing Enter invokes the selected menu option, and pressing the Esc key returns to the previous menu.

Figure 4-1 BIOS System Utilities menu



4

Click System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→Set Admin Password, and press ↵.

A password-entry form opens.

5

Enter a new password for the BIOS administrator account.

The password can be any combination of numbers, letters, and special characters, up to a maximum of 31 characters.

Note: Ensure that the BIOS password is stored in a secure location and available for retrieval when required.

6

Retype the password and press ↵. A confirmation dialog box appears.

7

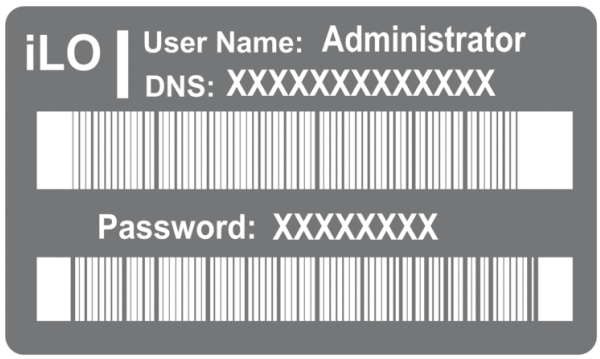
Click OK.

Change the iLO 6 administrator password

8

Pull out the serial label pull-tag beside the USB ports on the server front, as shown in Figure 4-2, “Serial label pull-tag” (p. 21).

Figure 4-2 Serial label pull-tag



9

Record the default iLO 6 username and password on the label.

10

From the System Utilities menu, select System Configuration→iLO 6 Configuration Utility.

11

Enter the recorded login credentials.

12

Select User Management→Edit/Remove User.

13

Choose Edit from the Action menu for the Administrator user.

14

Place the cursor in the Password field and then press Enter. The Enter your new password form opens.

15

Enter a new password. The Confirm your new password form opens.

16

Retype the password and press ↵. A confirmation dialog box appears.

17

Click OK.

Add or edit other iLO 6 user accounts

18

If you do not need to add or modify another iLO 6 user account, go to Step 24.

19

Perform one of the following.

a. Add a user; choose Add User from the Action menu.

b. Edit or remove a user; choose Edit/Remove from the Action menu of a listed user.

20

If required, change the user password.

1. Place the cursor in the Password field and then press Enter. The Enter your new password form opens.
2. Enter a new password. The Confirm your new password form opens.
3. Retype the password and press ↵. A confirmation dialog box appears.

4. Click OK.

21

If required, change the Login Name.

22

If required, modify the user account privileges.

1. To assign a privilege, select YES in the menu beside the privilege name.
2. To remove a privilege, select NO.

Note: The Login privilege is assigned to each user by default, so is not configurable in the iLO 6 Configuration Utility.

23

Perform Step 19 to Step 22 as required to add or modify another user account, if required.

Set iLO 6 IP address

24

From the System Utilities menu, select System Configuration→iLO 6 Configuration Utility.

You are prompted to enter your login credentials.

25

Enter the iLO 6 username and password.

26

Choose Network Options.

27

Configure the parameters as required.

28

Record the IP address and other parameter values that you specify.

29

When prompted to confirm the changes, click Yes – Save Changes to exit the utility and reboot the system.

END OF STEPS

4.5 To configure the SNMP settings on HPE servers

4.5.1 Purpose

Perform the following procedure to modify SNMP settings on HPE servers.

Note: Enable SNMP if you want to monitor the NSP Server from MDM, which may or may not be installed on the same NSP Server. As long as the NSP Server iLO IP is reachable, you can monitor NSP Server from any MDM that is part of the same network as the NSP Server's.

4.5.2 Steps

1

Enable the SNMP on the Settings screen under Management, SNMP Settings in the iLO web interface.

2

Configure an SNMPv3 user with the following credentials:

- **Security Name**→ username
- **Authentication Protocol**→ SHA
- **Privacy Protocol**→ AES
- **Authentication Passphrase**→ authentication password
- **Privacy Passphrase**→ privacy password
- **User Engine ID**→ (empty)

3

Set the SNMP alert destinations. These destinations are set in each server to an SNMP server address.

Specify the MDM IPv4 mediation IP address (both datacenters in a DR configuration). Set the protocol to SNMPv3 Trap and select the user you previously created.

END OF STEPS

4.6 To finalize the NSP Server setup

4.6.1 Purpose

Perform this procedure to configure NSP Server IP, address, hostname, and NTP.

4.6.2 Steps

1

Login via iLO as an IP address has not been assigned to the ens15f0 Ethernet interface yet.

2

Consult the RHEL 8 documentation to configure an IP address on the interfaces that will be used.

3

Set the hostname.

```
hostnamectl set-hostname <hostname>
```

4

Configure the chrony.

Note: The RHEL chrony packages are installed on the NSP Server, but not configured. See the RHEL documentation for information about configuring chrony.

END OF STEPS

4.7 To download NSP Server software and RHEL patches

4.7.1 Purpose

Perform this procedure to download the NSP Server software setup bundle and NSP Server RHEL patch bundle.

4.7.2 Steps

1

Log into the Nokia software download site and obtain the NSP Server Gen11 RHEL8 setup tar bundle and SHA256 checksum files:

- NSP_SERVER_GEN11_RHEL8_*yyyy.mm.dd*.tar.gz
- NSP_SERVER_GEN11_RHEL8_*yyyy.mm.dd*.sha256sum

where

yyyy.mm.dd is the software bundle release date

2

Transfer the files to the NSP Server into the /extra directory and verify the checksum.

1. Enter the following:

   ```
   # cat /extra/NSP_SERVER_GEN11_RHEL8_yyyy.mm.dd.sha256sum ↵
   ```

   where

   yyyy.mm.dd is the software bundle release date

   The expected SHA-256 checksum of the downloaded tar file is displayed.
2. Enter the following:

```
# sha256sum /extra/NSP_SERVER_GEN11_RHEL8_yyyy_mm.dd.tar.gz ↲
```

where

yyyy_mm_dd is the software bundle release date

The SHA-256 checksum of the NSP Server setup script tar bundle is displayed.

3. Verify that the checksum matches the associated checksum displayed in 1. If the checksum does not match, download a new copy of the file and repeat this step.

3

Enter the following:

```
# cd /extra ↲
```

4

Enter the following:

```
# tar -xvf /extra/NSP_SERVER_GEN11_RHEL8_yyyy_mm.dd.tar.gz ↲
```

where

yyyy.mm.dd is the software bundle release date

The NSP Server installation files are extracted to the current directory.

5

Log into the Nokia software download site and obtain the latest NSP RHEL patch bundle and SHA256 checksum files:

- NSP_RHEL8_OEM_UPDATE_*yy_mm*.tar.gz
- OEM_Images.cksum

where

yy_mm.dd is the issue dateof the OS update

6

Transfer the files to the NSP Server to the /extra/sw/rpms/rhel/ directory and verify the checksum.

1. Enter the following:

   ```
   # cat /extra/sw/rpms/rhel/OEM_Images.cksum ↲
   ```

   The expected SHA-256 checksum of the downloaded tar file is displayed.

2. Enter the following:

   ```
   # sha256sum /extra/sw/rpms/rhel/NSP_RHEL8_OEM_UPDATE_yy_mm.tar.gz ↲
   ```

   where

   yy_mm is the date of the OS update

   The SHA-256 checksum of the Nokia RHEL patch bundle is displayed.

3. Verify that the checksum matches the checksum displayed in 1. If the checksum does not match, download a new copy of the file and repeat this step.

END OF STEPS

4.8 To finalize NSP Server setup

4.8.1 Purpose

Perform this procedure to complete the software setup of the NSP Server, including security hardening, setting passwords, and partition creation.

4.8.2 Steps

1

Log into the NSP Server as the root user and run the pre-install script:

```
# /extra/sw/install/bin/preInstall.bash ↵
```

The script prompts for setting the root and nspadmin user passwords. Once the script is complete, ssh login with the root user is disabled, the nspadmin user must be used.

2

Reboot the NSP Server to complete the setup and patch application.

```
# systemctl reboot ↵
```

3

The station reboots.

END OF STEPS

5 NSP installation on the NSP Server

5.1 Overview

5.1.1 Installation Options

You can install the NSP components on the NSP Server only as VMs.

5.2 To install NSP components using the VM install option

5.2.1 Purpose

Perform this procedure to install NSP components using the VM install option.

5.2.2 Steps

1

Network bridges are preconfigured for the VMs to use. The bridges are configured on all interfaces except ens15f0. Consult the RHEL 8 documentation for virtual bridge creation and configuration.

2

Deploy VMs using the appropriate NSP RHEL OS instance. Consult the *NSP Installation and Upgrade Guide* along with the RHEL 8 documentation for VM deployment.

Note: The VM disks created from the NSP RHEL OS instance must be put in */var/lib/libvirt/images.* VMs deployed on the NSP Server must be instantiated from the NSP RHEL OS instance only. The only exceptions are the vCPAA and VSR-NRC.

Install the appropriate NSP or NFM-P application in each VM as per the appropriate procedures in the *NSP Installation and Upgrade Guide* .

END OF STEPS

Part III: Management

Overview

Purpose

This part of the *NSP Server Gen11 RHEL 8.x User Guide* describes how to perform occasional maintenance actions, how to recover a failed NSP Server, and how to obtain system information and support.

Contents

6 NSP Server administration

6.1 Updating RHEL on the NSP Server

6.1.1 Description

Nokia periodically issues RHEL OS updates for the NSP Server. The *Host Environment Compatibility Reference* is reissued when a new NSP RHEL OS update is delivered on the software download site. You can subscribe to receive documentation alerts so that you are notified when a new RHEL OS update is available. See 8.1.2 “Documentation alerts” (p. 45) for information about how to subscribe to this service.

Note: Nokia does not support the download or installation of any RHEL software or packages that are not distributed as part of a Nokia software update bundle; only published RHEL updates from Nokia are supported.

6.1.2 To apply an NSP RHEL OS update

1

Log into the NSP Server. The following steps are performed as the root user.

2

Open a console window.

3

Stop all the NSP components running as guest VMs. See the *NSP System Administrator Guide* for information, as required.

1. On each guest VM, run

   ```
   # shutdown -h now ↲
   ```

2. Enter the following, on the host OS, to verify that all VMs are shut down:

   ```
   # virsh list ↲
   ```

   The returned results should not list any VMs.

4

Enter the following:

```
# mkdir -p /extra/OSUpdate ↲
```

5

Download the following compressed file for the latest NSP release to the /extra/OSUpdate directory:

NSP_RHEL_*n*_OEM_UPDATE_*yy_mm*.tar.gz

where

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

yy_mm is the issue date of the OS update

6

Enter the following:

```
# cd /extra/OSUpdate ↵
```

7

Enter the following to expand the downloaded file:

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

The update files are extracted to the following directory:

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

where

R_r is the NSP release that introduces the OS update

V.v is the RHEL version, for example, 8.8

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

8

Enter the following:

```
# cd R_r-RHELV.v-yy.mm.dd ↵
```

9

Enter the following to perform the OS update:

```
# ./yum_update.sh ↵
```

10

Once the OS update is complete, enter the following to reboot the server:

```
# systemctl reboot ↵
```

11

The station reboots.

6.2 To apply the Gen11 Service Pack for ProLiant

6.2.1 Purpose

This procedure describes how to apply the HPE Gen11 Service Pack for ProLiant (SPP) to the NSP Server.

To use this procedure, a PC is required that can connect to the NSP Server iLO interface IP address previously configured during server deployment in “Set iLO 6 IP address” (p. 24). The Administrator iLO password updated in “Change the iLO 6 administrator password” (p. 22) is required.

Note: This procedure is service impacting because the VMs will be shut down and the NSP Server will be restarted. The SPP application can take many hours; therefore, it is recommended to schedule an appropriate maintenance window.

6.2.2 Steps

1

Review the *Host Environment Compatibility Guide for NSP and CLM* to determine the supported SPP versions and note any special instructions specific to the SPP to be installed.

Download the SPP

2

Log into the PC that will be used to apply the SPP.

3

Connect to the HPE support website and download the Gen11 Service Pack for ProLiant, identified in Step 1, to a local directory on the PC that will be used to connect to the NSP Server iLO interface. Also obtain the checksum file as it is used to verify the integrity of the .iso file.

Verify the checksum

4

Press the Window Start button on the taskbar and enter the following:

cmd ↵

A Windows command prompt window opens.

5

Enter the following to navigate to the folder that contains the downloaded files:

Note: The C:\> that precedes a command in subsequent steps represents the Windows command prompt, and is not to be included in a typed command.

C:\> **cd *path*** ↵

where *path* is the absolute file path of the downloaded folder

6

Enter the following:

C:\> **type *filename*** ↵

where *filename* is the checksum file that was downloaded with the SPP file

The expected SHA-256 checksum of the SPP file is displayed.

7

Enter the following:

```
C:\> certutil -hashfile filename sha256 ↵
```

where *filename* is the SPP .iso file

Verify that the checksum in the output matches the checksum displayed in Step 6. If the checksum does not match, download a new copy of the SPP file and repeat Step 4 to Step 7.

Shut down the VMs

8

Log into the NSP Server.

9

As the root user, stop all NSP components running as guest VMs. See the *NSP System Administrator Guide* for information, as required.

On each guest VM, run

```
# shutdown -h now ↵
```

Enter the following on the host OS to verify that all VMs are shut down:

```
# virsh list ↵
```

The returned results should not list any VMs.

Open the iLO web interface

10

Open a web browser on the PC.

11

Type the IP address assigned to the NSP Server iLO interface into the address bar and press Enter.

12

If a security warning is displayed, acknowledge the warning and proceed to the web page.

Note: The security warning may differ, depending on the browser. For example, in Google Chrome, you must click **Advanced**, and then click “Proceed to <*iLO IP address*> (unsafe)”.

The web interface shown in Figure 6-1, “iLO6 web interface” (p. 37) is displayed.

Figure 6-1 iLO6 web interface

Open the iLO remote console

13

Log in using the Administrator iLO username and password that was updated up in “Change the iLO 6 administrator password” (p. 22).

14

Choose **Remote Console & Media** from the menu at the left side of the page.

15

Scroll down to the HTML5 Integrated Remote Console section and click **New Window**.

Perform the SPP installation

16

Click on **Virtual Media** at the top left of the window.

17

Select **CD/DVD->Local *.iso file**. The Choose Disk Image File form opens.

18

Use the form to choose the Gen11 Service Pack for ProLiant .iso file downloaded in Step 2 and click Open.

The virtual disk image is attached to the server.

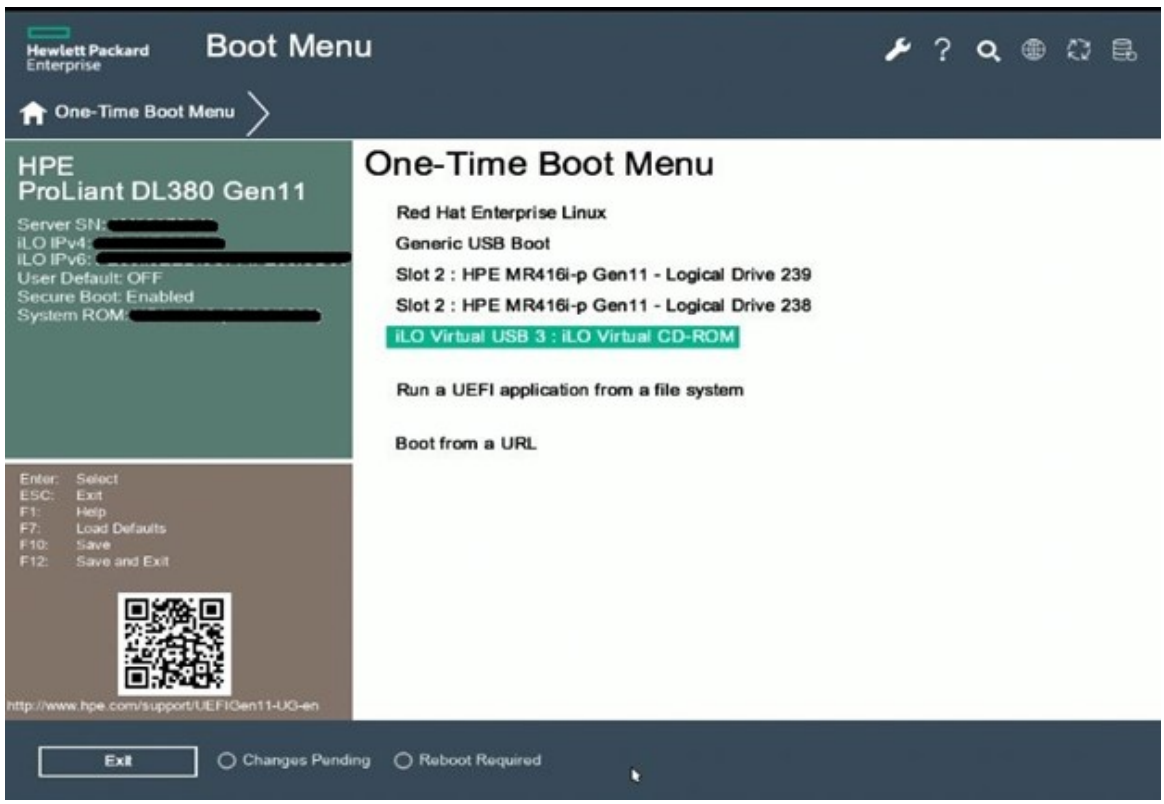
Navigate to Power & Thermal and select **Reset**.

19

When the POST screen appears, showing the different options at the bottom of the screen, press F11 (Boot Menu) to select the appropriate boot device. The One-Time Boot Menu screen opens, as shown in Figure 6-2, “Boot Menu” (p. 37).

Select **iLO Virtual USB 2 : iLO Virtual CD-ROM**.

Figure 6-2 Boot Menu



20

The server boots from the virtual disk.

Select **Interactive Firmware Update Version** *R.r*

where *R.r* is the SPP version

21

Select the preferred language and accept the End User License Agreement (EULA).

Click **Next**.

22

Select **Firmware Update**.

A form will open which requires the user to enter the iLO administrator username and password.

Select **OK**.

23

The Localhost Guided Update begins.

- Install Prerequisite components if not already installed.
  Note: The following warning is displayed.
  Warning: During the inventory process, some prerequisite components are required to be installed to list the FW versions for all the devices correctly. The installation of prerequisite components (like network interface option driver) may result in a network or system reset during the process, causing system outage.
- Baseline or Install Set
- Assign different baseline
  Here, select the baseline for the current SPP.

Click **OK**.

24

The next screen of the Localhost Guided Update opens.

In Step 1, Inventory, click **Next**.

In Step 2, Review, below Selected Components, choose **Select all**, then select **Ignore Warnings** and click **Deploy**.

If the Remote Console closes during the SPP update, it will need to be re-opened to complete the update.

25

Once the firmware update is complete, click **Reboot** and confirm the reboot.

If the VMs are not configured to auto-restart, they will need to be started once the NSP Server has full rebooted.

END OF STEPS

6.3 To install the Agentless Management Service on the NSP Server

6.3.1 Purpose

The HPE Agentless Management Service (AMS) can be installed on the NSP Server to allow server management and health monitoring through the iLO interface. Additional details on AMS and its capabilities can be obtained from HPE.

The AMS package is included with the HPE Gen11 SPP and needs to be downloaded from HPE for this procedure. The *Host Environment and Compatibility Guide for NSP and CLM* must be consulted to determine supported SPP versions.

6.3.2 Steps

1

Review the *Host Environment Compatibility Guide for NSP and CLM* to determine the supported SPP versions.

2

Connect to the HPE support website and download the Gen11 Service Pack for ProLiant, identified in Step 1. Also obtain the SPP checksum file to verify the integrity of the .iso file.

3

Log into the NSP Server. The following steps are performed as the root user.

4

Transfer the SPP .iso and checksum files to the NSP Server and verify the checksum.

1. Create a directory for the SPP file:

   # **mkdir /extra/SPP** ↵

2. Transfer the SPP ISO file and SPP checksum file downloaded in Step 2 into the /extra/SPP directory that was created in 1.

3. Enter the following to validate the checksum of the SPP file:

   # **sha256sum /extra/SPP/<SPP ISO FILE>** ↵

   where

   <SPP ISO FILE> is the file downloaded in Step 2

4. Compare the value obtained from 3 to the value in the checksum file downloaded with the SPP file. If the checksum does not match, download a new copy of the SPP file and repeat the checksum check.

5

Mount the SPP iso file to install the AMS package.

1. Enter the following:

```
# mount -o loop /extra/SPP/<SPP ISO FILE> /mnt ↵
```

where

<SPP ISO FILE> is the file downloaded in Step 2

2. Install the AMS package:

```
# yum install /mnt/packages/amsd-*.rhel8.x86_64.rpm ↵
```

6

Unmount the SPP:

```
# unmount /mnt ↵
```

END OF STEPS

7 Disaster recovery

7.1 Recovering a failed NSP Server

7.1.1 Restore NSP Server

Contact Nokia Support if the re-installation of the NSP Server host OS is required.

For component level disaster recovery option see *NSP Installation and Upgrade Guide* and *NFM-P Administrator Guide*.

8 Troubleshooting and support

8.1 Obtaining support

8.1.1 Contacting support

Before you contact technical support, ensure that you have the required information, for example, the NSP Server software release, a problem description, and any system logs that may help to diagnose the problem.

8.1.2 Documentation alerts

You can subscribe to receive NSP documentation alerts for the following from the Documentation Alerts Subscription page of the Nokia Support portal:

- Manuals and Guides
- Release Information
- Technical Notes

8.1.3 Product alerts

You can subscribe to receive the following types of NSP alerts from the Alerts Subscription page of the Nokia Support portal:

- Maintenance
- Security
- LifeCycle
- Informational
- Product Change

Part IV: Appendices

Overview

Purpose

This part of the *NSP Server Gen11 RHEL 8.x User Guide* provides platform reference information in separate appendices.

Contents

A NSP Server RHEL OS compliance with CIS benchmarks

A.1 RHEL CIS benchmarks and NSP Server compliance

A.1.1 Purpose

This appendix describes only the NSP Server host OS compliance with the Center for Internet Security, or CIS, security benchmarks for the RHEL OS.

Any VMs created on the NSP Server are created from the Nokia provided qcows. CIS compliance of the RHEL8 qcows can be found in the NSP Security Hardening Guide.

A.1.2 RHEL 8 CIS compliance

Table A-1, “RHEL 8 CIS benchmarks and NSP Server compliance” (p. 49) lists the CIS v1.0.1 benchmarks for RHEL 8 and the OS compliance of the NSP Server.

Compliance profiles

The following compliance profiles are referenced:

- Level 1—Server, or L1:

  Intent of recommendations is to:
  - be practical and prudent
  - provide clear security benefit
  - not inhibit utility of technology beyond acceptable degree
- Level 2—Server, or L2:

  Extension of L1 profile; recommendations have one or more of the following characteristics:
  - intended for environments or use cases in which security is crucial
  - considered intensive defense measure
  - may inhibit technology utility or performance

Note: It is strongly recommended that you maintain a log of all configuration changes that you make regarding CIS compliance. Such a log may be of great value during system troubleshooting. Each log entry must be dated and include the configuration details.

Table A-1 RHEL 8 CIS benchmarks and NSP Server compliance

Section	Recommendation (Scored, unless indicated otherwise)	Profile level	Compliance status	Notes
1	Initial Setup			
1.1	Filesystem Configuration			

Table A-1 RHEL 8 CIS benchmarks and NSP Server compliance (continued)

Section	Recommendation (Scored, unless indicated otherwise)	Profile level	Compliance status	Notes
1.1.1	Disable unused filesystems			
1.1.1.1	Ensure mounting of cramfs filesystems is disabled (Automated)	L1	Supported (default)	
1.1.1.2	Ensure mounting of vFAT filesystems is limited (Manual)	L2	Supported (default)	Since UEFI is used, vFAT is required for /boot/efi.
1.1.1.3	Ensure mounting of squashfs filesystems is disabled (Automated)	L1	Supported (default)	
1.1.1.4	Ensure mounting of udf filesystems is disabled (Automated)	L1	Supported (default)	
1.1.2	Ensure /tmp is configured (Automated)	L1	Supported (default)	
1.1.3	Ensure nodev option set on /tmp partition (Automated)	L1	Supported (default)	
1.1.4	Ensure nosuid option set on /tmp partition (Automated)	L1	Supported (default)	
1.1.5	Ensure noexec option set on /tmp partition (Automated)	L1	Supported (default)	
1.1.6	Ensure separate partition exists for /var (Automated)	L2	Supported (default)	
1.1.7	Ensure separate partition exists for /var/tmp (Automated)	L2	Supported (default)	
1.1.8	Ensure nodev option set on /var/tmp partition (Automated)	L1	Supported (default)	
1.1.9	Ensure nosuid option set on /var/tmp partition (Automated)	L1	Supported (default)	
1.1.10	Ensure noexec option set on /var/tmp partition (Automated)	L1	Supported (default)	
1.1.11	Ensure separate partition exists for /var/log (Automated)	L2	Supported (default)	
1.1.12	Ensure separate partition exists for /var/log/audit (Automated)	L2	Supported (default)	
1.1.13	Ensure separate partition exists for /home (Automated)	L2	Supported (default)	

Table A-1 RHEL 8 CIS benchmarks and NSP Server compliance (continued)

Section	Recommendation (Scored, unless indicated otherwise)	Profile level	Compliance status	Notes
1.1.14	Ensure nodev option set on /home partition (Automated)	L1	Supported (default)	
1.1.15	Ensure nodev option set on /dev/shm partition (Automated)	L1	Supported (default)	
1.1.16	Ensure nosuid option set on /dev/shm partition (Automated)	L1	Supported (default)	
1.1.17	Ensure noexec option set on /dev/shm partition (Automated)	L1	Supported (default)	
1.1.18	Ensure nodev option set on removable media partitions (Manual)	L1	Supported (default)	
1.1.19	Ensure nosuid option set on removable media partitions (Manual)	L1	Supported (default)	
1.1.20	Ensure noexec option set on removable media partitions (Manual)	L1	Supported (default)	
1.1.21	Ensure sticky bit is set on all world-writable directories (Automated)	L1	Supported (default)	
1.1.22	Disable Automounting (Automated)	L1	Supported (default)	
1.1.23	Disable USB Storage (Automated)	L1	Supported (default)	
1.2	Configure Software Updates			
1.2.1	Ensure Red Hat Subscription Manager connection is configured (Manual)	L1	Not supported	Not supported. RHEL package updates are provided via the NSP RHEL update patch bundle only.
1.2.2	Disable the rhnsd Daemon (Manual)	L1	Supported (default)	
1.2.3	Ensure GPG keys are configured (Manual)	L1	Supported (post-install)	
1.2.4	Ensure gpgcheck is globally activated (Automated)	L1	Supported (default)	

Table A-1 RHEL 8 CIS benchmarks and NSP Server compliance (continued)

Section	Recommendation (Scored, unless indicated otherwise)	Profile level	Compliance status	Notes
1.2.5	Ensure package manager repositories are configured (Manual)	L1	Not supported	Not supported. RHEL package updates are provided via the NSP RHEL update patch bundle only.
1.3	Configure sudo			
1.3.1	Ensure sudo is installed (Automated)	L1	Supported (default)	
1.3.2	Ensure sudo commands use pty (Automated)	L1	Supported (default)	
1.3.3	Ensure sudo log file exists (Automated)	L1	Supported (default)	
1.4	Filesystem Integrity Checking			
1.4.1	Ensure AIDE is installed (Automated)	L1	Not supported	
1.4.2	Ensure filesystem integrity is regularly checked (Automated)	L1	Not supported	May impact service. On redundant NSP setups, a filesystem check should be run periodically when that server is not the active server.
1.5	Secure Boot Settings			
1.5.1	Ensure permissions on bootloader config are configured (Automated)	L1	Supported (default)	
1.5.2	Ensure bootloader password is set (Automated)	L1	Supported (default)	
1.5.3	Ensure authentication required for single user mode (Automated)	L1	Supported (default)	
1.6	Additional Process Hardening			
1.6.1	Ensure core dumps are restricted (Automated)	L1	Supported (default)	

Table A-1 RHEL 8 CIS benchmarks and NSP Server compliance (continued)

Section	Recommendation (Scored, unless indicated otherwise)	Profile level	Compliance status	Notes
1.6.2	Ensure address space layout randomization (ASLR) is enabled (Automated)	L1	Supported (default)	
1.7	Mandatory Access Control			
1.7.1	Configure SELinux			
1.7.1.1	Ensure SELinux is installed (Automated)	L2	Supported (default)	
1.7.1.2	Ensure SELinux is not disabled in bootloader configuration (Automated)	L2	Supported (default)	
1.7.1.3	Ensure SELinux policy is configured (Automated)	L2	Supported (default)	
1.7.1.4	Ensure the SELinux state is enforcing (Automated)	L2	Supported (default)	
1.7.1.5	Ensure no unconfined services exist (Automated)	L2	Supported (default)	
1.7.1.6	Ensure SETroubleshoot is not installed (Automated)	L2	Supported (default)	
1.7.1.7	Ensure the MCS Translation Service (mcstrans) is not installed (Automated)	L2	Supported (default)	
1.8	Warning Banners			
1.8.1	Command Line Warning Banners			
1.8.1.1	Ensure message of the day is configured properly (Automated)	L1	Supported (default)	
1.8.1.2	Ensure local login warning banner is configured properly (Automated)	L1	Supported (default)	
1.8.1.3	Ensure remote login warning banner is configured properly (Automated)	L1	Supported (default)	
1.8.1.4	Ensure permissions on /etc/motd are configured (Automated)	L1	Supported (default)	
1.8.1.5	Ensure permissions on /etc/issue are configured (Automated)	L1	Supported (default)	
1.8.1.6	Ensure permissions on /etc/issue.net are configured (Automated)	L1	Supported (default)	

Table A-1 RHEL 8 CIS benchmarks and NSP Server compliance (continued)

Section	Recommendation (Scored, unless indicated otherwise)	Profile level	Compliance status	Notes
1.8.2	Ensure GDM login banner is configured (Automated)	L1	Supported (default)	
1.9	Ensure updates, patches, and additional security software are installed (Manual)	L1	Not supported	RHEL package updates are provided via the NSP RHEL update patch bundle only.
1.10	Ensure system-wide crypto policy is not legacy (Automated)	L1	Supported (default)	
1.11	Ensure system-wide crypto policy is FUTURE or FIPS (Automated)	L2	Supported (default)	
2	Services			
2.1	inetd Services			
2.1.1	Ensure xinetd is not installed (Automated)	L1	Supported (default)	
2.2	Special Purpose Services			
2.2.1	Time Synchronization			
2.2.1.1	Ensure time synchronization is in use (Manual)	L1	Supported (post-install)	Supported post-installation but not configured by default since configuration requires on-site network information.
2.2.1.2	Ensure chrony is configured (Automated)	L1	Supported (post-install)	Supported post-installation but not configured by default since configuration requires on-site network information.
2.2.2	Ensure X Window System is not installed (Automated)	L1	Not supported	
2.2.3	Ensure rsync service is not enabled (Automated)	L1	Supported (default)	

Table A-1 RHEL 8 CIS benchmarks and NSP Server compliance (continued)

Section	Recommendation (Scored, unless indicated otherwise)	Profile level	Compliance status	Notes
2.2.4	Ensure Avahi Server is not enabled (Automated)	L1	Supported (default)	
2.2.5	Ensure SNMP Server is not enabled (Automated)	L1	Supported (default)	
2.2.6	Ensure HTTP Proxy Server is not enabled (Automated)	L1	Supported (default)	
2.2.7	Ensure Samba is not enabled (Automated)	L1	Supported (default)	
2.2.8	Ensure IMAP and POP3 server is not enabled (Automated)	L1	Supported (default)	
2.2.9	Ensure HTTP Server is not enabled (Automated)	L1	Supported (default)	
2.2.10	Ensure FTP Server is not enabled (Automated)	L1	Supported (default)	
2.2.11	Ensure DNS Server is not enabled (Automated)	L1	Supported (default)	
2.2.12	Ensure NFS is not enabled (Automated)	L1	Supported (default)	
2.2.13	Ensure RPC is not enabled (Automated)	L1	Supported (default)	
2.2.14	Ensure LDAP server is not enabled (Automated)	L1	Supported (default)	
2.2.15	Ensure DHCP server is not enabled (Automated)	L1	Supported (default)	
2.2.16	Ensure CUPS is not enabled (Automated)	L1	Supported (default)	
2.2.17	Ensure NIS Server is not enabled (Automated)	L1	Supported (default)	
2.2.18	Ensure mail transfer agent is configured for local-only mode (Automated)	L1	Supported (default)	
2.3	Service Clients			
2.3.1	Ensure NIS Client is not installed (Automated)	L1	Supported (default)	

Table A-1 RHEL 8 CIS benchmarks and NSP Server compliance (continued)

Section	Recommendation (Scored, unless indicated otherwise)	Profile level	Compliance status	Notes
2.3.2	Ensure telnet client is not installed (Automated)	L1	Supported (default)	
2.3.3	Ensure LDAP client is not installed (Automated)	L1	Supported (default)	
3	Network Configuration			
3.1	Network Parameters (Host Only)			
3.1.1	Ensure IP forwarding is disabled (Automated)	L1	Not supported	libvirtd requires IPv4 forwarding
3.1.2	Ensure packet redirect sending is disabled (Automated)	L1	Supported (default)	
3.2	Network Parameters (Host and Router)			
3.2.1	Ensure source routed packets are not accepted (Automated)	L1	Supported (default)	
3.2.2	Ensure ICMP redirects are not accepted (Automated)	L1	Supported (default)	
3.2.3	Ensure secure ICMP redirects are not accepted (Automated)	L1	Supported (default)	
3.2.4	Ensure suspicious packets are logged (Automated)	L1	Supported (default)	
3.2.5	Ensure broadcast ICMP requests are ignored (Automated)	L1	Supported (default)	
3.2.6	Ensure bogus ICMP responses are ignored (Automated)	L1	Supported (default)	
3.2.7	Ensure Reverse Path Filtering is enabled (Automated)	L1	Supported (default)	
3.2.8	Ensure TCP SYN Cookies is enabled (Automated)	L1	Supported (default)	
3.2.9	Ensure IPv6 router advertisements are not accepted (Automated)	L1	Supported (default)	
3.3	Uncommon Network Protocols			
3.3.1	Ensure DCCP is disabled (Automated)	L2	Supported (default)	

Table A-1 RHEL 8 CIS benchmarks and NSP Server compliance (continued)

Section	Recommendation (Scored, unless indicated otherwise)	Profile level	Compliance status	Notes
3.3.2	Ensure SCTP is disabled (Automated)	L2	Supported (default)	
3.3.3	Ensure RDS is disabled (Automated)	L2	Supported (default)	
3.3.4	Ensure TIPC is disabled (Automated)	L2	Supported (default)	
3.4	Firewall Configuration			
3.4.1	Ensure Firewall software is installed			
3.4.1.1	Ensure a Firewall package is installed (Automated)	L1	Supported (default)	firewalld is installed and supported
3.4.2	Configure firewalld			
3.4.2.1	Ensure firewalld service is enabled and running (Automated)	L1	Supported (default)	
3.4.2.2	Ensure iptables service is not enabled with firewalld (Automated)	L1	Supported (default)	
3.4.2.3	Ensure nftables is not enabled with firewalld (Automated)	L1	Supported (default)	
3.4.2.4	Ensure firewalld default zone is set (Automated)	L1	Supported (post-install)	Supported post-installation but not configured by default since configuration requires on-site network information.
3.4.2.5	Ensure network interfaces are assigned to appropriate zone (Manual)	L1	Supported (post-install)	Supported post-installation but not configured by default since configuration requires on-site network information.

Table A-1 RHEL 8 CIS benchmarks and NSP Server compliance (continued)

Section	Recommendation (Scored, unless indicated otherwise)	Profile level	Compliance status	Notes
3.4.2.6	Ensure firewalld drops unnecessary services and ports (Manual)	L1	Supported (post-install)	Supported post-installation but not configured by default since configuration requires on-site network information.
3.4.3	Configure nftables			
3.4.3.1	Ensure iptables are flushed with nftables (Manual)	L1	Not supported	Only firewalld is supported
3.4.3.2	Ensure an nftables table exists (Automated)	L1	Not supported	Only firewalld is supported
3.4.3.3	Ensure nftables base chains exist (Automated)	L1	Not supported	Only firewalld is supported
3.4.3.4	Ensure nftables loopback traffic is configured (Automated)	L1	Not supported	Only firewalld is supported
3.4.3.5	Ensure nftables outbound and established connections are configured (Manual)	L1	Not supported	Only firewalld is supported
3.4.3.6	Ensure nftables default deny firewall policy (Automated)	L1	Not supported	Only firewalld is supported
3.4.3.7	Ensure nftables service is enabled (Automated)	L1	Not supported	Only firewalld is supported
3.4.3.8	Ensure nftables rules are permanent (Automated)	L1	Not supported	Only firewalld is supported
3.4.4	Configure iptables			
3.4.4.1	Configure IPv4 iptables			
3.4.4.1.1	Ensure iptables default deny firewall policy (Automated)	L1	Not supported	Only firewalld is supported
3.4.4.1.2	Ensure iptables loopback traffic is configured (Automated)	L1	Not supported	Only firewalld is supported
3.4.4.1.3	Ensure iptables outbound and established connections are configured (Manual)	L1	Not supported	Only firewalld is supported

Table A-1 RHEL 8 CIS benchmarks and NSP Server compliance (continued)

Section	Recommendation (Scored, unless indicated otherwise)	Profile level	Compliance status	Notes
3.4.4.1.4	Ensure iptables firewall rules exist for all open ports (Automated)	L1	Not supported	Only firewalld is supported
3.4.4.1.5	Ensure iptables is enabled and active (Automated)	L1	Not supported	Only firewalld is supported
3.4.4.2	Configure IPv6 ip6tables			
3.4.4.2.1	Ensure ip6tables default deny firewall policy (Automated)	L1	Not supported	Only firewalld is supported
3.4.4.2.2	Ensure ip6tables loopback traffic is configured (Automated)	L1	Not supported	Only firewalld is supported
3.4.4.2.3	Ensure ip6tables outbound and established connections are configured (Manual)	L1	Not supported	Only firewalld is supported
3.4.4.2.4	Ensure ip6tables firewall rules exist for all open ports (Automated)	L1	Not supported	Only firewalld is supported
3.4.4.2.5	Ensure ip6tables is enabled and active (Automated)	L1	Not supported	Only firewalld is supported
3.5	Ensure wireless interfaces are disabled (Automated)	L1		
3.6	Disable IPv6 (Manual)	L2	Supported (post-install)	Supported post-installation but not configured by default
4	Logging and Auditing			
4.1	Configure System Accounting (auditd)			
4.1.1	Ensure auditing is enabled			
4.1.1.1	Ensure auditd is installed (Automated)	L2	Supported (default)	
4.1.1.2	Ensure auditd service is enabled (Automated)	L2	Supported (default)	
4.1.1.3	Ensure auditing for processes that start prior to auditd is enabled (Automated)	L2	Supported (default)	
4.1.1.4	Ensure audit_backlog_limit is sufficient (Automated)	L2	Supported (default)	
4.1.2	Configure Data Retention			

Table A-1 RHEL 8 CIS benchmarks and NSP Server compliance (continued)

Section	Recommendation (Scored, unless indicated otherwise)	Profile level	Compliance status	Notes
4.1.2.1	Ensure audit log storage size is configured (Automated)	L2	Supported (default)	
4.1.2.2	Ensure audit logs are not automatically deleted (Automated)	L2	Supported (default)	
4.1.2.3	Ensure system is disabled when audit logs are full (Automated)	L2	Not supported	
4.1.3	Ensure changes to system administration scope (sudoers) is collected (Automated)	L2	Supported (default)	
4.1.4	Ensure login and logout events are collected (Automated)	L2	Supported (default)	
4.1.5	Ensure session initiation information is collected (Automated)	L2	Supported (default)	
4.1.6	Ensure events that modify date and time information are collected (Automated)	L2	Supported (default)	
4.1.7	Ensure events that modify the system's Mandatory Access Controls are collected (Automated)	L2	Supported (default)	
4.1.8	Ensure events that modify the system's network environment are collected (Automated)	L2	Supported (default)	
4.1.9	Ensure discretionary access control permission modification events are collected (Automated)	L2	Supported (default)	
4.1.10	Ensure unsuccessful unauthorized file access attempts are collected (Automated)	L2	Supported (default)	
4.1.11	Ensure events that modify user/group information are collected (Automated)	L2	Supported (default)	
4.1.12	Ensure successful file system mounts are collected (Automated)	L2	Supported (default)	
4.1.13	Ensure use of privileged commands is collected (Automated)	L2	Supported (default)	
4.1.14	Ensure file deletion events by users are collected (Automated)	L2	Supported (default)	

Table A-1 RHEL 8 CIS benchmarks and NSP Server compliance (continued)

Section	Recommendation (Scored, unless indicated otherwise)	Profile level	Compliance status	Notes
4.1.15	Ensure kernel module loading and unloading is collected (Automated)	L2	Supported (default)	
4.1.16	Ensure system administrator actions (sudolog) are collected (Automated)	L2	Supported (default)	
4.1.17	Ensure the audit configuration is immutable (Automated)	L2	Supported (default)	
4.2	Configure Logging			
4.2.1	Configure rsyslog			
4.2.1.1	Ensure rsyslog is installed (Automated)	L1	Supported (default)	
4.2.1.2	Ensure rsyslog Service is enabled (Automated)	L1	Supported (default)	
4.2.1.3	Ensure rsyslog default file permissions configured (Automated)	L1	Supported (default)	
4.2.1.4	Ensure logging is configured (Manual)	L1	Supported (post-install)	Supported post-installation but not configured by default since configuration requires on-site network information.
4.2.1.5	Ensure rsyslog is configured to send logs to a remote log host (Automated)	L1	Supported (post-install)	Supported post-installation but not configured by default since configuration requires on-site network information.
4.2.1.6	Ensure remote rsyslog messages are only accepted on designated log hosts. (Manual)	L1	Supported (default)	
4.2.2	Configure journald			
4.2.2.1	Ensure journald is configured to send logs to rsyslog (Automated)	L1	Supported (default)	

Table A-1 RHEL 8 CIS benchmarks and NSP Server compliance (continued)

Section	Recommendation (Scored, unless indicated otherwise)	Profile level	Compliance status	Notes
4.2.2.2	Ensure journald is configured to compress large log files (Automated)	L1	Supported (default)	
4.2.2.3	Ensure journald is configured to write logfiles to persistent disk (Automated)	L1	Supported (default)	
4.2.3	Ensure permissions on all logfiles are configured (Automated)	L1	Not supported	
4.3	Ensure logrotate is configured (Manual)	L1	Supported (post-install)	Supported post-installation but not configured by default
5	Access, Authentication and Authorization			
5.1	Configure cron			
5.1.1	Ensure cron daemon is enabled (Automated)	L1	Supported (default)	
5.1.2	Ensure permissions on /etc/crontab are configured (Automated)	L1	Supported (default)	
5.1.3	Ensure permissions on /etc/cron.hourly are configured (Automated)	L1	Supported (default)	
5.1.4	Ensure permissions on /etc/cron.daily are configured (Automated)	L1	Supported (default)	
5.1.5	Ensure permissions on /etc/cron.weekly are configured (Automated)	L1	Supported (default)	
5.1.6	Ensure permissions on /etc/cron.monthly are configured (Automated)	L1	Supported (default)	
5.1.7	Ensure permissions on /etc/cron.d are configured (Automated)	L1	Supported (default)	
5.1.8	Ensure at/cron is restricted to authorized users (Automated)	L1	Supported (default)	
5.2	SSH Server Configuration			
5.2.1	Ensure permissions on /etc/ssh/sshd_config are configured (Automated)	L1	Supported (default)	
5.2.2	Ensure SSH access is limited (Automated)	L1	Supported (post-install)	Supported post-installation

Table A-1 RHEL 8 CIS benchmarks and NSP Server compliance (continued)

Section	Recommendation (Scored, unless indicated otherwise)	Profile level	Compliance status	Notes
5.2.3	Ensure permissions on SSH private host key files are configured (Automated)	L1	Supported (default)	
5.2.4	Ensure permissions on SSH public host key files are configured (Automated)	L1	Supported (default)	
5.2.5	Ensure SSH LogLevel is appropriate (Automated)	L1	Supported (default)	
5.2.6	Ensure SSH X11 forwarding is disabled (Automated)	L1	Supported (default)	Can be enabled post-installation if SSH X11 forwarding is required.
5.2.7	Ensure SSH MaxAuthTries is set to 4 or less (Automated)	L1	Supported (default)	
5.2.8	Ensure SSH IgnoreRhosts is enabled (Automated)	L1	Supported (default)	
5.2.9	Ensure SSH HostbasedAuthentication is disabled (Automated)	L1	Supported (default)	
5.2.10	Ensure SSH root login is disabled (Automated)	L1	Supported (default)	
5.2.11	Ensure SSH PermitEmptyPasswords is disabled (Automated)	L1	Supported (default)	
5.2.12	Ensure SSH PermitUserEnvironment is disabled (Automated)	L1	Supported (default)	
5.2.13	Ensure SSH Idle Timeout Interval is configured (Automated)	L1	Supported (default)	
5.2.14	Ensure SSH LoginGraceTime is set to one minute or less (Automated)	L1	Supported (default)	
5.2.15	Ensure SSH warning banner is configured (Automated)	L1	Supported (default)	
5.2.16	Ensure SSH PAM is enabled (Automated)	L1	Supported (default)	
5.2.17	Ensure SSH AllowTcpForwarding is disabled (Automated)	L2	Supported (default)	
5.2.18	Ensure SSH MaxStartups is configured (Automated)	L1	Supported (default)	

Table A-1 RHEL 8 CIS benchmarks and NSP Server compliance (continued)

Section	Recommendation (Scored, unless indicated otherwise)	Profile level	Compliance status	Notes
5.2.19	Ensure SSH MaxSessions is set to 4 or less (Automated)	L1	Supported (default)	
5.2.20	Ensure system-wide crypto policy is not over-ridden (Automated)	L1	Supported (default)	
5.3	Configure authselect			
5.3.1	Create custom authselect profile (Automated)	L1	Supported (post-install)	Supported post-installation but not configured by default
5.3.2	Select authselect profile (Automated)	L1	Supported (post-install)	Supported post-installation but not configured by default
5.3.3	Ensure authselect includes with-faillock (Automated)	L1	Supported (post-install)	Supported post-installation but not configured by default
5.4	Configure PAM			
5.4.1	Ensure password creation requirements are configured (Automated)	L1	Supported (default)	
5.4.2	Ensure lockout for failed password attempts is configured (Automated)	L1	Supported (default)	
5.4.3	Ensure password reuse is limited (Automated)	L1	Supported (default)	
5.4.4	Ensure password hashing algorithm is SHA-512 (Automated)	L1	Supported (default)	
5.5	User Accounts and Environment			
5.5.1	Set Shadow Password Suite Parameters			
5.5.1.1	Ensure password expiration is 365 days or less (Automated)	L1	Supported (post-install)	
5.5.1.2	Ensure minimum days between password changes is 7 or more (Automated)	L1	Supported (post-install)	
5.5.1.3	Ensure password expiration warning days is 7 or more (Automated)	L1	Supported (default)	

Table A-1 RHEL 8 CIS benchmarks and NSP Server compliance (continued)

Section	Recommendation (Scored, unless indicated otherwise)	Profile level	Compliance status	Notes
5.5.1.4	Ensure inactive password lock is 30 days or less (Automated)	L1	Supported (default)	
5.5.1.5	Ensure all users last password change date is in the past (Automated)	L1	Supported (default)	
5.5.2	Ensure system accounts are secured (Automated)	L1	Supported (default)	
5.5.3	Ensure default user shell timeout is 900 seconds or less (Automated)	L1	Supported (default)	
5.5.4	Ensure default group for the root account is GID 0 (Automated)	L1	Supported (default)	
5.5.5	Ensure default user umask is 027 or more restrictive (Automated)	L1	Supported (default)	
5.6	Ensure root login is restricted to system console (Manual)	L1	Supported (post-install)	Supported post-installation but not configured by default
5.7	Ensure access to the su command is restricted (Automated)	L1	Supported (default)	
6	System Maintenance			
6.1	System File Permissions			
6.1.1	Audit system file permissions (Manual)	L2	Not applicable	Manual audit recommendation only. Transferred to customer for review.
6.1.2	Ensure permissions on /etc/passwd are configured (Automated)	L1	Supported (default)	
6.1.3	Ensure permissions on /etc/passwd- are configured (Automated)	L1	Supported (default)	
6.1.4	Ensure permissions on /etc/shadow are configured (Automated)	L1	Supported (default)	
6.1.5	Ensure permissions on /etc/shadow- are configured (Automated)	L1	Supported (default)	
6.1.6	Ensure permissions on /etc/gshadow are configured (Automated)	L1	Supported (default)	

Table A-1 RHEL 8 CIS benchmarks and NSP Server compliance (continued)

Section	Recommendation (Scored, unless indicated otherwise)	Profile level	Compliance status	Notes
6.1.7	Ensure permissions on /etc/gshadow- are configured (Automated)	L1	Supported (default)	
6.1.8	Ensure permissions on /etc/group are configured (Automated)	L1	Supported (default)	
6.1.9	Ensure permissions on /etc/group- are configured (Automated)	L1	Supported (default)	
6.1.10	Ensure no world writable files exist (Automated)	L1	Supported (default)	
6.1.11	Ensure no unowned files or directories exist (Automated)	L1	Supported (default)	
6.1.12	Ensure no ungrouped files or directories exist (Automated)	L1	Supported (default)	
6.1.13	Audit SUID executables (Manual)	L1	Not applicable	Manual audit recommendation only. Transferred to customer for review.
6.1.14	Audit SGID executables (Manual)	L1	Not applicable	Manual audit recommendation only. Transferred to customer for review.
6.2	User and Group Settings			
6.2.1	Ensure password fields are not empty (Automated)	L1	Supported (default)	
6.2.2	Ensure no legacy “+” entries exist in /etc/passwd Automated)	L1	Supported (default)	
6.2.3	Ensure root PATH Integrity (Automated)	L1	Supported (default)	
6.2.4	Ensure no legacy “+” entries exist in /etc/shadow (Automated)	L1	Supported (default)	
6.2.5	Ensure no legacy “+” entries exist in /etc/group (Automated)	L1	Supported (default)	
6.2.6	Ensure root is the only UID 0 account (Automated)	L1	Supported (default)	

Table A-1 RHEL 8 CIS benchmarks and NSP Server compliance (continued)

Section	Recommendation (Scored, unless indicated otherwise)	Profile level	Compliance status	Notes
6.2.7	Ensure users' home directories permissions are 750 or more restrictive (Automated)	L1	Supported (default)	
6.2.8	Ensure users own their home directories (Automated)	L1	Supported (default)	
6.2.9	Ensure users' dot files are not group or world writable (Automated)	L1	Supported (default)	
6.2.10	Ensure no users have .forward files (Automated)	L1	Supported (default)	
6.2.11	Ensure no users have .netrc files (Automated)	L1	Supported (default)	
6.2.12	Ensure users' .netrc Files are not group or world accessible (Automated)	L1	Supported (default)	
6.2.13	Ensure no users have .rhosts files (Automated)	L1	Supported (default)	
6.2.14	Ensure all groups in /etc/passwd exist in /etc/group (Automated)	L1	Supported (default)	
6.2.15	Ensure no duplicate UIDs exist (Automated)	L1	Supported (default)	
6.2.16	Ensure no duplicate GIDs exist (Automated)	L1	Supported (default)	
6.2.17	Ensure no duplicate user names exist (Automated)	L1	Supported (default)	
6.2.18	Ensure no duplicate group names exist (Automated)	L1	Supported (default)	
6.2.19	Ensure shadow group is empty (Automated)	L1	Supported (default)	
6.2.20	Ensure all users' home directories exist (Automated)	L1	Supported (default)	