System Setup and Software Installation Guide for Cisco NCS 1004

Cisco Network Convergence System 1004
Updated July 17, 2026

Full Cisco Trademarks with Software License

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Topics included

1 Bring-up Cisco NCS 1004

Topics:

Provides instructions for initializing the Cisco NCS 1004 system. It enables users to perform system boot-up using various methods, establish management connectivity, and implement essential security and synchronization settings for optimal operation.

After installing the hardware, boot the Cisco NCS 1004 system. You can connect to the XR console port and power on the system. NCS 1004 completes the boot process using the pre-installed operating system (OS) image. If no image is available, NCS 1004 can be booted using the iPXE boot, an external bootable USB drive, or Golden ISO.

After booting, create the root username and password, and then use it to log on to the XR console. From the XR console, access the System Admin console to configure system administration settings.

> **Note**
>
> The output of the examples in the procedures is not from the latest software release. The output will change for any explicit references to the current release.

Options to boot NCS 1004

This topic explains the boot options available on NCS 1004, including local SSD, network-based iPXE, Zero Touch Provisioning, and Golden ISO, to help you select the appropriate method for your deployment environment.

This topic explains the boot options available on NCS 1004, including local SSD, network-based iPXE, Zero Touch Provisioning, and Golden ISO, to help you select the appropriate method for your deployment environment.

The boot options available on NCS 1004 are:

- SSD (hard disk),
- USB drive,
- iPXE,
- ZTP, and
- Golden ISO.

> **Note**
>
> If bootable image is not available in any of these boot options, reboot the system.

Boot NCS 1004

Use this procedure to boot NCS 1004 by connecting a terminal to the console port of the Route Processor, configuring the terminal emulation settings, and powering on the router to start the boot sequence.

Boot NCS 1004 by establishing a console terminal session and powering on the device.

Use the console port to connect to NCS 1004. By default, the console port connects to the XR mode. If necessary, you can establish subsequent connections through the management port after it is configured.

Procedure

1. Connect a terminal to the console port of the Route Processor (RP).
2. Start the terminal emulation program on your workstation.

   The console settings are 115,200 bits per second (bps), eight data bits, one stop bit, and no parity.
3. Power on NCS 1004 by pressing the power switch upward to turn on the power shelves.

   When NCS 1004 boots up, the terminal emulation program displays the boot process details at the console.
4. Press **Enter**.

   The boot process is complete when the system prompts you to enter the root-system username. If the prompt does not appear, wait for NCS 1004 to complete the initial boot procedure, then press **Enter**.

NCS 1004 boots successfully, and the system prompts for the root-system username on your console terminal.

What to do next

Important

If the boot process fails, the preinstalled image on NCS 1004 may be corrupt. In this case, boot NCS 1004 using an external bootable USB drive.

Boot NCS 1004 from a USB drive

Use this procedure to create a bootable USB drive from the compressed boot file and use it to reimage or recover NCS 1004 when a valid bootable image is not available on the SSD.

Reimage or recover the NCS 1004 by booting it from a USB drive when the internal SSD does not have a valid bootable image.

Before you begin

- Obtain a USB drive that has at least 4 GB of storage and a single partition.
- Download the NCS 1004 software image from the Software Download page on the website.
- Copy the compressed boot file (for example, `ncs1004-usb-boot-7.0.1.zip`) from the website to your local machine.

The bootable USB drive is used to reimage NCS 1004 for system upgrade or to boot NCS 1004 in case of boot failure. A bootable USB drive is created by copying a compressed boot file to the drive. After you extract the contents of the compressed file, the USB drive becomes bootable.

You can complete this task using Windows, Linux, or macOS. The exact operation for each step depends on the operating system.

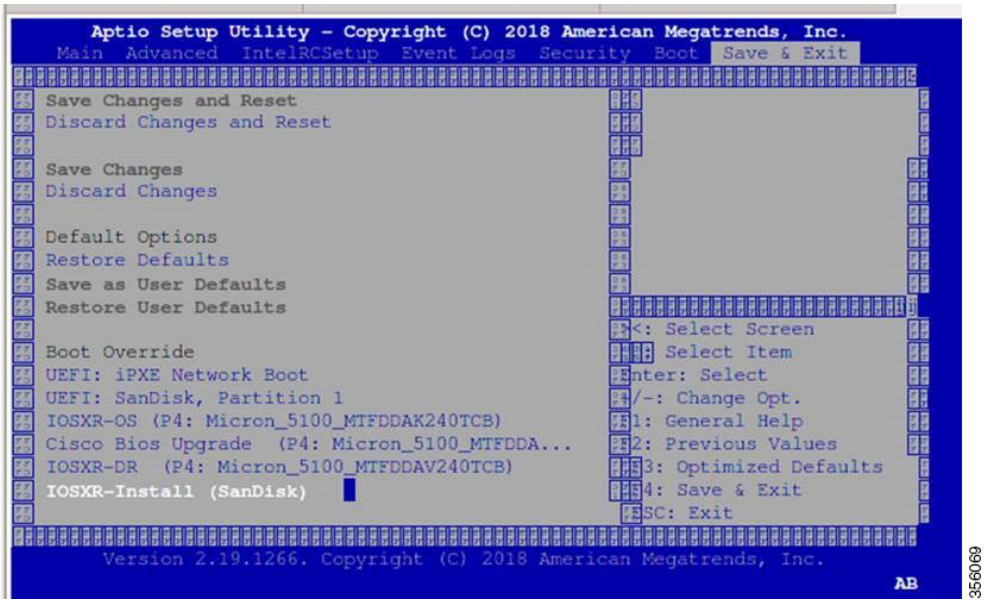
Procedure

1. Connect the USB drive to your local machine and format it with the FAT32 file system.
2. Copy the compressed boot file to the USB drive.
3. Verify that the copy is successful by comparing the file size and MD5 checksum at the source and destination.
4. Extract the content of the compressed boot file directly into the root folder of the USB drive.

   Note

   Extract the `EFI` and `boot` directories directly to the root of the USB drive. If the unzipping application places the extracted files in a new subfolder, move `EFI` and `boot` to the root of the USB drive.

5. Insert the USB drive into one of the USB ports of NCS 1004.
6. Reboot NCS 1004 using a power cycle or the console.
7. Press **Esc** to enter BIOS.
8. Select the **Save & Exit** tab in BIOS.



9. Choose **IOS-XR Install**.

   The system detects the USB drive and boots from it. You can observe the boot progress on the console.

```
Admin Console:
GNU GRUB version 2.00
Press F2 to goto grub Menu..
Booting from USB..
Loading Kernel..

Validating End Entity Certificate...

Validating SubCA Certificate...

Validating Root Certificate...
Loading initrd..

Validating End Entity Certificate...

Validating SubCA Certificate...

Validating Root Certificate...
CiscoSec: Image signature verification completed.
XR Console:
CiscoSec: Image signature verified.
[    9.957281] i8042: No controller found
Starting udev
udevd[972]: failed to execute '/etc/udev/scripts/network.sh'
'/etc/udev/scripts/network.sh': No such file or directory
Populating dev cache
Running postinst /etc/rpm-postinsts/100-dnsmasq...
update-rc.d: /etc/init.d/run-postinsts exists during rc.d purge (continuing)

 Removing any system startup links for run-postinsts ...
  /etc/rcS.d/S99run-postinsts
Configuring network interfaces... done.
```

10. Remove the USB drive when prompted.

NCS 1004 reboots automatically.

```
Setting maximal mount count to -1
Setting interval between checks to 0 seconds
Fri Dec 11 20:35:56 UTC 2015: Install EFI on /dev/mb_disk4
Fri Dec 11 20:35:57 UTC 2015: Install finished on mb_disk
Rebooting system after installation ...
[  116.973666] reboot: Restarting system
Version 2.17.1245. Copyright (C) 2015 American Megatrends, Inc.

BIOS Date: 11/29/2015 12:02:45 Ver: 0ACBZ1110

Press <DEL> or <ESC> to enter setup.

CiscoSec: Image signature verified.


GNU GRUB version 2.00
Press F2 to goto grub Menu..
Booting from Disk..
Loading Kernel..

Validating End Entity Certificate...

Validating SubCA Certificate...

Validating Root Certificate...
Loading initrd..

Validating End Entity Certificate...

Validating SubCA Certificate...

Validating Root Certificate...
CiscoSec: Image signature verification completed.
Initrd, addr=0xff69a000, size=0x955cb0
[    1.745686] i8042: No controller found
```

The NCS 1004 boots from the USB drive, successfully reimages, and reboots from the new installation.

iPXE network boot

This topic explains the iPXE network boot feature on NCS 1004, which enables you to download and install a fresh IOS XR ISO image from an HTTP, FTP, or TFTP server when the router cannot boot from its local storage.

iPXE (Preboot eXecution Environment) network boot feature enables you to download and install a fresh IOS XR ISO image from an HTTP, FTP, or TFTP server.

iPXE is a pre-boot execution environment included in the network card of the management interfaces. It operates at the system firmware (UEFI) level of the chassis. You can use iPXE to reimage the system and boot the chassis if there is a boot failure or no valid bootable partition. iPXE downloads the ISO image, installs the image, and then boots into the new installation.

> **Note**
>
> The time taken for iPXE to download the ISO image depends on the network speed. Ensure that the network speed is sufficient to complete the image download in less than ten minutes. The chassis reloads if the image is not downloaded within ten minutes.

iPXE acts as a bootloader and provides the flexibility to choose the image that the system will boot based on the Platform Identifier (PID), the Serial Number, or the management MAC address. You must define iPXE in the DHCP server configuration file.

Configure a DHCP server for iPXE boot

Use this procedure to configure a DHCP server with the required boot file options for iPXE network boot on NCS 1004, supporting IPv4-only, IPv6-only, or dual-stack environments.

Ensure your DHCP server supports iPXE network boot for NCS 1004, allowing devices to receive correct boot files in IPv4-only, IPv6-only, or dual-stack setups.

A DHCP server must be configured for IPv4, IPv6, or both communication protocols.

> **Note**
>
> For DHCPv6, a routing advertisement (RA) message must be sent to all nodes to indicate how to obtain the IPv6 address. The Router Advertisement Daemon (radvd) enables clients to send DHCP requests.

```
interface eth3
{
        AdvSendAdvert on;
        MinRtrAdvInterval 60;
        MaxRtrAdvInterval 180;
        AdvManagedFlag on;
        AdvOtherConfigFlag on;
        prefix 2001:1851:c622:1::/64
        {
                AdvOnLink on;
                AdvAutonomous on;
                AdvRouterAddr off;
        };
};
```

Procedure

1. Create the `dhcpd.conf` file (for IPv4, IPv6 or both communication protocols), `dhcpd.conf` file (for IPv6), or both in the `/etc/` directory.

   This configuration file stores network information, such as the path to the script, the location of the ISO install file, the location of the provisioning configuration file, the serial number, and the MAC address of the chassis. You can create this file for IPv4, IPv6, or both communication protocols.

2. Test the server once the DHCP server is running.

a) Use the MAC address of the chassis.

Example

```
host ncs1004
{
hardware ethernet ab:cd:ef:01:23:45;
fixed-address <ip address>;
filename "http://<httpserver-address>/<path-to-image>/ncs1004-mini-x.iso";
}
```

b) Use the serial number of the chassis.

Example

```
host demo {
option dhcp-client-identifier "<chassis-serial-number>";
  filename "http://<IP-address>/<hardware-platform>-mini-x.iso";
  fixed-address <IP-address>;
}
```

The serial number of the chassis is derived from the BIOS and is used as an identifier.

The DHCP server is configured for iPXE boot, enabling NCS 1004 devices to obtain the correct boot file in IPv4, IPv6, or dual-stack environments.

```
host 10.89.205.202 {
    hardware ethernet 40:55:39:56:0c:e8;
    fixed-address 10.89.205.210;
    if exists user-class {
        if option user-class = "iPXE" or option user-class = "\x04iPXE" {
            filename "http://10.89.205.127/box1/ncs1004-x64.iso";
        } else {
            filename "http://10.89.205.127/box1/startup.cfg";
        }
    } else {
        filename "http://10.89.205.127/box1/startup.cfg";
    }
}
```

Boot NCS 1004 using iPXE

Use this procedure to boot NCS 1004 over the network using iPXE boot by running the appropriate command from the System Admin console after DHCP and HTTP servers are configured.

Boot NCS 1004 using iPXE to reimage the chassis with a network-based ISO image.

Use iPXE to reimage NCS 1004 from the network when you want to deploy or upgrade software without relying on local storage. This process uses DHCP and HTTP servers to deliver the ISO image.

Before you begin

- The DHCP server is set up and running. See Set up a DHCP server for iPXE boot.
- Log in to the System Admin console using the **admin** command.

Procedure

1. Run the **hw-module location all bootmedia network reload** command in the System Admin console to start the iPXE boot process and reimage the chassis.

   Example

   ```
   sysadmin-vm:0_RP0# hw-module location all bootmedia network reload
   Tue Feb 12 15:29:57.376 UTC
   Reload hardware module ? [no,yes]
   ```

2. Enter **yes** when prompted to confirm the reload.

   The iPXE bootloader contacts the DHCP server, downloads the ISO image, and installs it. Monitor the progress on the console.

   ```
   iPXE 1.0.0+ (3e573) -- Open Source Network Boot Firmware -- http://ipxe.org
   Features: DNS HTTP TFTP VLAN EFI ISO9660 NBI Menu
   Trying net0...
   net0: c4:72:95:a6:14:e1 using dh8900cc on PCI01:00.1 (open)
   [Link:up, TX:0 TXE:0 RX:0 RXE:0]
   Configuring (net0 c4:72:95:a6:14:e1)................. Ok
   net0: 10.37.1.101/255.255.0.0 gw 10.37.1.0
   Next server: 10.37.1.235
   Filename: http://10.37.1.235/ncs1004/ncs1004-mini-x.iso
   http://10.37.1.235/ncs1004/ncs1004-mini-x.iso... 58%
   ```

NCS 1004 boots and installs the specified ISO image from the network. You can monitor and verify installation progress in the System Admin console.

Zero Touch Provisioning (ZTP) boot

This topic explains ZTP, an automated deployment method that installs IOS XR software and applies startup configurations on NCS 1004 without requiring manual intervention at each chassis.

Zero Touch Provisioning (ZTP) allows you to deploy minimal configurations on several chassis. You can use ZTP to boot, set up, and configure the system. You can automate the configuration of the management Ethernet interface, the installation of SMUs, applications, and optional packages using ZTP. ZTP does not execute if a username is already configured in the system.

ZTP auto provisioning allows you to perform these actions:

- **Configuration**: Downloads and runs the configuration files. The first line of the file must include the words "IOS XR" so ZTP can process the file as a configuration.
- **Script**: Downloads and runs the script files. These scripts use a programmatic approach to complete a task. For example, scripts created using IOS XR commands to perform patch upgrades. The first line of the file must contain `#! /bin/bash` or `#! /bin/sh` for ZTP to process the file as a script.

You can use either the ZTP bash script or the ZTP configuration file.

```
host ncs1004 {
  #hardware ethernet 00:a0:c9:00:00:00;
  option dhcp-client-identifier "<chassis-serial-number>";
```

```
    filename "http://<IP-address>/<folder>/ncs1004-ztp.script";
    #filename "http://<IP-address>/<folder>/ncs1004-ztp.cfg";
  }
```

ZTP bash script sample

This is the sample content of the ZTP bash script:

```
#! /bin/bash
#
# NCS1004 Demo Sample
# ZTP installation of config and day-0 SMU's
#
source ztp_helper

wget http://downloads.sourceforge.net/project/yourcode/application.tgz
#install the downloaded application.tgz

#Run XR CLI's from the script
`xrcmd "show version"`
```

ZTP configuration file sample

This is the sample content of the ZTP configuration file. You can automate all the configurations.

```
!! IOS XR Configuration version = 7.0.1
!
telnet vrf default ipv4 server max-servers 20
!
vty-pool default 0 20 line-template default
!
interface MgmtEth0/RP0/CPU0/0
 ipv4 address dhcp
 no shutdown
!
router static
 address-family ipv4 unicast
  0.0.0.0/0 10.77.132.1
!
end
```

Golden ISO

This topic explains the Golden ISO (GISO) feature, which packages the IOS XR mini ISO, optional SMUs, and a startup configuration file into a single bootable image for efficient NCS 1004 deployment.

A Golden ISO is a bootable image format that

- packages the IOS XR mini ISO, optional Software Maintenance Updates (SMUs), and a startup configuration file,
- enables NCS 1004 installation and configuration in a single boot cycle, and
- reduces manual installation steps by automating image assembly and deployment.

Benefits of Golden ISO

- Saves installation effort and time.

- Makes the system available in a single command and boot.

Limitations

- Install operation over IPv6 is not supported.

Building a Golden ISO

You can build a Golden ISO using the `gisobuild.py` script located at `/pkg/bin/gisobuild.py`. Before running the build command, copy the script from NCS 1004 to a Linux environment.

Example:

```
gisobuild.py -i ./ncs1004-mini-x.iso -r ./rpm-directory -c ./xr-config -l label
```

Where:

- *rpm-directory*: Directory where SMUs (XR, Calvados, and host) are stored.
- *xr-config*: IOS XR configuration applied after booting.
- *label* : Label for the Golden ISO.

Use one of these formats when creating the Golden ISO file name:

- *platform-name*`-golden-x-`*version*`.`*label*`.iso` (without k9sec RPM).

  Example: `ncs1004-golden-x-7.0.1.014I-V1.iso`

- *platform-name*`-goldenk9-x-`*version*`.`*label*`.iso` (with k9sec RPM).

  Example: `ncs1004-goldenk9-x-7.0.1.014I-V1.iso`

Verify boot operation

Use this procedure to verify that NCS 1004 has booted successfully by running the show version command and confirming that the installed software version matches the expected release.

Procedure

Use the **show version** command to compare the displayed version with the boot image version.

The versions must be the same.

Example

```
RP/0/RP0/CPU0:ios# show version
Thu Apr 30 21:57:48.371 IST
Cisco IOS XR Software, Version 7.2.1 Copyright (c) 2013-2020 by Cisco Systems,
 Inc.

Build Information:
 Built By     : ahoang
 Built On     : Wed Apr 29 19:22:26 PDT 2020
 Built Host   : iox-lnx-023
 Workspace    : /auto/srcarchive14/prod/7.2.1/ncs1004/ws
 Version      : 7.2.1
```

```
 Location     : /opt/cisco/XR/packages/
 Label        : 7.2.1

cisco NCS-1004 () processor
System uptime is 5 hours 25 minutes
```

Golden ISO for OpenROADM

This topic explains how to boot NCS 1004 using a Golden ISO image for Open ROADM deployments, covering the composition of the GISO image, the build process, USB boot file creation, and post-boot verification.

From Release 7.3.1, NCS 1004 supports booting with a GISO image specifically prepared for Open ROADM deployments.

The GISO image is bundled with these files:

- Mini ISO image,
- Open ROADM RPM,
- OTN-XP RPM, and
- Startup configuration file.

Components of Golden ISO image for OpenROADM deployment

This topic explains the Golden ISO support for Open ROADM on NCS 1004, available from Release 7.3.1, and describes the components that the GISO image must contain for a successful Open ROADM deployment.

This topic explains the Golden ISO support for Open ROADM on NCS 1004, available from Release 7.3.1, and describes the components that the GISO image must contain for a successful Open ROADM deployment.

The Golden ISO (GISO) image includes these bundled files:

- Mini ISO image,
- Open ROADM RPM,
- OTN-XP RPM, and
- Startup configuration file.

In new Open ROADM deployments, you must include the startup configuration file to enable Open ROADM. This file contains:

- DHCP client configuration for IPv4 and IPv6 addresses,
- SSH server configuration,
- XR Netconf configuration, and
- Telnet configuration for IPv4 and IPv6 addresses.

Build a GISO image for OpenROADM

Use this procedure to build a Golden ISO image for Open ROADM by bundling the mini ISO, Open ROADM RPM packages, and a startup configuration file into a single bootable image.

Generate a bootable Golden ISO image that includes the necessary mini ISO, Open ROADM RPM files, and a startup configuration for Open ROADM deployments.

A Golden ISO image is required to install Open ROADM software in a single step. This procedure enables deployment consistency by packaging required files together. Place the mini ISO file, the RPM directory, and the startup configuration file in the same location before you start the build.

Procedure

Use the **gisobuild.py** script available at the `/pkg/bin/gisobuild.py` location to build the Golden ISO.

Syntax: gisobuild.py -i ./ncs1004-mini-x.iso -r ./rpm-directory -c ./xr-config -l label

Example

```
gisobuild.py -i ./ncs1004-mini-xr-7.3.1.iso -r ./RPMS -c ./giso.startup.txt
-l V1
```

Where:

- *gisobuild.py*: Python script to run the GISO image build. Download the script from the GitHub site.
- *rpm-directory*: Directory containing Open ROADM RPM files and OTN-XP RPM files.

  Example: `ncs1004-tp-sw-1.0.0.0-r731.rpm` and `ncs1004-sysadmin-otn-xp-dp-7.3.1-r731.rpm`.
- *xr-config*: IOS XR startup configuration file, for example, `giso.startup.txt`, which includes Open ROADM-specific configurations.
- *label*: Label for identifying the Golden ISO image.

Example

```
gisobuild.py -i ./ncs1004-mini-xr-7.3.1.iso -r ./RPMS -c giso.startup.txt -l
V1

System requirements check [PASS]
Golden ISO build process starting...

Platform: ncs1004 Version: 7.3.1

XR-Config file (/.../giso.startup.txt) will be encapsulated in Golden ISO.

...RPM compatibility check [PASS]

Building Golden ISO...
Summary .....

XR rpms:
ncs1004-k9sec-2.1.0.0-r731.x86_64.rpm

XR Config file:
giso.startup.txt

...Golden ISO creation SUCCESS.

Golden ISO Image Location: /.../ncs1004-goldenk9-x-7.3.1-v1.iso
```

Golden ISO image is created successfully, consolidating the mini ISO, RPMs, and startup config. The output location for the Golden ISO image is displayed on completion.

Create a USB file for OpenROADM

Use this procedure to generate a compressed bootable USB file from the Open ROADM GISO image and copy it to a USB drive to enable NCS 1004 boot for Open ROADM deployment.

Create a bootable USB file so you can deploy NCS 1004 for Open ROADM.

Once the Golden ISO image is available, create a bootable compressed USB file. Use this USB file to boot NCS 1004.

Procedure

1. Generate the USB file using the GISO image.

   Example

   ```
   ./create_usb_zip ncs1004 ncs1004-golden-x-7.3.1-V1.iso
   ```

   The bootable compressed USB file is created.

2. Copy the generated boot file from the system to the USB drive, extract the contents of the USB file onto the drive, and reboot NCS 1004.

   For more information, see Boot NCS 1004 using a USB file for Open ROADM.

NCS 1004 is ready to boot for an Open ROADM deployment using the USB drive you prepared.

Boot NCS 1004 from a USB file for OpenROADM

Use this procedure to boot NCS 1004 using a USB drive loaded with the Open ROADM compressed GISO boot file and BIOS selection.

Initialize or reimage the NCS 1004 system with the Open ROADM image using a USB boot drive.

Before you begin

- Obtain a USB drive that has at least 8 GB of storage and a single partition.
- Download the NCS 1004 software image from the Software Download page on the website.
- Copy the compressed boot file (for example, `ncs1004-usb-boot-7.1.3.zip`) from the website to your local machine.
- Plug the USB drive into the USB 0 port on NCS 1004.

The bootable USB drive is used to reimage NCS 1004 for system upgrade or to boot NCS 1004 in case of boot failure. A bootable USB drive is created by copying a compressed boot file to the drive. After you extract the contents of the compressed file, the USB drive becomes bootable.

You can complete this task using Windows, Linux, or macOS. The exact operation for each step depends on the operating system.

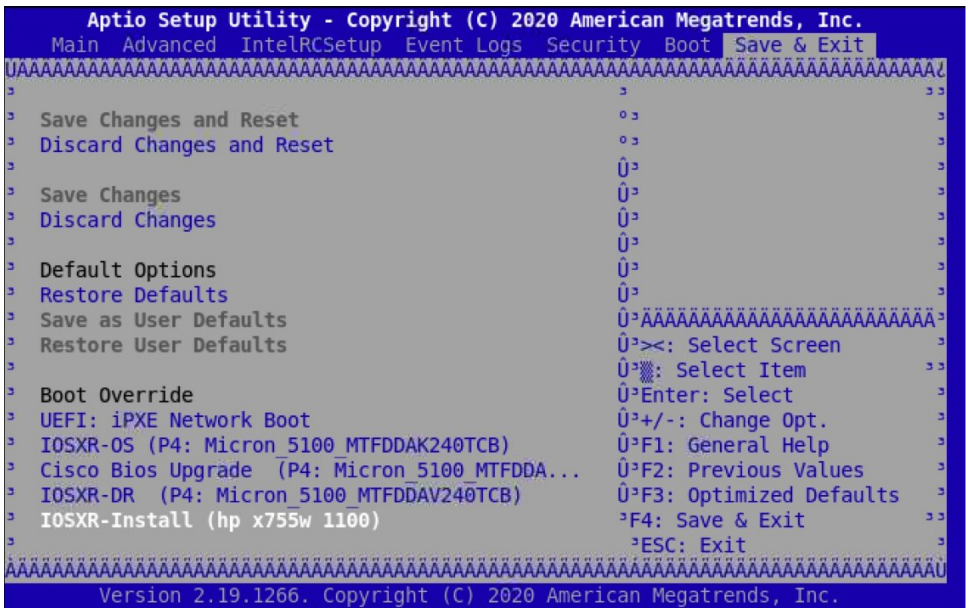
Procedure

1. Connect the USB drive to your local machine and format it with the FAT32 file system.

2. Copy the compressed boot file to the USB drive.
3. Verify that the copy is successful by comparing the file size and MD5 checksum at the source and destination.
4. Extract the content of the compressed boot file directly into the root folder of the USB drive.

> **Note**
>
> Extract the `EFI` and `boot` directories directly to the root of the USB drive. If the unzipping application places the extracted files in a new subfolder, move `EFI` and `boot` to the root of the USB drive.

5. Insert the USB drive into one of the USB ports of NCS 1004.
6. Reboot NCS 1004 using a power cycle or the console.
7. Press **Esc** to enter BIOS.
8. Select the **Save & Exit** tab in BIOS.



9. Choose **IOS-XR Install**.

   The system detects the USB drive and boots the GISO image. The Open ROADM startup configuration is applied automatically on first boot.

```
TAM: Chip DB Verified
CiscoSec: Image Signature Verified
GNU GRUB version 2.00
Press F2 to goto grub Menu..
Booting from USB..
Loading Kernel..
Kernel Secure Boot Validation Result: PASSED
Loading initrd….
Initrd Secure Boot Validation Result: PASSED
Starting udev…..
Running postinst /etc/rpm-postinsts/100-dnsmasq...
Sun Mar  7 19:22:30 UTC 2021: pd_download_giso
Write at Address 0x7bbe000098 (mmap addr 0x7fe08ec87000(0x98)) value 0x1 len
 4 width 4 byte
Write at Address 0x7bbe000098 (mmap addr 0x7f54fc88b000(0x98)) value 0x2 len
```

```
 4 width 4 byte
 Watchdog timer reset done, next reset needed within 10 minutes
Golden ISO type = 1.1 and PKG_VER = 1.0
Current Boot: IOSXR-Install
Current Boot: USB…
 * First booting, filesystem will be relabeled...
Finished Calvados patch for lxc
Starting to prepare calvados logical volume---
 Create sub partition on /dev/panini_vol_grp/calvados_lv0
 Create data sub partition on /dev/panini_vol_grp/calvados_data_lv0
 File system creation on /dev/panini_vol_grp/calvados_lv0 took 6 seconds
 Install sysadmin-vm image on /dev/panini_vol_grp/calvados_lv0
 RP based installation
 Starting Calvados patch for lxc for sysadmin-vm
 Uninstalling rpm task-nxos-core
 Uninstalling rpm gdb
 Uninstalling rpm smartmontools
NCS1004: Complete Patch Calvados
Enable selinux to relabel filesystem from initramfs
Checking SELinux security contexts:
 * First booting, filesystem will be relabeled...
 Finished Calvados patch for lxc
 Installing sysadmin-vm image size of 1.9G took 53 seconds
---Starting to prepare repository---
 File system creation on /dev/cpu_disk2 took 3 seconds
 Check for unwanted iso and remove if required.
 Copying /iso/host.iso to repository /iso directory
 Copying /iso/ncs1004-sysadmin.iso to repository /iso directory
 Copy Sysadmin rpms to repository
 Copy XR rpms to repository
 Copy giso_info.txt to repository
 Copying /iso/ncs1004-xr.iso to repository /iso directory
 Copying all ISOs to repository took 12 seconds
 Install EFI on /dev/cpu_disk4
pd_notify_img_install_done
Checking disk error for: sdb
 Chassis disk smartctl -a output
 Chassis disk smartctl output done
 Disk model: Micron_5100_MTFDDAV240TCB
 No failures found in dmesg
 Checking Chassis disk mount failures.
 No mount failures found in Chassis disk /dev/sdb2
 No mount failures found in Chassis disk /dev/BHDisasterRecovery/golden_image

 Chassis disk partitions exist
 Install finished on cpu_disk
```

10. Remove the USB drive.

    NCS 1004 reboots automatically.

```
Rebooting system after installation ...
[201.715171] reboot: Restarting system
ERROR: Class:0; Subclass:10000; Operation: 1004
NCS1004: Initializing Devices
Version 2.19.1266. Copyright (C) 2020 American Megatrends, Inc.
BIOS Date: 10/23/2020 09:03:42 Ver: 0ACHI470
Press <DEL> or <ESC> to enter setup
TAM: Chip DB
CiscoSec: Image Signature Verified
```

```
GNU GRUB version 2.00
Press F2 to goto grub Menu..
Booting from Disk..
Loading Kernel..
Kernel Secure Boot Validation Result: PASSED
Loading initrd..
Initrd Secure Boot Validation Result: PASSED
[3.836637] i8042: No controller found
Enable selinux to relabel filesystem from initramfs



Load IMA appraise policy: OK



Switching to new root and running init.



Sourcing /etc/sysconfig/udev



Starting udev: [  OK  ]



Starting udev



Running postinst /etc/rpm-postinsts/100-dnsmasq...



update-rc.d: /etc/init.d/run-postinsts exists during rc.d purge (continuing)



 Removing any system startup links for run-postinsts
  /etc/rcS.d/S99run-postinsts
Configuring network interfaces... done.
Starting system message bus: dbus.
Starting OpenBSD Secure Shell server: sshd
  generating ssh RSA key...
  generating ssh ECDSA key...
  generating ssh DSA key...
  generating ssh ED25519 key...
sshd start/running, process 3559
Starting rpcbind daemon...done.
Starting kdump:[  OK  ]
Starting random number generator daemon.
Starting system log daemon...0
Starting kernel log daemon...0
tftpd-hpa disabled in /etc/default/tftpd-hpa
Starting internet superserver: xinetd.
Starting S.M.A.R.T. daemon: smartd.
Starting Lighttpd Web Server: lighttpd.
Starting libvirtd daemon: [  OK  ]
Starting crond: OK
Starting cgroup-init
```

```
Network ieobc_br defined from /etc/init/ieobc_br_network.xml
Network local_br defined from /etc/init/local_br_network.xml
Network xr_local_br defined from /etc/init/xr_local_br_network.xml
Network ieobc_br started
Network local_br started
Network xr_local_br started
mcelog start/running, process 4647
diskmon start/running, process 4653
Creating default host password file
Start serial incoming on , Clearing ..
initctl: Unknown instance: /dev/ttyS0
Connecting to 'default-sdr--1' console
bootlogd: ioctl(/dev/pts/2, TIOCCONS): Device or resource busy
Running postinst /etc/rpm-postinsts/100-dnsmasq...
update-rc.d: /etc/init.d/run-postinsts exists during rc.d purge (continuing)
Removing any system startup links for run-postinsts ...
  /etc/rcS.d/S99run-postinsts
Configuring network interfaces... done.
Starting system message bus: dbus.
Starting OpenBSD Secure Shell server: sshd
  generating ssh RSA key...
  generating ssh ECDSA key...
  generating ssh DSA key...
  generating ssh ED25519 key...
sshd start/running, process 2197
Starting rpcbind daemon...done.
Starting random number generator daemon.
Starting system log daemon...0
Starting kernel log daemon...0
tftpd-hpa disabled in /etc/default/tftpd-hpa
Starting internet superserver: xinetd.
net.ipv4.ip_forward = 1
Libvirt not initialized for container instance
Starting crond: OK
SIOCADDRT: File exists
Start serial incoming on , Clearing ..
ios con0/RP0/CPU0 is now available
Press RETURN to get started.
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply third-party
authority to import, export, distribute or use encryption. Importers,
exporters, distributors and users are responsible for compliance with
U.S. and local country laws. By using this product you agree to comply
with applicable laws and regulations. If you are unable to comply with
U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be
found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
```

NCS 1004 boots from the USB drive and installs the Open ROADM image. Upon completion, the system reboots and applies the Open ROADM startup configuration, with confirmation messages indicating successful installation and startup.

Verify the boot operation for OpenROADM

Use this procedure to verify that NCS 1004 booted successfully with the Open ROADM GISO image by running the show version command and confirming the installed GISO version and label.

Ensure NCS 1004 is running the correct Open ROADM GISO image and is ready for operation.

Procedure

Use the **show version** command to compare the displayed version with the intended Open ROADM boot image version.

The displayed version and label must match the GISO image intended for this device.

Example

```
RP/0/RP0/CPU0:ios#show version
Sun Mar  7 19:31:38.139 UTC
Cisco IOS XR Software, Version 7.3.1
Copyright (c) 2013-2021 by Cisco Systems, Inc.

Build Information:
Built By     : ingunawa
Built On     : Thu Feb 25 19:10:10 PST 2021
Built Host   : iox-lnx-070
Workspace    : /auto/srcarchive17/prod/7.3.1/ncs1004/ws
Version      : 7.3.1
Location     : /opt/cisco/XR/packages/
Label        : 7.3.1-0

cisco NCS-1004 () processor
System uptime is 1 minute
```

NCS 1004 successfully runs the intended Open ROADM GISO version and label, confirming proper boot operation.

Bring up a line card

Use this procedure to bring up a line card on NCS 1004 by inserting the card, verifying the LED status, configuring the LC mode, and upgrading the field-programmable devices (FPDs).

Procedure

1. Insert the line card into the designated slot.
2. Wait until the LED on the line card turns green, indicating successful hardware initialization.
3. Configure the OTN-XP card with LC mode.

   For more information, see LC mode on OTN-XP card.

4. Upgrade the FPDs (field-programmable devices) of the line card if required based on the output of **show hw-module location 0/***line-card-slot* **fpd**.

The line card is successfully installed and operational, ready for further network configuration and use.

Disaster recovery

This topic explains key details of the disaster recovery feature on NCS 1004, which automatically restores node software and configuration with minimal downtime when you replace the CPU or chassis.

The disaster recovery feature on NCS 1004 enables you to quickly and automatically restore node software and configuration after hardware replacement, minimizing system downtime and manual intervention. The feature operates without requiring console access. Before replacing a CPU, use the **graceful-recovery backup initiate** command to back up the XR configuration. The node also creates a backup of the running XR configuration after 20 minutes. After rebooting, the node immediately backs up the XR configuration.

CPU replacement

Consider these points for CPU replacement:

- The node runs in headless mode.
- You can insert the CPU with SSD, and the node then starts to boot the OS from the CPU SSD.
- The system compares the versions of the images in the CPU SSD and the chassis SSD.
- If the version is different, configuration is taken from chassis SSD as the chassis golden image has priority.
- If the version is the same, the node boots up. The node performs this version comparison during every reboot, including power cycles.
- The node always uses the configuration from the chassis. If the chassis SSD is not functional, the node boots using only the CPU.

Chassis replacement

Consider these points for chassis replacement:

- Chassis replacement results in minimum downtime.
- When you receive the chassis, connect the CPU and boot the system. After receiving the empty chassis through RMA, insert the CPU to restore the configuration.
- You can also swap the CPU from other units; however, the chassis image and configuration will be replaced on the CPU.

Health check for proper backup ISO image

This topic explains the health check feature that continuously monitors the backup ISO image stored on NCS 1004 and raises an alarm if it detects image corruption, ensuring a reliable recovery path during disaster recovery.

This feature performs a basic validation of the backup ISO image intended for use during disaster recovery.

Table 1: Feature history

Feature name	Release information	Feature description
Health check for proper backup ISO image	Release 7.5.2	This feature performs a basic validation of the backup ISO image intended for use during disaster recovery. The validation happens before copying the image to the CPU disk and motherboard disks, and thereafter the copied image is audited every 12 hours. Image corruption triggers the **Disaster recovery is disabled due to corrupted ISO** alarm. This health check feature ensures error-free booting of NCS 1004 during disaster recovery operations.

Note

To clear the **DISASTER-RECOVERY-DISABLED** alarm, log in to the Technical Support website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Note

Verify that there is no **Disaster recovery is disabled due to corrupted ISO** alarm using the **show alarms** command before sending the CPU for RMA.

Access the system admin console

Use this procedure to switch from the XR console to the System Admin console on NCS 1004 to perform system administration and hardware management tasks that require System Admin mode.

All system administration and hardware management setup is performed from the System Admin console.

Procedure

1. Log in to the XR console as the root user.
2. Press **Ctrl+O** to disconnect from the XR console and connect to the System Admin console.

Example

```
RP/0/RP0/CPU0:ios#
Disconnecting from 'default-sdr--1' console. Continue(Y/N)?

Y
```

```
Connecting to 'sysadmin' console

System Admin Username: root
Password:
root connected from 127.0.0.1 using console on sysadmin-vm:0_RP0
sysadmin-vm:0_RP0#
```

After you enter the System Admin console, the prompt changes to:

```
sysadmin-vm:0_RP0#
```

Configure the management interface

Use this procedure to configure the management Ethernet interface on NCS 1004. Assign an IP address and subnet mask, and add a static default route to enable connectivity with remote management stations or TFTP servers.

Establish management connectivity for NCS 1004 by setting up its management Ethernet interface.

Before you begin

- Consult your network administrator or system planner to obtain IP addresses and a subnet mask for the management port.
- Ensure that the management port is physically connected to the management network.

Procedure

1. Enter configuration mode.

   Example

   ```
   RP/0/RP0/CPU0:ios# configure
   ```

2. Use the **interface mgmtEth** *rack/slot/instance/port* command to enter the interface configuration mode for the management interface.

   Example

   ```
   RP/0/RP0/CPU0:ios(config)# interface mgmtEth 0/RP0/CPU0/0
   ```

3. Use the **ipv4 address** *ipv4-address subnet-mask* command to assign an IP address and a subnet mask to the interface.

   Example

   ```
   RP/0/RP0/CPU0:ios(config-if)# ipv4 address 10.1.1.1 255.0.0.0
   ```

4. Use the **no shutdown** command to bring the interface up.

   Example

   ```
   RP/0/RP0/CPU0:ios(config-if)# no shutdown
   ```

5. Exit the interface configuration mode.

   Example

   ```
   RP/0/RP0/CPU0:ios(config-if)# exit
   ```

6. Use the **router static address-family ipv4 unicast** command to configure a default static route.

   Example

   ```
   RP/0/RP0/CPU0:ios(config)# router static address-family ipv4 unicast 0.0.0.0/0
    192.0.2.1
   ```

   Specifies the IP address of the default gateway to configure a static route. Use this IP address for communication with devices on other networks.

7. Use the **commit** or **end** command.
   - **commit** – saves the configuration changes and remains within the configuration session.
   - **end** – prompts you to save (**Yes**), discard (**No**), or stay in the session (**Cancel**).

The management Ethernet interface is configured with an IP address, subnet mask, and default route, enabling remote management connectivity.

What to do next

Proceed to configure Telnet and SSH access for remote administration, if required.

Configure the Telnet server access on NCS 1004

Use this procedure to configure the Telnet server on NCS 1004 and verify connectivity by establishing a Telnet session to the management interface.

Enable and configure the Telnet server on NCS 1004, specify the maximum allowed connections, and verify server accessibility.

Telnet allows remote access for management and troubleshooting. By default, Telnet is disabled on NCS 1004 systems.

Procedure

---

1. Enter configuration mode.

   Example

   ```
   RP/0/RP0/CPU0:ios# configure
   ```

   Enters the configuration mode.

2. Use the **telnet {ipv4 | ipv6} server max-servers** *limit* command to specify the number of allowable Telnet servers.

Example

```
RP/0/RP0/CPU0:ios(config)# telnet ipv4 server max-servers 10
```

This command specifies the number of allowable Telnet servers (up to 100). By default, Telnet servers are not allowed. You must configure this command to enable Telnet servers.

3. Use the **commit** or **end** command.
   - **commit** – saves the configuration changes and remains within the configuration session.
   - **end** – prompts you to save (**Yes**), discard (**No**), or stay in the session (**Cancel**).

The Telnet server is enabled on NCS 1004, allowing remote connections according to your configured session limit.

Configure SSH server access on NCS 1004

Use this procedure to configure SSH server version 2 on the NCS 1004 device and verify secure connectivity to the management interface.

Enable SSH server version 2 on NCS 1004 to allow secure remote administration.

Before you begin

- Install the `ncs1004-k9sec` package on NCS 1004. For package installation, see the Install Packages section.
- Generate the crypto key for SSH using the **crypto key generate dsa** command.

Enabling SSH server access ensures secure connections to the management interface port using the IP address.

Procedure

1. Enter configuration mode.

   Example

   ```
   RP/0/RP0/CPU0:ios# configure
   ```

2. Use the **ssh server v2** command to enable the SSH server to accept only SSHv2 client connections:

   Example

   ```
   RP/0/RP0/CPU0:ios(config)# ssh server v2
   ```

3. Use the **commit** or **end** command.
   - **commit** – saves the configuration changes and remains within the configuration session.
   - **end** – prompts the user to save (**Yes**), discard (**No**), or stay in the session (**Cancel**).

4. Use the **show ssh session details** command to verify that the SSH sessions are established.

Example

```
RP/0/RP0/CPU0:ios# show ssh session details

Tue Feb 12 16:03:51.455 UTC
SSH version : Cisco-2.0

id  key-exchange          pubkey              incipher   outcipher  inmac
      outmac
-----------------------------------------------------------------------------------------
Incoming Sessions
1   ecdh-sha2-nistp256    ecdsa-sha2-nistp256 aes128-ctr aes128-ctr
hmac-sha2-256 hmac-sha2-256
```

Displays a detailed report of the SSHv2 connections to and from NCS 1004.

SSH server version 2 is enabled, and you can establish a secure SSH session to the management interface of NCS 1004 using its configured IP address.

Synchronize the system clock with an NTP server

Use this procedure to perform NTP server synchronization on NCS 1004 to keep the system clock accurate and prevent time deviation between NCS 1004 and network management systems.

Connect the NCS 1004 system clocks (XR and System Admin) to a Network Time Protocol (NTP) server to ensure they remain accurate and synchronized with network management systems.

Before you begin

Configure and connect to the management port. See Configure the management interface.

NCS 1004 has distinct system clocks for the XR and System Admin. When you synchronize the XR clock with an NTP server, both system clocks align. Synchronizing the clocks reduces the risk of time drift.

Procedure

1. Enter configuration mode.

   Example

   ```
   RP/0/RP0/CPU0:ios# configure
   ```

   Enters XR configuration mode.
2. Use the **ntp server** command to configure the NTP server.

   Example

   ```
   RP/0/RP0/CPU0:ios(config)# ntp server 192.0.2.55
   ```

   The XR clock is configured to synchronize with the specified NTP server.

The XR clock is synchronized with the NTP server. The System Admin clock automatically synchronizes with the XR clock, ensuring accurate time throughout NCS 1004.

2 Configure AAA

Topics:

Provides instructions for implementing task-based authorization to control user access through TACACS+ and RADIUS servers. It details updated security practices regarding password and secret encryption, as well as procedures for configuring server groups, authentication methods, and accounting features to enhance system security and management.

AAA can be implemented on NCS 1004 using administrative models of task-based authorization. Implementation involves configuring TACACS+ and RADIUS servers and groups to control user access in the software system.

Note

From Release 24.4.1, the AAA local database supports configuring up to 3000 usernames. Although you can configure more than 3000 users, it may impact the system's scale and performance, which are not assured beyond this limit.

RADIUS security protocol

This topic explains how RADIUS security protocol supports centralized authentication, authorization, and accounting management in distributed networks.

RADIUS is a network protocol that provides centralized authentication, authorization, and accounting management for users who connect and use a network service. The protocol operates on a client-server model.

- RADIUS clients operate on network devices such as NCS 1004.
- RADIUS clients send authentication and accounting requests to the central RADIUS server.
- RADIUS servers contain all the user authentication and network service access information.

The AAA security paradigm supports RADIUS, which can be used with other security protocols such as TACACS+, Kerberos, and local username lookup.

Configure RADIUS server groups

Use this procedure to enable centralized authentication and accounting for network access.

Before you begin

Ensure that the external server is accessible at the time of configuration.

RADIUS server groups allow you to organize external RADIUS servers into logical groups that can be referenced from AAA method lists for authentication, authorization, or accounting services.

You can enter one or more **server** commands. The **server** command specifies the hostname or IP address of an external RADIUS server and its port numbers. After configuration, the server group is referenced from the AAA method lists for authentication, authorization, or accounting.

You can configure up to 30 servers and private servers for each RADIUS server group.

Procedure

1. Configure RADIUS server parameters. For details, see Configure RADIUS server parameters.
2. Enable AAA authentication for the RADIUS server group. For details, see Enable RADIUS authentication.

Configure RADIUS server parameters

Use this procedure to configure the RADIUS server group and add external RADIUS servers with their connection parameters.

This task configures the basic RADIUS server group and adds external RADIUS servers with their IP addresses, authentication ports, accounting ports, and encryption keys.

Procedure

1. Enter global configuration mode.

   Example

   ```
   RP/0/RP0/CPU0:ios# configure
   ```

2. Enter the **aaa group server radius** command to create a RADIUS server group and enter server group configuration mode.

Example

```
RP/0/RP0/CPU0:ios(config)# aaa group server radius radgroup1
```

This command groups different server hosts into distinct lists.

3. Enter the **radius-server host** command to specify the hostname or IP address of the RADIUS server host.

   Example

   ```
   RP/0/RP0/CPU0:ios(config)# radius-server host 192.168.20.0
   ```

4. Enter the **auth-port** command to specify the User Datagram Protocol (UDP) destination port for authentication requests.

   Example

   ```
   RP/0/RP0/CPU0:ios(config)# auth-port 1812
   ```

   If you set the value to 0, the host is not used for authentication. If you do not specify a value, the port number is 1645 by default.

5. Enter the **acct-port** command to specify the UDP destination port for accounting requests.

   Example

   ```
   RP/0/RP0/CPU0:ios(config)# acct-port 1813
   ```

   If you set the value to 0, the host is not used for accounting. If you do not specify a value, the port number is 1646 by default.

6. Enter the **key** command to specify the authentication and encryption key used between NCS 1004 and the RADIUS server.

   Example

   ```
   RP/0/RP0/CPU0:ios(config-radius-host)# key 7 08984B1A4D0C19157A5F57
   ```

   This key overrides the global setting of the **radius-server key** command. If you do not specify a key string, the global value is used.

   The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command syntax. This is because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

7. Repeat steps 3 through 6 for each external RADIUS server that you want to add to the server group.

What to do next

After configuring the RADIUS server parameters, enable AAA authentication for the RADIUS server group. For details, see Enable RADIUS authentication.

Enable RADIUS authentication

Use this procedure to use the configured RADIUS server group for user login validation.

Enable AAA for the RADIUS server group and verify the configuration.

Before you begin

Before you begin, ensure that you have configured RADIUS server parameters. For details, see Configure RADIUS server parameters.

Follow these steps to enable RADIUS authentication:

Procedure

1. Enter the **aaa authentication login** command to specify the default method list for authentication and enable authentication for console in global configuration mode.

   Example

   ```
   RP/0/RP0/CPU0:ios(config-radius-host)# aaa authentication login default group
    radius local
   ```

2. Commit the configuration changes.

   Example

   ```
   RP/0/RP0/CPU0:ios(config-radius-host)# commit
   ```

   Alternatively, you can use the **end** command to commit and exit configuration mode.

3. (Optional) Enter the **show radius server-groups** command to display information about each configured RADIUS server group in the system.

   Example

   ```
   RP/0/RP0/CPU0:ios# show radius server-groups
   ```

TACACS+ security protocol

This topic explains how TACACS+ security protocol enhances device security by centralizing user authentication, authorization, and accounting.

TACACS+ is a security protocol designed to provide centralized authentication, authorization, and accounting services for network devices. The protocol offers:

- centralized user validation for enhanced security,
- detailed accounting information for monitoring user activities, and
- flexible administrative control over user access and permissions.

TACACS+ authentication flow on NCS 1004

The TACACS+ application is designed to enhance the security of the NCS 1004 device by centralizing user validation. It uses AAA commands and can be enabled and configured on NCS 1004 for improved security.

When the TACACS+ server is configured and protocol is enabled on the node, user credentials are authenticated through the TACACS+ server. When the user attempts to log into the node, the user name and password are forwarded to the configured TACACS+ servers to obtain authentication status.

If authentication fails through the TACACS+ server, the credentials are sent to the node and authenticated locally. If the authentication fails against the node, the user is not allowed to log into the node.

Configure TACACS+ server groups

Use this procedure to enable centralized authentication, authorization, and accounting for network access.

TACACS+ server groups help organize existing server hosts into logical groups. This allows you to select a subset of preconfigured server hosts for a particular service.

Before you begin

For successful configuration, the external server must be accessible at the time of configuration. If you assign the same IP address for global configuration, you must specify server-private parameters.

Configuring NCS 1004 to use AAA server groups allows you to group existing server hosts. The system uses a server group along with a global server host list. The server group includes the IP addresses of selected server hosts.

You can enter one or more **server** commands. The **server** command specifies the hostname or IP address of an external TACACS+ server. After configuration, you can reference this server group from the AAA method lists for authentication, authorization, or accounting.

To configure TACACS+ server groups, complete these subtasks:

Procedure

1. Configure TACACS+ server parameters. For details, see Configure TACACS+ server parameters.
2. Enable AAA authentication and authorization for the TACACS+ server group. For details, see Enable TACACS+ authentication and authorization.

Configure TACACS+ server parameters

Use this procedure to configure the TACACS+ server group and add external TACACS+ servers with their connection parameters.

This task configures the basic TACACS+ server group and adds external TACACS+ servers with their IP addresses, port numbers, encryption keys, and timeout values.

Procedure

1. Enter the IOS XR configuration mode.

   Example

   ```
   RP/0/RP0/CPU0:ios# configure
   ```

2. Enter the **aaa group server tacacs+** command to create an AAA server-group and access the server-group sub-configuration mode.

   Example

   ```
   RP/0/RP0/CPU0:ios(config)# aaa group server tacacs+ tacgroup1
   ```

3. Enter the **server-private** command to configure the IP address of the private TACACS+ server for the group server.

   Example

   ```
   RP/0/RP0/CPU0:ios(config-sg-tacacs+)# server-private 10.1.1.1 port 49 key
   a_secret
   ```

   Note

   - You can configure up to ten TACACS+ private servers in a server group.
   - If you do not specify private server parameters, the system uses global configurations. If you do not specify global configurations, the system uses default values.

4. Enter the **key** command to configure the authentication and encryption key used between NCS 1004 and the TACACS+ daemon running on the TACACS+ server.

   Example

   ```
   RP/0/RP0/CPU0:ios(config-sg-tacacs+)# key 7 08984B1A4D0C19157A5F57
   ```

   If no key string is specified, the global value is used.

5. Enter the **timeout** command to configure the timeout value that sets the length of time the AAA server waits to receive a response from the TACACS+ server.

   Example

   ```
   RP/0/RP0/CPU0:ios(config-sg-tacacs-private)# timeout 4
   ```

6. Repeat steps 3 through 5 to add additional servers to the server group.

What to do next

After configuring the TACACS+ server parameters, enable AAA authentication and authorization for the TACACS+ server group. For details, see Enable TACACS+ authentication and authorization.

Enable TACACS+ authentication and authorization

Use this procedure to configure TACACS+ authentication and authorization with the configured server group. This enables user login validation and access control.

Enable AAA for the TACACS+ server group and verify the configuration.

Before you begin

Ensure that you have configured the TACACS+ server parameters. For details, see Configure TACACS+ server parameters.

Procedure

1. Enter the **aaa authorization exec** command to configure certificate-based authentication for users in TACACS+ server groups.

   Example

   ```
   RP/0/RP0/CPU0:ios(config-sg-tacacs-private)# aaa authorization exec default
   group TACACS_ALL local
   ```

2. Enter the **aaa authorization login** command to set the default authentication method list and enable authentication for the console in global configuration mode.

   Example

   ```
   RP/0/RP0/CPU0:ios(config-sg-tacacs-private)# aaa authentication login default
    group TACACS_ALL local
   ```

3. Commit the changes and exit all configuration modes.

   Example

   ```
   RP/0/RP0/CPU0:ios(config-sg-tacacs-private)# commit
   RP/0/RP0/CPU0:ios(config-sg-tacacs-private)# end
   ```

4. (Optional) Enter the **show tacacs server-groups** command to verify the TACACS+ server group configuration details.

   Example

   ```
   RP/0/RP0/CPU0:ios# show tacacs server-groups
   ```

User activity accounting records are sent to the TACACS+ security server. This enables robust management, billing, and auditing.

Configure TACACS+ server

Use this procedure to track network services and resource usage for management, billing, or auditing purposes.

Enabling the AAA accounting feature on a switch allows it to track the network services that users are accessing and the amount of network resources they are using. The switch then sends this user activity data to the TACACS+ security server in the form of accounting records. Each record contains attribute-value pairs and is saved on the security server for analysis. This data can be used for network management, client billing, or auditing purposes.

Procedure

1. Enter the IOS XR configuration mode.

   Example

   ```
   RP/0/RP0/CPU0:ios# configure
   ```

2. Enter the **aaa accounting exec** command to enable the TACACS+ accounting to send a start-record accounting notice at the beginning of a privileged EXEC process and a stop-record at the end.

   Example

   ```
   RP/0/RP0/CPU0:ios(config)# aaa accounting exec default start-stop group
   TACACS_ALL
   ```

3. Enter the **aaa accounting exec** command to create a default command accounting method list for accounting services provided by a TACACS+ security server.

   Example

   ```
   RP/0/RP0/CPU0:ios(config)# aaa accounting exec default start-stop group
   TACACS_ALL
   ```

   This list is configured for privilege level commands and set with a stop-only restriction.

The switch begins recording user access to network services and sends accounting records to the TACACS+ server for management, billing, or auditing.

Deprecation of Type 7 password and Type 5 secret

This topic explains information about the deprecation of Type 7 password and Type 5 secret configurations, including changes in command-line interface (CLI) options, upgrade behavior, and migration paths.

Password configuration options before Release 24.4.1:

Until Release 24.4.1, there were two options for configuring a password:

- Password: uses Type 7 encryption to store the password.
- Secret: supports Type 5, 8, 9, or 10 hashing algorithms to store the password securely.

Starting with Release 24.4.1, Type 7 password and Type 5 secret are deprecated because of security concerns. The deprecation process began in Release 24.4.1 and will be complete in a future release. We recommend using the default option, Type 10 secret.

password

The **password** options available in CLI from Release 24.4.1:

```
RP/0/RP0/CPU0:ios(config-un)#password ?
LINE The type 7 password followed by '7 ' OR SHA512-based password (deprecated,
 use 'secret')
```

Changes:

- All the options that were present until Release 24.4.1 are removed except LINE (to accept cleartext).
- During upgrade: Any configuration using the Type 7 password configuration is automatically converted to Type 10 secret.
- Post-upgrade: You can still use the Type 7 password option in new commits, but the password is stored as Type 10 secret.

- New syslog has been added to indicate the deprecation process:

```
%SECURITY-PSLIB-4-DEPRECATED_PASSWORD_TYPE : The password configuration is
deprecated.
 Converting it to a Type 10 secret for user <user name>.
```

- **show running configuration** command output before upgrade:

```
username example
password 7 106D000A0618
!
```

show running configuration command output post-upgrade:

```
username example
secret 10
$6$P53pb/FFxNIT4b/.$yVakako4fp9PZiIYYh1xS0.W6b/yPrSyC8j4gLs6xli57iClOryPXyN9y8yojRD2nhAWb9pjr/WAIhbXqp8st.
!
```

masked-password

The **masked-password** options available in CLI from Release 24.4.1:

```
RP/0/RP0/CPU0:ios(config-un)#masked-password ?
0 Specifies a cleartext password will follow
clear Config deprecated. Will be removed in 7.7.1. Specify '0' instead.
<cr> The cleartext user password
```

Changes:

- The options 7 and encrypted, available in Release 24.4.1 and earlier, are removed.
- During upgrade: Any configuration using the Type 7 password configuration is automatically converted to Type 10 secret.
- Post-upgrade: Masked-password remains an alternate method for configuring the password. When you use the masked-password keyword with a clear string in new commits, the password is stored as Type 10 secret.
- New syslog has been added to indicate the deprecation process:

```
%SECURITY-PSLIB-4-DEPRECATED_PASSWORD_TYPE : The password configuration is
deprecated.
 Converting it to a Type 10 secret for user <user name>.
```

- **show running configuration** command output before upgrade:

```
username example
password 7 106D000A0618
!
```

show running configuration command output post-upgrade:

```
username example
secret 10
$6$P53pb/FFxNIT4b/.$yVakako4fp9PZiIYYh1xS0.W6b/yPrSyC8j4gLs6xli57iClOryPXyN9y8yojRD2nhAWb9pjr/WAIhbXqp8st.
!
```

password-policy

The **password-policy** options available in CLI from Release 24.4.1:

```
RP/0/RP0/CPU0:ios(config-un)#password-policy ?
WORD Specify the password policy name

RP/0/RP0/CPU0:ios(config-un)#password-policy abcd password ?
0 Specifies an UNENCRYPTED password will follow
7 Specifies that an encrypted password will follow
LINE The UNENCRYPTED (cleartext) user password
clear Config deprecated. Will be removed in 7.7.1. Specify '0' instead.
encrypted Config deprecated. Will be removed in 7.7.1. Specify '7' instead.
```

Changes:

- All the options that were present until 24.4.1 are removed except LINE (to accept cleartext).
- During upgrade: Any configuration using the Type 7 password configuration is automatically converted to Type 10 secret.
- Post-upgrade: You can still use the password-policy option with new commits, but the password is stored as Type 10 secret.

aaa password-policy

The **aaa password-policy** options available in CLI from Release 24.4.1:

```
RP/0/RP0/CPU0:ios(config)#aaa password-policy abcd
RP/0/RP0/CPU0:ios(config-pp)#?
min-char-change Number of characters change required between old and new
passwords (deprecated, will be removed in 25.3.1)
restrict-password-advanced Advanced restrictions on new password (deprecated,
 will be removed in 25.3.1)
restrict-password-reverse Restricts the password to be same as reversed old
password (deprecated, will be removed in 25.3.1)
```

Changes:

- The options min-char-change, restrict-password-advanced, and restrict-password-reverse, available in Release 24.4.1 and earlier, are now deprecated.
- During upgrade: These deprecated configurations do not go through any change during upgrade.
- Post-upgrade: These deprecated keywords do not take effect when configured post-upgrade.
- New syslog messages have been added to indicate the deprecation process:

```
%SECURITY-LOCALD-4-DEPRECATED_PASSWORD_POLICY_OPTION : The password policy
option 'min-char-change' is deprecated.
Password/Secret will not be checked against this option now.
```

```
%SECURITY-LOCALD-4-DEPRECATED_PASSWORD_POLICY_OPTION : The password policy
option 'restrict-password-reverse' is deprecated.
 Password/Secret will not be checked against this option now.
```

```
%SECURITY-LOCALD-4-DEPRECATED_PASSWORD_POLICY_OPTION : The password policy
option 'restrict-password-advanced' is deprecated.
Password/Secret will not be checked against this option now.
```

- **show running configuration** command output before upgrade:

```
aaa password-policy abcd
lower-case 3
min-char-change 1
restrict-password-reverse
restrict-password-advanced
!
```

show running configuration command output post-upgrade:

```
aaa password-policy abcd
lower-case 3
min-char-change 1
restrict-password-reverse
restrict-password-advanced
!
```

secret

The **secret** options available in CLI from Release 24.4.1:

```
RP/0/RP0/CPU0:ios(config-un)#secret ?
0 Specifies a cleartext password will follow
10 Specifies that SHA512-based password will follow
8 Specifies that SHA256-based password will follow
9 Specifies that Scrypt-based password will follow
LINE The cleartext user password
```

```
RP/0/RP0/CPU0:ios(config-un)#secret 0 enc-type ?
<8-10> Specifies which algorithm to use. Only 8,9,10 supported [Note: Option
'5' is not available to use from 24.4]
```

Changes:

- The options 5 and encrypted are removed.
- During upgrade: Configurations using Type 5 secret will remain unchanged.
- Post-upgrade: Although keyword 5 is deprecated, you can still use existing configurations with Type 5 secret.
- New syslog has been added to indicate the deprecation process:

```
%SECURITY-LOCALD-2-DEPRECATED_SECRET_TYPE : Type 5 secret is deprecated.
Please use the 'secret' keyword with option type 10 for user.
```

- **show running configuration** command output before upgrade:

```
username example
secret 5 $1$kACo$2RtpcwyiRuRB/DhWzabfU1
!
!
```

show running configuration command output post-upgrade:

```
username example
secret 5 $1$kACo$2RtpcwyiRuRB/DhWzabfU1
!
!
```

masked-secret

The **masked-secret** options available in CLI from Release 24.4.1:

```
RP/0/RP0/CPU0:ios(config-un)#masked-secret ?
0 Specifies a cleartext password will follow
10 Specifies that SHA512-based password will follow
8 Specifies that SHA256-based password will follow
9 Specifies that Scrypt-based password will follow
clear Config deprecated. Will be removed in 7.7.1. Specify '0' instead.
<cr> The cleartext user password
```

Changes:

- The options 5 and encrypted are removed.
- During upgrade: Configurations using masked-secret with Type 5 will remain unchanged.
- Post-upgrade: Although keyword 5 is deprecated, you can still use existing configurations with Type 5 masked secret.
- New syslog has been added to indicate the deprecation process:

  ```
  %SECURITY-LOCALD-2-DEPRECATED_SECRET_TYPE : Type 5 secret is deprecated.
  Please use the 'secret' keyword with option type 10 for user.
  ```

- **show running configuration** command output before upgrade:

  ```
  username example
  secret 5 $1$kACo$2RtpcwyiRuRB/DhWzabfU1
  !
  !
  ```

  show running configuration command output post-upgrade:

  ```
  username example
  secret 5 $1$kACo$2RtpcwyiRuRB/DhWzabfU1
  !
  !
  ```

3 Perform Preliminary Checks

Topics:

Provides essential procedures for verifying the operational status and configuration of the Cisco NCS 1004 system. Users can perform these checks to confirm hardware integrity, software versions, and environmental parameters, ensuring the platform is ready for further deployment and configuration.

After successfully logging into the console, you must perform some preliminary checks to verify the default setup. If any setup issue is detected, take corrective action before making further configurations.

Note

The output of the examples in the procedures is not from the latest software release. The output will change for any explicit references to the current release.

Verify status of hardware components

Use this procedure to verify the status of all the hardware components installed on NCS 1004.

Before you begin

Ensure that all required hardware components are installed on NCS 1004. For installation details, see the *Cisco Network Convergence System 1004 Hardware Installation Guide*.

Procedure

1. Enter the **show platform** command in Cisco IOS XR EXEC mode to display the status of Cisco IOS XR.

   Example

```
RP/0/RP0/CPU0:ios# show platform
Wed Mar  4 06:21:26.929 UTC
Node               Type                         State             Config state
--------------------------------------------------------------------------------
0/0                NCS1K4-LC-FILLER             PRESENT           NSHUT
0/1                NCS1K4-1.2T-K9               OPERATIONAL       NSHUT
0/2                NCS1K4-1.2TL-K9              OPERATIONAL       NSHUT
0/3                NCS1K4-LC-FILLER             PRESENT           NSHUT
0/RP0/CPU0         NCS1K4-CNTLR-K9(Active)      IOS XR RUN        NSHUT
0/FT0              NCS1K4-FAN                   OPERATIONAL       NSHUT
0/FT1              NCS1K4-FAN                   OPERATIONAL       NSHUT
0/FT2              NCS1K4-FAN                   OPERATIONAL       NSHUT
0/PM0              NCS1K4-AC-PSU                OPERATIONAL       NSHUT
0/PM1              NCS1K4-AC-PSU                OPERATIONAL       NSHUT
0/SC0              NCS1004                      OPERATIONAL       NSHUT
```

```
RP/0/RP0/CPU0:ios# show platform
Thu May  7 10:03:03.394 UTC
Node               Type                         State             Config state
--------------------------------------------------------------------------------
0/0                NCS1K4-1.2T-K9               OPERATIONAL       NSHUT
0/1                NCS1K4-OTN-XP                OPERATIONAL       NSHUT
0/2                NCS1K4-OTN-XP                OPERATIONAL       NSHUT
0/3                NCS1K4-OTN-XP                OPERATIONAL       NSHUT
0/RP0/CPU0         NCS1K4-CNTLR-K9(Active)      IOS XR RUN        NSHUT
0/FT0              NCS1K4-FAN                   OPERATIONAL       NSHUT
0/FT1              NCS1K4-FAN                   OPERATIONAL       NSHUT
0/FT2              NCS1K4-FAN                   OPERATIONAL       NSHUT
0/PM0              NCS1K4-DC-PSU                OPERATIONAL       NSHUT
0/PM1              NCS1K4-DC-PSU                OPERATIONAL       NSHUT
0/SC0              NCS1004                      OPERATIONAL       NSHUT
```

   a) If Cisco IOS XR is not operational, no output appears. Use the **show sdr** command in Cisco IOS XR mode to verify the state of the service domain router (SDR) on the node.

      This example shows sample output of the **show sdr** command in Cisco IOS XR mode.

```
RP/0/RP0/CPU0:ios# show sdr
Wed Mar  4 06:23:16.143 UTC
Type                 NodeName       NodeState      RedState
PartnerName
--------------------------------------------------------------------------------
NCS1K4-LC-FILLER     0/0            PRESENT                       N/A
```

```
NCS1K4-1.2T-K9        0/1            OPERATIONAL                    N/A
NCS1K4-1.2TL-K9       0/2            OPERATIONAL                    N/A
NCS1K4-LC-FILLER      0/3            PRESENT                        N/A
RP                    0/RP0/CPU0     IOS XR RUN     ACTIVE          NONE
NCS1K4-CNTLR-K9       0/RP0          OPERATIONAL                    N/A
NCS1K4-FAN            0/FT0          OPERATIONAL                    N/A
NCS1K4-FAN            0/FT1          OPERATIONAL                    N/A
NCS1K4-FAN            0/FT2          OPERATIONAL                    N/A
NCS1K4-AC-PSU         0/PM0          OPERATIONAL                    N/A
NCS1K4-AC-PSU         0/PM1          OPERATIONAL                    N/A
NCS1004               0/SC0          OPERATIONAL                    N/A
```

```
RP/0/RP0/CPU0:ios# show sdr
Thu May  7 10:50:08.651 UTC
Type                  NodeName       NodeState      RedState
PartnerName
-------------------------------------------------------------------------------
NCS1K4-1.2T-K9        0/0            OPERATIONAL                    N/A
NCS1K4-OTN-XP         0/1            OPERATIONAL                    N/A
NCS1K4-OTN-XP         0/2            OPERATIONAL                    N/A
NCS1K4-OTN-XP         0/3            OPERATIONAL                    N/A
RP                    0/RP0/CPU0     IOS XR RUN     ACTIVE          NONE
NCS1K4-CNTLR-K9       0/RP0          OPERATIONAL                    N/A
NCS1K4-FAN            0/FT0          OPERATIONAL                    N/A
NCS1K4-FAN            0/FT1          OPERATIONAL                    N/A
NCS1K4-FAN            0/FT2          OPERATIONAL                    N/A
NCS1K4-DC-PSU         0/PM0          OPERATIONAL                    N/A
NCS1K4-DC-PSU         0/PM1          OPERATIONAL                    N/A
NCS1004               0/SC0          OPERATIONAL                    N/A
```

2. Enter the **admin** command to enter System Admin EXEC mode.

Example

```
RP/0/RP0/CPU0:ios# admin
```

3. Enter the **show platform** command to display the information and status of each node in the system.

Example

```
sysadmin-vm:0_RP0# show platform
Wed Mar  4  06:24:46.700 UTC+00:00
Location  Card Type               HW State      SW State      Config State
-------------------------------------------------------------------------------
0/0       NCS1K4-LC-FILLER        PRESENT       N/A           NSHUT
0/1       NCS1K4-1.2T-K9          OPERATIONAL   N/A           NSHUT
0/2       NCS1K4-1.2TL-K9         OPERATIONAL   N/A           NSHUT
0/3       NCS1K4-LC-FILLER        PRESENT       N/A           NSHUT
0/RP0     NCS1K4-CNTLR-K9         OPERATIONAL   OPERATIONAL   NSHUT
0/FT0     NCS1K4-FAN              OPERATIONAL   N/A           NSHUT
0/FT1     NCS1K4-FAN              OPERATIONAL   N/A           NSHUT
0/FT2     NCS1K4-FAN              OPERATIONAL   N/A           NSHUT
0/PM0     NCS1K4-AC-PSU           OPERATIONAL   N/A           NSHUT
```

```
0/PM1     NCS1K4-AC-PSU           OPERATIONAL   N/A           NSHUT
0/SC0     NCS1004                 OPERATIONAL   N/A           NSHUT
```

```
sysadmin-vm:0_RP0# show platform
Thu May  7  10:58:09.331 UTC+00:00
Location  Card Type               HW State      SW State      Config State
--------------------------------------------------------------------------------
0/0       NCS1K4-1.2T-K9          OPERATIONAL   N/A           NSHUT
0/1       NCS1K4-OTN-XP           OPERATIONAL   N/A           NSHUT
0/2       NCS1K4-OTN-XP           OPERATIONAL   N/A           NSHUT
0/3       NCS1K4-OTN-XP           OPERATIONAL   N/A           NSHUT
0/RP0     NCS1K4-CNTLR-K9         OPERATIONAL   OPERATIONAL   NSHUT
0/FT0     NCS1K4-FAN              OPERATIONAL   N/A           NSHUT
0/FT1     NCS1K4-FAN              OPERATIONAL   N/A           NSHUT
0/FT2     NCS1K4-FAN              OPERATIONAL   N/A           NSHUT
0/PM0     NCS1K4-DC-PSU           OPERATIONAL   N/A           NSHUT
0/PM1     NCS1K4-DC-PSU           OPERATIONAL   N/A           NSHUT
0/SC0     NCS1004                 OPERATIONAL   N/A           NSHUT
```

Ensure that the output displays all NCS 1004 components. Both the hardware and software states must be OPERATIONAL.

The various hardware and software states are:

Hardware states

- OPERATIONAL: node is operating normally and is fully functional.
- POWERED_ON: power is on and the node is booting up.
- FAILED: node is powered on but has encountered an internal failure.
- PRESENT: node is in intermediate state in the boot sequence.
- POWERED_OFF: power is off and the node cannot be accessed.

Software states

- OPERATIONAL: software is operating normally and is fully functional.
- SW_INACTIVE: software is not completely operational.

4. Enter the **show inventory** command in Cisco IOS XR EXEC mode to display the details of the physical entities of NCS 1004 along with the details of QSFPs.

Example

```
RP/0/RP0/CPU0:ios# show inventory
Wed Mar  4 05:10:17.107 UTC
NAME: "0/0", DESCR: "Network Convergence System 1004 Filler"
PID: NCS1K4-LC-FILLER, VID: V01, SN: N/A

NAME: "0/1", DESCR: "NCS1K4 12x QSFP28 2 Trunk C-Band DWDM card"
PID: NCS1K4-1.2T-K9, VID: V00, SN: CAT2250B0AE

NAME: "0/1-Optics0/1/0/2", DESCR: "Cisco 100G QSFP28 AOC Pluggable Optics
Module"
PID: QSFP-100G-AOC3M   , VID: V03, SN: INL22262339-A

NAME: "0/1-Optics0/1/0/4", DESCR: "Cisco 100GE QSFP28 SR4 Pluggable Optics
Module"
PID: QSFP-100G-SR4-S, VID: V03, SN: AVF2219S16U
```

```
NAME: "0/1-Optics0/1/0/5", DESCR: "Cisco 100G QSFP28 LR4-S Pluggable Optics
Module"
PID: QSFP-100G-LR4-S, VID: V02, SN: JFQ2145701U

NAME: "0/1-Optics0/1/0/6", DESCR: "Cisco 100GE QSFP28 SR4 Pluggable Optics
Module"
PID: QSFP-100G-SR4-S, VID: ES1, SN: AVF1925G012

NAME: "0/1-Optics0/1/0/7", DESCR: "Cisco 100G QSFP28 LR4-S Pluggable Optics
Module"
PID: QSFP-100G-LR4-S, VID: V02, SN: JFQ2145706N

NAME: "0/1-Optics0/1/0/8", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4, VID: V01, SN: JFQ19026014

NAME: "0/1-Optics0/1/0/9", DESCR: "Cisco 100G QSFP28 LR4-S Pluggable Optics
Module"
PID: QSFP-100G-LR4-S, VID: V02, SN: OPM220518HS

NAME: "0/1-Optics0/1/0/10", DESCR: "Cisco 100G QSFP28 SM-SR Pluggable Optics
 Module"
PID: QSFP-100G-SM-SR, VID: V02, SN: INL21490043

NAME: "0/1-Optics0/1/0/11", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics
 Module"
PID: QSFP-100G-CWDM4-S , VID: V01, SN: JFQ211930JL

NAME: "0/1-Optics0/1/0/12", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics
 Module"
PID: QSFP-100G-CWDM4-S, VID: V02, SN: JFQ2210801H

NAME: "0/2", DESCR: "NCS1K4 12x QSFP28 2 Trunk L-Band DWDM card"
PID: NCS1K4-1.2TL-K9   , VID: V00, SN: CAT2337B0S4

NAME: "0/2-Optics0/2/0/2", DESCR: "Cisco 100G QSFP28 AOC Pluggable Optics
Module"
PID: QSFP-100G-AOC3M, VID: V03, SN: INL22262332-A

NAME: "0/2-Optics0/2/0/4", DESCR: "Cisco 100G QSFP28 SM-SR Pluggable Optics
Module"
PID: QSFP-100G-SM-SR, VID: V02, SN: FNS22070HWF

NAME: "0/2-Optics0/2/0/5", DESCR: "Cisco 100G QSFP28 SM-SR Pluggable Optics
Module"
PID: QSFP-100G-SM-SR, VID: V02, SN: SPT2225302D

NAME: "0/2-Optics0/2/0/6", DESCR: "Cisco 100G QSFP28 LR4-S Pluggable Optics
Module"
PID: QSFP-100G-LR4-S, VID: V02, SN: FNS22310Z1X

NAME: "0/2-Optics0/2/0/8", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4, VID: V01, SN: FNS20520R8Z

NAME: "0/2-Optics0/2/0/9", DESCR: "Cisco 100G QSFP28 AOC Pluggable Optics
Module"
PID: QSFP-100G-AOC3M, VID: V03, SN: INL23312282-A

NAME: "0/2-Optics0/2/0/10", DESCR: "Cisco 100G QSFP28 AOC Pluggable Optics
Module"
PID: QSFP-100G-AOC3M, VID: V03, SN: INL23312282-B
```

```
NAME: "0/2-Optics0/2/0/11", DESCR: "Cisco 100G QSFP28 LR4-S Pluggable Optics
 Module"
PID: QSFP-100G-LR4-S, VID: V02, SN: FNS23080LKF

NAME: "0/3", DESCR: "Network Convergence System 1004 Filler"
PID: NCS1K4-LC-FILLER, VID: V01, SN: N/A

:
:
:
```

```
RP/0/RP0/CPU0:ios# show inventory
Thu May  7 11:05:13.211 UTC
NAME: "0/0", DESCR: "NCS1K4 12x QSFP28 2 Trunk C-Band DWDM card"
PID: NCS1K4-1.2T-K9    , VID: V00, SN: CAT2237B25A

NAME: "0/0-Optics0/0/0/2", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS2333080E

NAME: "0/0-Optics0/0/0/3", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS23330801

NAME: "0/0-Optics0/0/0/4", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS21140GZK

NAME: "0/0-Optics0/0/0/6", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS233209CN

NAME: "0/0-Optics0/0/0/10", DESCR: "Cisco 40GE QSFP+ LR4 Pluggable Optics
Module"
PID: QSFP-40G-LR4      , VID: V02, SN: FNS23110TYD

NAME: "0/1", DESCR: "NCS1K4 4xDD,8xQSFP28,2xCFP2 DCO OTNXponder"
PID: NCS1K4-OTN-XP     , VID: V00, SN: CAT2352B007

NAME: "0/1-Optics0/1/0/0", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS2333080J

NAME: "0/1-Optics0/1/0/1", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS23330806

NAME: "0/1-Optics0/1/0/2", DESCR: "Cisco 4x10GE QSFP+ MLR Pluggable Optics
Module"
PID: ONS-QSFP-4X10-MLR , VID: V01, SN: INL21010391

NAME: "0/1-Optics0/1/0/4", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics
Module"
PID: QSFP-40G-SR4      , VID: V03, SN: JFQ20332007

NAME: "0/1-Optics0/1/0/5", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics
Module"
PID: QSFP-40G-SR4      , VID: V03, SN: JFQ20332088

NAME: "0/1-Optics0/1/0/6", DESCR: "Cisco 4x10GE QSFP+ MLR Pluggable Optics
Module"
PID: ONS-QSFP-4X10-MLR , VID: V01, SN: INL21010471

NAME: "0/1-Optics0/1/0/7", DESCR: "Cisco 4x10GE QSFP+ MLR Pluggable Optics
Module"
PID: ONS-QSFP-4X10-MLR , VID: V01, SN: INL21010376

NAME: "0/2", DESCR: "NCS1K4 4xDD,8xQSFP28,2xCFP2 DCO OTNXponder"
```

```
PID: NCS1K4-OTN-XP      , VID: V00, SN: CAT2352B015

NAME: "0/2-Optics0/2/0/0", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4     , VID: V01, SN: FNS20360V1R

NAME: "0/2-Optics0/2/0/4", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics
Module"
PID: QSFP-40G-SR4       , VID: V03, SN: JFQ21502017

NAME: "0/2-Optics0/2/0/5", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics
Module"
PID: QSFP-40G-SR4       , VID: V03, SN: JFQ202120DY

NAME: "0/3", DESCR: "NCS1K4 4xDD,8xQSFP28,2xCFP2 DCO OTNXponder"
PID: NCS1K4-OTN-XP      , VID: V00, SN: CAT2352B00A

NAME: "0/3-Optics0/3/0/0", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4     , VID: V01, SN: FNS23320BS3

NAME: "0/3-Optics0/3/0/4", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics
Module"
PID: QSFP-40G-SR4       , VID: V03, SN: AVP2217S09L

NAME: "0/3-Optics0/3/0/5", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics
Module"
PID: QSFP-40G-SR4       , VID: V03, SN: AVP2107S0RZ

NAME: "0/RP0", DESCR: "Network Convergence System 1004 Controller"
PID: NCS1K4-CNTLR-K9    , VID: V01, SN: CAT2323B0SG
:
:
:
:
NAME: "0/PM1", DESCR: "Network Convergence System 1004 DC Power Supply Unit"
PID: NCS1K4-DC-PSU      , VID: V01, SN: POG2308CT4W
```

Verify software version

Use this procedure to verify the installed Cisco IOS XR software version on NCS 1004 and determine whether a system upgrade is required.

NCS 1004 is shipped with Cisco IOS XR software preinstalled. Check whether the software version is current. If a newer version is available, upgrade the system to access the latest features on NCS 1004.

Procedure

Enter the **show version** command to display the software version and details such as system uptime.

Example

```
RP/0/RP0/CPU0:ios# show version
Wed Feb 10 19:35:38.274 IST
Cisco IOS XR Software, Version 7.3.2
Copyright (c) 2013-2021 by Cisco Systems, Inc.
Build Information:
```

```
 Built By     : ingunawa
 Built On     : Tue Feb  9 11:45:12 PST 2021
 Built Host   : iox-lnx-068
 Workspace    : /auto/iox-lnx-068-san1/prod/7.3.2/ncs1k/ws
 Version      : 7.3.2
 Location     : /opt/cisco/XR/packages/
 Label        : 7.3.2
cisco NCS-1002 () processor
System uptime is 3 hours 37 minutes
```

What to do next

Verify the software version to determine if a system upgrade is required. If an upgrade is needed, see the Perform System Upgrade and Install Feature Packages chapter.

Verify the firmware version

Use this procedure to verify the firmware version on NCS 1004 hardware components to ensure compatibility with the installed Cisco IOS XR image.

The firmware on NCS 1004 hardware components must be compatible with the installed Cisco IOS XR image. NCS 1004 may malfunction if the firmware version is incompatible.

Procedure

1. Enter the **show hw-module fpd** command in the Cisco IOS XR EXEC mode to display the firmware information of various hardware components of NCS 1004.

   Example

```
RP/0/RP0/CPU0:ios#
                          show hw-module fpd
Fri Nov 26 14:53:27.188 UTC
Auto-upgrade:Disabled
                                                                                FPD
 Versions

==============
Location   Card type             HWver FPD device       ATR Status    Running
   Programd
-------------------------------------------------------------------------------
0/0        NCS1K4-OTN-XPL         3.0   LC_CPU_MOD_FW        CURRENT    75.10
     75.10
0/0        NCS1K4-OTN-XPL         7.0   LC_DP_MOD_FW         CURRENT     3.10
      3.10
0/0       NCS1K4-OTN-XPL        2.0   LC_QSFPDD_PORT_11    CURRENT    61.2013
   61.2013
0/0       NCS1K4-OTN-XPL        2.0   LC_QSFPDD_PORT_9     CURRENT    61.2013
   61.2013
0/1        NCS1K4-OTN-XP          2.0   LC_CPU_MOD_FW        CURRENT    75.10
     75.10
0/1        NCS1K4-OTN-XP          7.0   LC_DP_MOD_FW         CURRENT     3.10
      3.10
0/1       NCS1K4-OTN-XP         2.0   LC_QSFPDD_PORT_11    CURRENT    61.2013
```

```
   61.2013
0/1        NCS1K4-OTN-XP         2.0   LC_QSFPDD_PORT_9     CURRENT    61.2013
   61.2013
0/RP0      NCS1K4-CNTLR-K9       5.0   CSB_IMG           S  CURRENT     0.200
     0.200
0/RP0      NCS1K4-CNTLR-K9       5.0   TAM_FW               CURRENT    36.08
     36.08
0/RP0      NCS1K4-CNTLR-K9       1.14  BIOS              S  CURRENT     5.30
      5.30
0/RP0      NCS1K4-CNTLR-K9       5.0   CPU_FPGA             CURRENT     1.14
      1.14
0/PM1      NCS1K4-AC-PSU         0.1   PO-PriMCU            CURRENT     2.70
      2.70
0/SC0      NCS1004               2.0   BP_FPGA              CURRENT     1.25
      1.25
0/SC0      NCS1004               2.0   XGE_FLASH            CURRENT    18.04
     18.04
```

In this output, some of the significant fields are:

- FPD Device: name of the hardware component such as FPD, CFP, and so on.
- ATR: attribute of the hardware component. Some attributes are:
  - B: backup image
  - S: secure image
  - P: protected image
- Status: upgrade status of the firmware. The different states are:
  - CURRENT: The firmware version is the latest version.
  - NOT READY: The firmware of the FPD is not ready for upgrade.
  - NEED UPGD: A newer firmware version is available in the installed image. We recommend that upgrade be performed.
  - UPGD PREP: The firmware of the FPD is preparing for upgrade.
  - RLOAD REQ: The upgrade is completed, and the card requires a reload.
  - UPGD DONE: The firmware upgrade is successful.
  - UPGD FAIL: The firmware upgrade has failed.
  - UPGD SKIP: The upgrade is skipped because the installed firmware version is higher than the version available in the image.
  - Running: Current version of the firmware running on the FPD.

2. Enter the **show fpd package** command to display the FPD image version available with this software release for each hardware component.

```
                          RP/0/RP0/CPU0:ios#
                          show fpd package
Fri May  8 05:11:47.819 UTC
================================
=============================================
                                        Field Programmable Device Package
```

```
================================================
                                                  Req     SW      Min Req   Min
 Req
Card Type            FPD Description              Reload  Ver     SW Ver  Board
 Ver
==================== ========================== ====== ======= ========
=========
-------------------------------------------------------------------------------
NCS1004-K9           BP_FPGA(A)                  NO      1.25    1.25    0.0
                     XGE_FLASH(A)                YES    18.04   18.04    0.0
-------------------------------------------------------------------------------
NCS1K4-1.2T-K9       LC_CPU_MOD_FW(A)            YES    75.10   75.10    0.0
                     LC_OPT_MOD_FW(A)            YES     1.25    1.25    0.0
-------------------------------------------------------------------------------
NCS1K4-1.2T-L-K9     LC_CPU_MOD_FW(A)            YES    75.10   75.10    0.0
                     LC_OPT_MOD_FW(A)            YES     1.25    1.25    0.0
-------------------------------------------------------------------------------
NCS1K4-1.2TL-K9      LC_CPU_MOD_FW(A)            YES    75.10   75.10    0.0
                     LC_OPT_MOD_FW(A)            YES     1.25    1.25    0.0
-------------------------------------------------------------------------------
NCS1K4-2-QDD-C-K9    LC_CPU_MOD_FW(A)            YES    75.10   75.10    0.0
                     LC_OPT_MOD_FW(A)            YES     1.26    1.26    0.0
-------------------------------------------------------------------------------
NCS1K4-2KW-AC        PO-PriMCU(A)                NO      2.70    2.70    0.0
                     PO-PriMCU(A)                NO      2.70    2.70    0.1
-------------------------------------------------------------------------------
NCS1K4-AC-PSU        PO-PriMCU(A)                NO      2.70    2.70    0.0
                     PO-PriMCU(A)                NO      2.70    2.70    0.1
-------------------------------------------------------------------------------
NCS1K4-CNTLR         BIOS(A)                     YES     5.30    5.30    1.5
                     CSB_IMG                     YES     0.200   0.200   0.0
-------------------------------------------------------------------------------
NCS1K4-CNTLR-B-K9    BIOS(A)                     YES     5.30    5.30    1.0
                     CSB_IMG                     YES     0.200   0.200   0.0
-------------------------------------------------------------------------------
NCS1K4-DC-PSU        PO-PriMCU(A)                NO      1.12    1.12    0.0
                     PO-PriMCU(A)                NO      1.12    1.12    0.1
-------------------------------------------------------------------------------
NCS1K4-OTN-XP        LC_CFP2_PORT_0(A)           NO      0.00    0.00    0.0
   LC_CFP2_PORT_0(A)           NO      1.00    1.00    1.0
                     LC_CFP2_PORT_0(A)           NO      1.52    1.52    2.0
                     LC_CFP2_PORT_1(A)           NO      0.00    0.00    0.0
                     LC_CFP2_PORT_1(A)           NO      1.00    1.00    1.0
                     LC_CFP2_PORT_1(A)           NO      1.52    1.52    2.0
                     LC_CPU_MOD_FW(A)            YES     75.10   75.10   0.0
                     LC_DP_MOD_FW(A)             YES     3.10    3.10    1.0
                     LC_DP_MOD_FW(A)             YES     11.10   11.10   2.0
                     LC_DP_MOD_FW(A)             YES     11.10   11.10   3.0
                     LC_DP_MOD_FW(A)             YES     1.10    1.10    4.0
                     LC_DP_MOD_FW(A)             YES     3.10    3.10    7.0
                     LC_DP_MOD_FW(A)             YES     1.10    1.10    8.0
                     LC_QSFPDD_PORT_11(A)         NO     0.00    0.00    0.0
                     LC_QSFPDD_PORT_11(A)         NO     61.2013 61.2013 1.0
                     LC_QSFPDD_PORT_11(A)         NO     61.2013 61.2013 2.0
                     LC_QSFPDD_PORT_9(A)          NO     0.00    0.00    0.0
                     LC_QSFPDD_PORT_9(A)          NO     61.2013 61.2013 1.0
                     LC_QSFPDD_PORT_9(A)          NO     61.2013 61.2013 2.0
-------------------------------------------------------------------------------
NCS1K4-OTN-XPL       LC_CFP2_PORT_0(A)           NO      0.00    0.00    0.0
   LC_CFP2_PORT_0(A)           NO      1.00    1.00    1.0
                     LC_CFP2_PORT_0(A)           NO      1.52    1.52    2.0
```

```
                    LC_CFP2_PORT_1(A)           NO      0.00    0.00    0.0
                    LC_CFP2_PORT_1(A)           NO      1.00    1.00    1.0
                    LC_CFP2_PORT_1(A)           NO      1.52    1.52    2.0
                    LC_CPU_MOD_FW(A)            YES     75.10   75.10   0.0
                    LC_DP_MOD_FW(A)             YES     3.10    3.10    1.0
                    LC_DP_MOD_FW(A)             YES     11.10   11.10   2.0
                    LC_DP_MOD_FW(A)             YES     11.10   11.10   3.0
                    LC_DP_MOD_FW(A)             YES     1.10    1.10    4.0
                    LC_DP_MOD_FW(A)             YES     3.10    3.10    7.0
                    LC_DP_MOD_FW(A)             YES     1.10    1.10    8.0
                    LC_QSFPDD_PORT_11(A)         NO     0.00    0.00    0.0
                    LC_QSFPDD_PORT_11(A)         NO     61.2013 61.2013 1.0
                    LC_QSFPDD_PORT_11(A)         NO     61.2013 61.2013 2.0
                    LC_QSFPDD_PORT_9(A)          NO     0.00    0.00    0.0
                    LC_QSFPDD_PORT_9(A)          NO     61.2013 61.2013 1.0
                    LC_QSFPDD_PORT_9(A)          NO     61.2013 61.2013 2.0
--------------------------------------------------------------------------------
NCS1K4-TESTUNIT      LC_CPU_MOD_FW(A)           YES     0.01    0.01    0.0
```

What to do next

Upgrade all FPDs using the **upgrade hw-module location all fpd all** command in the Cisco IOS XR EXEC mode. If the upgrade requires a reload, the Status column shows RLOAD REQ.

If reload is required

1. If the FPGA location is 0/RP0, enter the **admin hw-module location 0/RP0 reload** command. This command reboots only the CPU. This reboot does not impact traffic.
2. If the FPGA location is 0/0, enter the **admin hw-module location all reload** command. The chassis reboots, which impacts traffic. When the reload is complete, the new FPGA runs the current firmware version.

> **Caution**
>
> The upgrade of OTNXP LC_DP_MOD_FW and LC_OPT_MOD_FW FPDs affect traffic. Perform this upgrade during a maintenance window.

If Firmware upgrade fails

If the firmware upgrade fails, enter the **show logging** command to view more details. Then, upgrade the firmware again using these commands.

> **Note**
>
> Upgrade the firmware version of power modules only when both power modules are present and powered on.

Verify the management interface status

Use this procedure to verify the operational status and configuration of the management interface using show commands.

Procedure

Enter the **show interfaces mgmtEth** *instance* command to display the management interface configuration.

Example

```
RP/0/RP0/CPU0:ios# show interfaces MgmtEth 0/RP0/CPU0/0
Wed Mar  4 06:13:12.381 UTC
MgmtEth0/RP0/CPU0/0 is up, line protocol is up
  Interface state transitions: 1
  Hardware is Management Ethernet, address is b026.80ff.d870 (bia
b026.80ff.d870)
  Internet address is 10.127.60.184/24
  MTU 1514 bytes, BW 1000000 Kbit (Max: 1000000 Kbit)
     reliability 255/255, txload 0/255, rxload 0/255
  Encapsulation ARPA,
  Full-duplex, 1000Mb/s, CX, link type is autonegotiation
  loopback not set,
  Last link flapped 1d23h
  ARP type ARPA, ARP timeout 04:00:00
  Last input 00:00:00, output 00:00:00
  Last clearing of "show interface" counters never
  5 minute input rate 1368000 bits/sec, 193 packets/sec
  5 minute output rate 95000 bits/sec, 194 packets/sec
     6447256 packets input, 3947875102 bytes, 0 total input drops
     0 drops for unrecognized upper-level protocol
     Received 661276 broadcast packets, 271649 multicast packets
              0 runts, 0 giants, 0 throttles, 0 parity
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     7190033 packets output, 3906991430 bytes, 0 total output drops
     Output 0 broadcast packets, 0 multicast packets
     0 output errors, 0 underruns, 0 applique, 0 resets
     0 output buffer failures, 0 output buffers swapped out
     1 carrier transitions
```

```
RP/0/RP0/CPU0:ios# show interfaces MgmtEth 0/RP0/CPU0/0

Fri May  8 04:40:41.519 UTC
MgmtEth0/RP0/CPU0/0 is up, line protocol is up
  Interface state transitions: 1
  Hardware is Management Ethernet, address is dc8c.37c3.e1a8 (bia
dc8c.37c3.e1a8)
  Internet address is 10.105.57.103/25
  MTU 1514 bytes, BW 1000000 Kbit (Max: 1000000 Kbit)
     reliability 255/255, txload 0/255, rxload 0/255
  Encapsulation ARPA,
  Full-duplex, 1000Mb/s, CX, link type is autonegotiation
  loopback not set,
  Last link flapped 1d04h
  ARP type ARPA, ARP timeout 04:00:00
  Last input 00:00:00, output 00:00:00
  Last clearing of "show interface" counters never
  5 minute input rate 106000 bits/sec, 140 packets/sec
  5 minute output rate 108000 bits/sec, 139 packets/sec
     7303357 packets input, 696872907 bytes, 0 total input drops
     0 drops for unrecognized upper-level protocol
     Received 40679 broadcast packets, 41523 multicast packets
              0 runts, 0 giants, 0 throttles, 0 parity
```

```
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     7231570 packets output, 740818886 bytes, 0 total output drops
     Output 0 broadcast packets, 0 multicast packets
     0 output errors, 0 underruns, 0 applique, 0 resets
     0 output buffer failures, 0 output buffers swapped out
          MgmtEth0/RP0/CPU0/0 is up, line protocol is up
```

The output shows that the management interface is administratively down.

You can also use the **show interfaces summary** or **show interfaces brief** commands in the Cisco IOS XR EXEC mode to verify the management interface status.

This example shows sample output from the **show interfaces summary** command.

```
RP/0/RP0/CPU0:ios# show interfaces summary
Wed Mar  4 06:14:52.995 UTC
Interface Type          Total    UP       Down     Admin Down
--------------          -----    --       ----     ----------
ALL TYPES               4        2        0        2
--------------
IFT_ETHERNET            3        1        0        2
IFT_NULL                1        1        0        0
```

```
RP/0/RP0/CPU0:ios# show interfaces summary
Fri May  8 04:43:57.355 UTC
Interface Type          Total    UP       Down     Admin Down
--------------          -----    --       ----     ----------
ALL TYPES               6        5        0        1
--------------
IFT_LOOPBACK            2        2        0        0
IFT_ETHERNET            3        2        0        1
IFT_NULL                1        1        0        0
```

This example shows sample output from the **show interfaces brief** command.

```
RP/0/RP0/CPU0:ios# show interfaces brief
Wed Mar  4 06:15:51.689 UTC
               Intf       Intf        LineP              Encap  MTU        BW

              Name       State       State              Type (byte)    (Kbps)
--------------------------------------------------------------------------------

                Nu0          up          up               Null  1500
 0
    Mg0/RP0/CPU0/0          up          up              ARPA  1514    1000000

    Mg0/RP0/CPU0/1  admin-down  admin-down              ARPA  1514    1000000

    Mg0/RP0/CPU0/2  admin-down  admin-down              ARPA  1514    1000000
```

```
RP/0/RP0/CPU0:ios# show interfaces brief
Fri May  8 04:44:41.558 UTC
               Intf       Intf        LineP              Encap  MTU        BW
```

```
              Name       State       State               Type (byte)    (Kbps)
--------------------------------------------------------------------------------

                Lo0          up          up           Loopback  1500
0
                Lo1          up          up           Loopback  1500
0
                Nu0          up          up               Null  1500
0
    Mg0/RP0/CPU0/0          up          up               ARPA  1514    1000000

    Mg0/RP0/CPU0/1  admin-down  admin-down               ARPA  1514    1000000

    Mg0/RP0/CPU0/2          up          up               ARPA  1514    1000000
```

What to do next

Perform these steps if the management interface is administratively down.

- Check the Ethernet cable connection.
- Verify the IP address configuration of the management interface. For details on configuring the management interface, see Configure Management Interface.
- Use the **show running-config interface mgmtEth** command to verify whether the management interface is in the no shut state.

  This example shows sample output from the **show running-config interface mgmtEth** command.

```
RP/0/RP0/CPU0:ios# show running-config interface mgmtEth 0/RP0/CPU0/0

Wed Mar  4 06:17:33.833 UTC
interface MgmtEth0/RP0/CPU0/0
 ipv4 address dhcp
!
```

```
RP/0/RP0/CPU0:ios# show running-config interface mgmtEth 0/RP0/CPU0/0

Fri May  8 04:46:29.582 UTC
interface MgmtEth0/RP0/CPU0/0
 ipv4 address 10.105.57.103 255.255.255.128
!
```

  The output shows that the management interface is in the no shut state.

Verify alarms

Use this procedure to view and verify alarm information on NCS 1004 to identify any critical system conditions that require attention.

The **show alarms** command displays alarm information for the NCS 1004. You can view alarms in brief or detailed format. You can also filter alarms by location, card, rack, or system level.

Procedure

Use the **show alarms** command with the desired options to display alarm information.

```
show alarms [ brief [ card | rack | system ] [ location location ] [ active |
history ] | detail [ card | rack | system ] [ location location ] [ active |
clients | history | stats ] ]
```

This command displays alarms in brief or detail format.

Example

```
RP/0/RP0/CPU0:ios# show alarms brief card location 0/RP0/CPU0 active

Wed Mar  4 06:10:55.959 UTC

------------------------------------------------------------------------------
Active Alarms
------------------------------------------------------------------------------
Location        Severity     Group            Set Time
Description

------------------------------------------------------------------------------
0/1             Major        FPD_Infra        03/02/2020 07:09:04 UTC    One
Or More FPDs Need Upgrade Or Not In Current State

0/2             Major        FPD_Infra        03/03/2020 14:27:33 UTC    One
Or More FPDs Need Upgrade Or Not In Current State

0/2             Major        Ethernet         03/03/2020 20:33:33 UTC
HundredGigECtrlr0/2/0/9 - Carrier Loss On The LAN

0/2             Critical     Controller       03/03/2020 20:34:05 UTC
Optics0/2/0/3 - Improper Removal

0/2             NotAlarmed   OTN              03/03/2020 20:34:08 UTC
ODU40/2/0/0/2 - OPUK Client Signal Failure

0/2             NotAlarmed   OTN              03/03/2020 20:34:05 UTC
ODU40/2/0/1/2 - OPUK Client Signal Failure
```

```
RP/0/RP0/CPU0:ios# show alarms brief card location 0/RP0/CPU0 active

Fri May  8 04:46:29.582 UTC

------------------------------------------------------------------------------
Active Alarms
------------------------------------------------------------------------------
Location        Severity     Group            Set Time
Description

------------------------------------------------------------------------------
0/2             NotReported  OTN              05/07/2020 14:25:05 UTC
ODU20/2/0/0/2/3 - Path Monitoring Alarm Indication Signal

0/2             NotReported  OTN              05/07/2020 14:25:05 UTC
ODU2E0/2/0/0/2/4 - Path Monitoring Alarm Indication Signal

0/1             NotReported  OTN              05/07/2020 14:24:41 UTC
ODU20/1/0/0/2/3 - Path Monitoring Alarm Indication Signal
```

```
0/1             NotReported  OTN             05/07/2020 14:25:03 UTC
ODU20/1/0/1/11/3 - Path Monitoring Alarm Indication Signal

0/1             NotReported  OTN             05/07/2020 14:25:03 UTC
ODU2E0/1/0/1/11/4 - Path Monitoring Alarm Indication Signal

0/3             NotReported  OTN             05/07/2020 14:24:41 UTC
ODU20/3/0/0/2/3 - Path Monitoring Alarm Indication Signal

0/3             NotReported  OTN             05/07/2020 14:24:41 UTC
ODU2E0/3/0/0/2/4 - Path Monitoring Alarm Indication Signal

0/1             Major        Ethernet        05/07/2020 14:24:41 UTC
TenGigECtrlr0/1/0/4/1 - Remote Fault
```

Note

In maintenance mode, all alarms are suppressed and the **show alarms** command will not display alarms details. Use the **show controllers** `controllertype R/S/I/P` command to view the client and trunk alarms.

Review the alarm output to identify any critical or major alarms that require immediate attention. Resolve these alarms before making additional configurations.

Verify environmental parameters

Use this procedure to verify that the environmental parameters of NCS 1004 such as temperature, power, voltage, and fan speed are within acceptable ranges to ensure proper system operation.

The **show environment** command displays the environmental parameters of NCS 1004. Monitoring these parameters helps ensure the system operates within safe limits and prevents hardware damage.

Procedure

1. Enter the **admin** command to access System Admin EXEC mode.

   Example

   ```
   RP/0/RP0/CPU0:ios# admin
   ```

2. Use the **show environment** command with the appropriate options to view the environmental parameters of NCS 1004.

   ```
   show environment [ all | altitude | fan | power | voltages | current |
   temperatures ] [ location | location ]
   ```

   These examples show sample output for different environmental parameters:

Example

Fan speed example:

```
sysadmin-vm:0_RP0# show environment fan
Wed Mar  4  05:36:33.678 UTC+00:00
=============================================
                        Fan speed (rpm)
Location     FRU Type           FAN_0   FAN_1
---------------------------------------------
0/FT0        NCS1K4-FAN          7020    6930
0/FT1        NCS1K4-FAN          6780    6690
0/FT2        NCS1K4-FAN          6810    6720

0/PM0        NCS1K4-AC-PSU      25376   24352

0/PM1        NCS1K4-AC-PSU      11200   11232
```

Temperature example:

```
sysadmin-vm:0_RP0# show environment temperatures location 0/RP0
Wed Mar  4  05:44:51.221 UTC+00:00
=============================================================================
Location  TEMPERATURE                Value   Crit Major Minor Minor Major
Crit
          Sensor                    (deg C)   (Lo)  (Lo)   (Lo)   (Hi)   (Hi)
(Hi)
-----------------------------------------------------------------------------
0/RP0
          TEMP_LOCAL                   32    -10    -5     0    55    65
  70
          TEMP_REMOTE1                 32    -10    -5     0    55    65
  70
          TEMP_CPU_DIE                 31    -10    -5     0    75    80
  90
```

Power example:

```
sysadmin-vm:0_RP0# show environment power
Wed Mar  4  05:45:35.640 UTC+00:00
=============================================================================
CHASSIS LEVEL POWER INFO: 0
=============================================================================

   Total output power capacity (N + 1)             :    2000W +       0W
   Total output power required                     :     910W
   Total power input                               :     456W
   Total power output                              :     407W

Power Group 0:
=============================================================================

   Power       Supply     ------Input----   ------Output---      Status
   Module      Type        Volts     Amps    Volts     Amps
=============================================================================

   0/PM0       2kW-AC        0.0      0.0      0.0      0.0    FAILED or NO
PWR

Total of Power Group 0:          0W/  0.0A         0W/  0.0A

Power Group 1:
```

```
==============================================================================

   Power       Supply     ------Input----   ------Output---      Status
   Module      Type        Volts     Amps    Volts     Amps

==============================================================================

   0/PM1       2kW-AC      227.8      2.0     12.0     33.9    OK

Total of Power Group 1:        456W/  2.0A       407W/ 33.9A

==============================================================================

   Location     Card Type            Power       Power       Status
                                     Allocated   Used
                                     Watts       Watts

==============================================================================

   0/0          NCS1K4-LC-FILLER       0           -       RESERVED
   0/1          NCS1K4-1.2T-K9       260         101       ON
   0/2          NCS1K4-1.2TL-K9      260         168       ON
   0/3          NCS1K4-LC-FILLER       0           -       RESERVED
   0/RP0        NCS1K4-CNTLR-K9       55           -       ON
   0/FT0        NCS1K4-FAN           100           -       ON
   0/FT1        NCS1K4-FAN           100           -       ON
   0/FT2        NCS1K4-FAN           100           -       ON
   0/SC0        NCS1004               35           -       ON
```

```
sysadmin-vm:0_RP0# show environment power
Thu May  7  11:55:13.388 UTC+00:00
==============================================================================
CHASSIS LEVEL POWER INFO: 0
==============================================================================

   Total output power capacity (N + 1)             :    2000W +       0W
   Total output power required                     :    1670W
   Total power input                               :    1007W
   Total power output                              :     956W

Power Group 0:
==============================================================================

   Power       Supply     ------Input----   ------Output---      Status
   Module      Type        Volts     Amps    Volts     Amps

==============================================================================

   0/PM0       2kW-DC       50.3     20.0     12.1     79.0    OK

Total of Power Group 0:       1006W/ 20.0A       956W/ 79.0A

Power Group 1:
==============================================================================

   Power       Supply     ------Input----   ------Output---      Status
   Module      Type        Volts     Amps    Volts     Amps

==============================================================================

   0/PM1       2kW-DC        1.3      0.6      0.0      0.0    FAILED or NO
PWR

Total of Power Group 1:          1W/  0.6A         0W/  0.0A

==============================================================================
```

```
   Location     Card Type            Power       Power       Status
                                     Allocated   Used
                                     Watts       Watts
==============================================================================

   0/0          NCS1K4-1.2T-K9         260         194       ON
   0/1          NCS1K4-OTN-XP          340         182       ON
   0/2          NCS1K4-OTN-XP          340         153       ON
   0/3          NCS1K4-OTN-XP          340         160       ON
   0/RP0        NCS1K4-CNTLR-K9         55           -       ON
   0/FT0        NCS1K4-FAN             100           -       ON
   0/FT1        NCS1K4-FAN             100           -       ON
   0/FT2        NCS1K4-FAN             100           -       ON
   0/SC0        NCS1004                 35           -       ON
```

Voltage example:

```
sysadmin-vm:0_RP0# show environment voltages location 0/RP0
Wed Mar  4  05:47:24.668 UTC+00:00
==============================================================================
Location  VOLTAGE                       Value    Crit Minor Minor  Crit
          Sensor                        (mV)     (Lo) (Lo)  (Hi)   (Hi)
------------------------------------------------------------------------------
0/RP0
          ADM1266_VH1_12V              12028  10800 11040 12960 13200
          ADM1266_VH3_3V3               3306   3036  3135  3465  3564
          ADM1266_VH4_2V5               2492   2300  2375  2625  2700
          ADM1266_VP1_1V8               1801   1656  1710  1890  1944
          ADM1266_VP2_1V2               1201   1104  1140  1260  1296
          ADM1266_3V3_STAND_BY          3293   3036  3135  3465  3564
          ADM1266_VP4_3V3_CPU           3301   3036  3135  3465  3564
          ADM1266_VP5_2V5_CPU           2494   2300  2375  2625  2700
          ADM1266_VP6_1V8_CPU           1797   1656  1710  1890  1944
          ADM1266_VP7_1V24_VCCREF       1236   1140  1178  1302  1339
          ADM1266_VP8_1V05_CPU          1045    966   997  1102  1134
          ADM1266_VP9_1V2_DDR_VDDQ      1196   1104  1140  1260  1296
          ADM1266_VP10_1V0_VCCRAM       1074    500   650  1300  1400
          ADM1266_VP11_VNN               882    400   550  1300  1400
          ADM1266_VP12_VCCP             1068    300   450  1300  1400
          ADM1266_VP13_0V6_VTT           599    552   570   630   648
          ADM1293_DB_5V0                5007   4600  4750  5250  5400
          ADM1293_DB_3V3                3305   3036  3135  3465  3564
          ADM1293_DB_5V0_USB_0          5007   4000  4500  5500  6000
          ADM1293_DB_5V0_USB_1          5017   4000  4500  5500  6000
          ADM1293_MB_5V0_PMOD0          5062   4600  4750  5250  5400
          ADM1293_MB_5V0_PMOD1          5032   4600  4750  5250  5400
          ADM1293_MB_2V5_PLL            2483   2300  2375  2625  2700
```

Verify that all environmental parameters are within acceptable ranges. If any parameter is outside the normal range, investigate and resolve the issue before proceeding.

What to do next

Environment parameter anomalies are logged in the syslog. If an environment parameter displayed in the **show environment** command output is not as expected, check the syslog using the **show logging** command. The syslog provides details on any logged problems.

Verify inventory

Use this procedure to display and verify the hardware inventory of all physical entities of NCS 1004. This helps confirm that all physical components are properly recognized by the system.

The **show inventory** command displays hardware inventory details of NCS 1004. These details include the product identifiers (PID), version identifiers (VID), and serial numbers (SN) of all the installed components.

Procedure

1. Use the **show inventory** command in Cisco IOS XR EXEC mode to display the hardware inventory details of NCS 1004.

   Example

```
RP/0/RP0/CPU0:ios# show inventory
Wed Mar  4 05:10:17.107 UTC
NAME: "0/0", DESCR: "Network Convergence System 1004 Filler"
PID: NCS1K4-LC-FILLER, VID: V01, SN: N/A

NAME: "0/1", DESCR: "NCS1K4 12x QSFP28 2 Trunk C-Band DWDM card"
PID: NCS1K4-1.2T-K9, VID: V00, SN: CAT2250B0AE

NAME: "0/1-Optics0/1/0/2", DESCR: "Cisco 100G QSFP28 AOC Pluggable Optics
Module"
PID: QSFP-100G-AOC3M   , VID: V03, SN: INL22262339-A

NAME: "0/1-Optics0/1/0/4", DESCR: "Cisco 100GE QSFP28 SR4 Pluggable Optics
Module"
PID: QSFP-100G-SR4-S, VID: V03, SN: AVF2219S16U

NAME: "0/1-Optics0/1/0/5", DESCR: "Cisco 100G QSFP28 LR4-S Pluggable Optics
Module"
PID: QSFP-100G-LR4-S, VID: V02, SN: JFQ2145701U

NAME: "0/1-Optics0/1/0/6", DESCR: "Cisco 100GE QSFP28 SR4 Pluggable Optics
Module"
PID: QSFP-100G-SR4-S, VID: ES1, SN: AVF1925G012

NAME: "0/1-Optics0/1/0/7", DESCR: "Cisco 100G QSFP28 LR4-S Pluggable Optics
Module"
PID: QSFP-100G-LR4-S, VID: V02, SN: JFQ2145706N

NAME: "0/1-Optics0/1/0/8", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4, VID: V01, SN: JFQ19026014

NAME: "0/1-Optics0/1/0/9", DESCR: "Cisco 100G QSFP28 LR4-S Pluggable Optics
Module"
PID: QSFP-100G-LR4-S, VID: V02, SN: OPM220518HS

NAME: "0/1-Optics0/1/0/10", DESCR: "Cisco 100G QSFP28 SM-SR Pluggable Optics
 Module"
PID: QSFP-100G-SM-SR, VID: V02, SN: INL21490043

NAME: "0/1-Optics0/1/0/11", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics
 Module"
PID: QSFP-100G-CWDM4-S , VID: V01, SN: JFQ211930JL

NAME: "0/1-Optics0/1/0/12", DESCR: "Cisco 100G QSFP28 CWDM4 Pluggable Optics
```

```
 Module"
PID: QSFP-100G-CWDM4-S, VID: V02, SN: JFQ2210801H

NAME: "0/2", DESCR: "NCS1K4 12x QSFP28 2 Trunk L-Band DWDM card"
PID: NCS1K4-1.2TL-K9   , VID: V00, SN: CAT2337B0S4

NAME: "0/2-Optics0/2/0/2", DESCR: "Cisco 100G QSFP28 AOC Pluggable Optics
Module"
PID: QSFP-100G-AOC3M, VID: V03, SN: INL22262332-A

NAME: "0/2-Optics0/2/0/4", DESCR: "Cisco 100G QSFP28 SM-SR Pluggable Optics
Module"
PID: QSFP-100G-SM-SR, VID: V02, SN: FNS22070HWF

NAME: "0/2-Optics0/2/0/5", DESCR: "Cisco 100G QSFP28 SM-SR Pluggable Optics
Module"
PID: QSFP-100G-SM-SR, VID: V02, SN: SPT2225302D

NAME: "0/2-Optics0/2/0/6", DESCR: "Cisco 100G QSFP28 LR4-S Pluggable Optics
Module"
PID: QSFP-100G-LR4-S, VID: V02, SN: FNS22310Z1X

NAME: "0/2-Optics0/2/0/8", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4, VID: V01, SN: FNS20520R8Z

NAME: "0/2-Optics0/2/0/9", DESCR: "Cisco 100G QSFP28 AOC Pluggable Optics
Module"
PID: QSFP-100G-AOC3M, VID: V03, SN: INL23312282-A

NAME: "0/2-Optics0/2/0/10", DESCR: "Cisco 100G QSFP28 AOC Pluggable Optics
Module"
PID: QSFP-100G-AOC3M, VID: V03, SN: INL23312282-B

NAME: "0/2-Optics0/2/0/11", DESCR: "Cisco 100G QSFP28 LR4-S Pluggable Optics
 Module"
PID: QSFP-100G-LR4-S, VID: V02, SN: FNS23080LKF

NAME: "0/3", DESCR: "Network Convergence System 1004 Filler"
PID: NCS1K4-LC-FILLER, VID: V01, SN: N/A

NAME: "0/RP0", DESCR: "Network Convergence System 1004 Controller"
PID: NCS1K4-CNTLR-K9, VID: V00, SN: CAT2231B069

NAME: "0/SC0", DESCR: "Network Convergence System 1004 Chassis"
PID: NCS1004, VID: V00, SN: CAT2231B192

NAME: "Rack 0", DESCR: "Network Convergence System 1004 Chassis"
PID: NCS1004, VID: V00, SN: CAT2231B192

NAME: "0/FT0", DESCR: "Network Convergence System 1004 Fan"
PID: NCS1K4-FAN, VID: V00, SN: CAT2231B2GL

NAME: "0/FT1", DESCR: "Network Convergence System 1004 Fan"
PID: NCS1K4-FAN, VID: V00, SN: CAT2231B2H4

NAME: "0/FT2", DESCR: "Network Convergence System 1004 Fan"
PID: NCS1K4-FAN, VID: V00, SN: CAT2231B2GW

NAME: "0/PM0", DESCR: "Network Convergence System 1004 AC Power Supply Unit"
PID: NCS1K4-AC-PSU, VID: V00, SN: POG2221CL1V
```

```
NAME: "0/PM1", DESCR: "Network Convergence System 1004 AC Power Supply Unit"
PID: NCS1K4-AC-PSU, VID: V00, SN: POG2221CL04
```

```
RP/0/RP0/CPU0:ios# show inventory
Thu May  7 11:37:33.960 UTC
NAME: "0/0", DESCR: "NCS1K4 12x QSFP28 2 Trunk C-Band DWDM card"
PID: NCS1K4-1.2T-K9    , VID: V00, SN: CAT2237B25A

NAME: "0/0-Optics0/0/0/2", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS2333080E

NAME: "0/0-Optics0/0/0/3", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS23330801

NAME: "0/0-Optics0/0/0/4", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS21140GZK

NAME: "0/0-Optics0/0/0/6", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS233209CN

NAME: "0/0-Optics0/0/0/10", DESCR: "Cisco 40GE QSFP+ LR4 Pluggable Optics
Module"
PID: QSFP-40G-LR4      , VID: V02, SN: FNS23110TYD

NAME: "0/1", DESCR: "NCS1K4 4xDD,8xQSFP28,2xCFP2 DCO OTNXponder"
PID: NCS1K4-OTN-XP     , VID: V00, SN: CAT2352B007

NAME: "0/1-Optics0/1/0/0", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS2333080J

NAME: "0/1-Optics0/1/0/1", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS23330806

NAME: "0/1-Optics0/1/0/2", DESCR: "Cisco 4x10GE QSFP+ MLR Pluggable Optics
Module"
PID: ONS-QSFP-4X10-MLR , VID: V01, SN: INL21010391

NAME: "0/1-Optics0/1/0/4", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics
Module"
PID: QSFP-40G-SR4      , VID: V03, SN: JFQ20332007

NAME: "0/1-Optics0/1/0/5", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics
Module"
PID: QSFP-40G-SR4      , VID: V03, SN: JFQ20332088

NAME: "0/1-Optics0/1/0/6", DESCR: "Cisco 4x10GE QSFP+ MLR Pluggable Optics
Module"
PID: ONS-QSFP-4X10-MLR , VID: V01, SN: INL21010471

NAME: "0/1-Optics0/1/0/7", DESCR: "Cisco 4x10GE QSFP+ MLR Pluggable Optics
Module"
PID: ONS-QSFP-4X10-MLR , VID: V01, SN: INL21010376

NAME: "0/2", DESCR: "NCS1K4 4xDD,8xQSFP28,2xCFP2 DCO OTNXponder"
PID: NCS1K4-OTN-XP     , VID: V00, SN: CAT2352B015

NAME: "0/2-Optics0/2/0/0", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS20360V1R

NAME: "0/2-Optics0/2/0/4", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics
Module"
PID: QSFP-40G-SR4      , VID: V03, SN: JFQ21502017
```

```
NAME: "0/2-Optics0/2/0/5", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics
Module"
PID: QSFP-40G-SR4      , VID: V03, SN: JFQ202120DY

NAME: "0/3", DESCR: "NCS1K4 4xDD,8xQSFP28,2xCFP2 DCO OTNXponder"
PID: NCS1K4-OTN-XP     , VID: V00, SN: CAT2352B00A

NAME: "0/3-Optics0/3/0/0", DESCR: "Cisco QSFP-100G-LR4 Pluggable Optics Module"
PID: ONS-QSFP28-LR4    , VID: V01, SN: FNS23320BS3

NAME: "0/3-Optics0/3/0/4", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics
Module"
PID: QSFP-40G-SR4      , VID: V03, SN: AVP2217S09L

NAME: "0/3-Optics0/3/0/5", DESCR: "Cisco 40GE QSFP+ SR4 Pluggable Optics
Module"
PID: QSFP-40G-SR4      , VID: V03, SN: AVP2107S0RZ

NAME: "0/RP0", DESCR: "Network Convergence System 1004 Controller"
PID: NCS1K4-CNTLR-K9   , VID: V01, SN: CAT2323B0SG

NAME: "0/RP0-SFP-Port", DESCR: "Cisco SFP Pluggable Optics Module"
PID: SFP-GE-S          , VID: V01, SN: FNS15512KVG

NAME: "0/SC0", DESCR: "Network Convergence System 1004 4 line card slots"
PID: NCS1004           , VID: V01, SN: CAT2323B0DC

NAME: "Rack 0", DESCR: "Network Convergence System 1004 4 line card slots"
PID: NCS1004           , VID: V01, SN: CAT2323B0DC

NAME: "0/FT0", DESCR: "Network Convergence System 1004 Fan"
PID: NCS1K4-FAN        , VID: V01, SN: CAT2325B1NW

NAME: "0/FT1", DESCR: "Network Convergence System 1004 Fan"
PID: NCS1K4-FAN        , VID: V01, SN: CAT2324B0Z6

NAME: "0/FT2", DESCR: "Network Convergence System 1004 Fan"
PID: NCS1K4-FAN        , VID: V01, SN: CAT2324B0Z8

NAME: "0/PM0", DESCR: "Network Convergence System 1004 DC Power Supply Unit"
PID: NCS1K4-DC-PSU     , VID: V01, SN: POG2310CT00

NAME: "0/PM1", DESCR: "Network Convergence System 1004 DC Power Supply Unit"
PID: NCS1K4-DC-PSU     , VID: V01, SN: POG2308CT4W
```

2. Enter the **admin** command to access system admin EXEC mode.
3. Use the **show inventory** command in system admin EXEC mode to display the inventory information of all physical entities of NCS 1004.

Example

```
sysadmin-vm:0_RP0# show inventory
Wed Mar  4  05:27:26.231 UTC+00:00

 Name: Rack 0               Descr: Network Convergence System 1004 Chassis
 PID: NCS1004               VID: V00                   SN: CAT2231B192

 Name: 0/0                  Descr: Network Convergence System 1004 Filler
 PID: NCS1K4-LC-FILLER      VID: V01                   SN: N/A
```

```
 Name: 0/1-Optics0/1/0/2     Descr: Cisco 100G QSFP28 AOC Pluggable Optics
Module
 PID: QSFP-100G-AOC3M        VID: V03                   SN: INL22262339-A

 Name: 0/1-Optics0/1/0/4     Descr: Cisco 100GE QSFP28 SR4 Pluggable Optics
Module
 PID: QSFP-100G-SR4-S        VID: V03                   SN: AVF2219S16U

 Name: 0/1-Optics0/1/0/5     Descr: Cisco 100G QSFP28 LR4-S Pluggable Optics
 Module
 PID: QSFP-100G-LR4-S        VID: V02                   SN: JFQ2145701U

 Name: 0/1-Optics0/1/0/6     Descr: Cisco 100GE QSFP28 SR4 Pluggable Optics
Module
 PID: QSFP-100G-SR4-S        VID: ES1                   SN: AVF1925G012

 Name: 0/1-Optics0/1/0/7     Descr: Cisco 100G QSFP28 LR4-S Pluggable Optics
 Module
 PID: QSFP-100G-LR4-S        VID: V02                   SN: JFQ2145706N

 Name: 0/1-Optics0/1/0/8     Descr: Cisco QSFP-100G-LR4 Pluggable Optics
Module
 PID: ONS-QSFP28-LR4         VID: V01                   SN: JFQ19026014

 Name: 0/1-Optics0/1/0/9     Descr: Cisco 100G QSFP28 LR4-S Pluggable Optics
 Module
 PID: QSFP-100G-LR4-S        VID: V02                   SN: OPM220518HS

 Name: 0/1-Optics0/1/0/10    Descr: Cisco 100G QSFP28 SM-SR Pluggable Optics
 Module
 PID: QSFP-100G-SM-SR        VID: V02                   SN: INL21490043

 Name: 0/1-Optics0/1/0/11    Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics
 Module
 PID: QSFP-100G-CWDM4-S      VID: V01                   SN: JFQ211930JL

 Name: 0/1-Optics0/1/0/12    Descr: Cisco 100G QSFP28 CWDM4 Pluggable Optics
 Module
 PID: QSFP-100G-CWDM4-S      VID: V02                   SN: JFQ2210801H

 Name: 0/1                   Descr: NCS1K4 12x QSFP28 2 Trunk C-Band DWDM
card
 PID: NCS1K4-1.2T-K9         VID: V00                   SN: CAT2250B0AE

 Name: 0/2-Optics0/2/0/2     Descr: Cisco 100G QSFP28 AOC Pluggable Optics
Module
 PID: QSFP-100G-AOC3M        VID: V03                   SN: INL22262332-A

 Name: 0/2-Optics0/2/0/4     Descr: Cisco 100G QSFP28 SM-SR Pluggable Optics
 Module
 PID: QSFP-100G-SM-SR        VID: V02                   SN: FNS22070HWF

 Name: 0/2-Optics0/2/0/5     Descr: Cisco 100G QSFP28 SM-SR Pluggable Optics
 Module
 PID: QSFP-100G-SM-SR        VID: V02                   SN: SPT2225302D

 Name: 0/2-Optics0/2/0/6     Descr: Cisco 100G QSFP28 LR4-S Pluggable Optics
 Module
 PID: QSFP-100G-LR4-S        VID: V02                   SN: FNS22310Z1X

Name: 0/2-Optics0/2/0/8     Descr: Cisco QSFP-100G-LR4 Pluggable Optics Module
```

```
 PID: ONS-QSFP28-LR4          VID: V01                    SN: FNS20520R8Z

 Name: 0/2-Optics0/2/0/9      Descr: Cisco 100G QSFP28 AOC Pluggable Optics
Module
 PID: QSFP-100G-AOC3M         VID: V03                    SN: INL23312282-A

 Name: 0/2-Optics0/2/0/10     Descr: Cisco 100G QSFP28 AOC Pluggable Optics
Module
 PID: QSFP-100G-AOC3M         VID: V03                    SN: INL23312282-B

 Name: 0/2-Optics0/2/0/11     Descr: Cisco 100G QSFP28 LR4-S Pluggable Optics
 Module
 PID: QSFP-100G-LR4-S         VID: V02                    SN: FNS23080LKF

 Name: 0/2                    Descr: NCS1K4 12x QSFP28 2 Trunk L-Band DWDM
card
 PID: NCS1K4-1.2TL-K9         VID: V00                    SN: CAT2337B0S4

 Name: 0/3                    Descr: Network Convergence System 1004 Filler
 PID: NCS1K4-LC-FILLER        VID: V01                    SN: N/A

 Name: 0/RP0                 Descr: Network Convergence System 1004 Controller

 PID: NCS1K4-CNTLR-K9         VID: V00                    SN: CAT2231B069

 Name: 0/FT0                  Descr: Network Convergence System 1004 Fan
 PID: NCS1K4-FAN              VID: V00                    SN: CAT2231B2GL

 Name: 0/FT1                  Descr: Network Convergence System 1004 Fan
 PID: NCS1K4-FAN              VID: V00                    SN: CAT2231B2H4

 Name: 0/FT2                  Descr: Network Convergence System 1004 Fan
 PID: NCS1K4-FAN              VID: V00                    SN: CAT2231B2GW

 Name: 0/PM0                 Descr: Network Convergence System 1004 AC Power
 Supply Unit
 PID: NCS1K4-AC-PSU           VID: V00                    SN: POG2221CL1V

 Name: 0/PM1                 Descr: Network Convergence System 1004 AC Power
 Supply Unit
 PID: NCS1K4-AC-PSU           VID: V00                    SN: POG2221CL04

 Name: 0/SC0                  Descr: Network Convergence System 1004 Chassis
 PID: NCS1004                 VID: V00                    SN: CAT2231B192
```

```
sysadmin-vm:0_RP0# show inventory
Thu May  7  11:40:11.150 UTC+00:00

 Name: Rack 0                 Descr: Network Convergence System 1004 4 line
card slots
 PID: NCS1004                 VID: V01                    SN: CAT2323B0DC

 Name: 0/0-Optics0/0/0/2      Descr: Cisco QSFP-100G-LR4 Pluggable Optics
Module
 PID: ONS-QSFP28-LR4          VID: V01                    SN: FNS2333080E

 Name: 0/0-Optics0/0/0/3      Descr: Cisco QSFP-100G-LR4 Pluggable Optics
Module
 PID: ONS-QSFP28-LR4          VID: V01                    SN: FNS23330801

 Name: 0/0-Optics0/0/0/4      Descr: Cisco QSFP-100G-LR4 Pluggable Optics
Module
```

```
 PID: ONS-QSFP28-LR4         VID: V01                   SN: FNS21140GZK

 Name: 0/0-Optics0/0/0/6     Descr: Cisco QSFP-100G-LR4 Pluggable Optics
Module
 PID: ONS-QSFP28-LR4         VID: V01                   SN: FNS233209CN

 Name: 0/0-Optics0/0/0/10    Descr: Cisco 40GE QSFP+ LR4 Pluggable Optics
Module
 PID: QSFP-40G-LR4           VID: V02                   SN: FNS23110TYD

 Name: 0/0                   Descr: NCS1K4 12x QSFP28 2 Trunk C-Band DWDM
card
 PID: NCS1K4-1.2T-K9         VID: V00                   SN: CAT2237B25A

 Name: 0/1-Optics0/1/0/0     Descr: Cisco QSFP-100G-LR4 Pluggable Optics
Module
 PID: ONS-QSFP28-LR4         VID: V01                   SN: FNS2333080J

 Name: 0/1-Optics0/1/0/1     Descr: Cisco QSFP-100G-LR4 Pluggable Optics
Module
 PID: ONS-QSFP28-LR4         VID: V01                   SN: FNS23330806

 Name: 0/1-Optics0/1/0/2     Descr: Cisco 4x10GE QSFP+ MLR Pluggable Optics
Module
 PID: ONS-QSFP-4X10-MLR      VID: V01                   SN: INL21010391

 Name: 0/1-Optics0/1/0/4     Descr: Cisco 40GE QSFP+ SR4 Pluggable Optics
Module
 PID: QSFP-40G-SR4           VID: V03                   SN: JFQ20332007

 Name: 0/1-Optics0/1/0/5     Descr: Cisco 40GE QSFP+ SR4 Pluggable Optics
Module
 PID: QSFP-40G-SR4           VID: V03                   SN: JFQ20332088

 Name: 0/1-Optics0/1/0/6     Descr: Cisco 4x10GE QSFP+ MLR Pluggable Optics
Module
 PID: ONS-QSFP-4X10-MLR      VID: V01                   SN: INL21010471

 Name: 0/1-Optics0/1/0/7     Descr: Cisco 4x10GE QSFP+ MLR Pluggable Optics
Module
 PID: ONS-QSFP-4X10-MLR      VID: V01                   SN: INL21010376

 Name: 0/1                  Descr: NCS1K4 4xDD,8xQSFP28,2xCFP2 DCO OTNXponder

 PID: NCS1K4-OTN-XP          VID: V00                   SN: CAT2352B007

 Name: 0/2-Optics0/2/0/0     Descr: Cisco QSFP-100G-LR4 Pluggable Optics
Module
 PID: ONS-QSFP28-LR4         VID: V01                   SN: FNS20360V1R

Name: 0/2-Optics0/2/0/4     Descr: Cisco 40GE QSFP+ SR4 Pluggable Optics
Module
 PID: QSFP-40G-SR4           VID: V03                   SN: JFQ21502017

 Name: 0/2-Optics0/2/0/5     Descr: Cisco 40GE QSFP+ SR4 Pluggable Optics
Module
 PID: QSFP-40G-SR4           VID: V03                   SN: JFQ202120DY

 Name: 0/2                  Descr: NCS1K4 4xDD,8xQSFP28,2xCFP2 DCO OTNXponder

 PID: NCS1K4-OTN-XP          VID: V00                   SN: CAT2352B015
```

```
 Name: 0/3-Optics0/3/0/0     Descr: Cisco QSFP-100G-LR4 Pluggable Optics
Module
 PID: ONS-QSFP28-LR4         VID: V01                   SN: FNS23320BS3

 Name: 0/3-Optics0/3/0/4     Descr: Cisco 40GE QSFP+ SR4 Pluggable Optics
Module
 PID: QSFP-40G-SR4           VID: V03                   SN: AVP2217S09L

 Name: 0/3-Optics0/3/0/5     Descr: Cisco 40GE QSFP+ SR4 Pluggable Optics
Module
 PID: QSFP-40G-SR4           VID: V03                   SN: AVP2107S0RZ

 Name: 0/3                  Descr: NCS1K4 4xDD,8xQSFP28,2xCFP2 DCO OTNXponder

 PID: NCS1K4-OTN-XP          VID: V00                   SN: CAT2352B00A

 Name: 0/RP0-SFP-Port        Descr: Cisco SFP Pluggable Optics Module
 PID: SFP-GE-S               VID: V01                   SN: FNS15512KVG

 Name: 0/RP0                Descr: Network Convergence System 1004 Controller

 PID: NCS1K4-CNTLR-K9        VID: V01                   SN: CAT2323B0SG

 Name: 0/FT0                 Descr: Network Convergence System 1004 Fan
 PID: NCS1K4-FAN             VID: V01                   SN: CAT2325B1NW

 Name: 0/FT1                 Descr: Network Convergence System 1004 Fan
 PID: NCS1K4-FAN             VID: V01                   SN: CAT2324B0Z6

 Name: 0/FT2                 Descr: Network Convergence System 1004 Fan
 PID: NCS1K4-FAN             VID: V01                   SN: CAT2324B0Z8

 Name: 0/PM0                Descr: Network Convergence System 1004 DC Power
 Supply Unit
 PID: NCS1K4-DC-PSU          VID: V01                   SN: POG2310CT00

 Name: 0/PM1                Descr: Network Convergence System 1004 DC Power
 Supply Unit
 PID: NCS1K4-DC-PSU          VID: V01                   SN: POG2308CT4W

 Name: 0/SC0                 Descr: Network Convergence System 1004 4 line
card slots
 PID: NCS1004                VID: V01                   SN: CAT2323B0DC
```

The significant fields in this output are:

- **PID:** physical model name of the chassis or node
- **VID:** physical hardware revision of the chassis or node
- **SN:** physical serial number of the chassis or node

Check that all expected hardware components are listed in the inventory output. Confirm that the product identifiers, version identifiers, and serial numbers match your hardware configuration.

Verify context

Use this procedure to display and verify the core dump context information of NCS 1004. This helps ensure that unexpected core dumps do not exist in the system.

The **show context** command displays core dump context information of NCS 1004. This information helps you identify system crashes or unexpected core dumps that require attention.

Procedure

1. Use the **show context** command in Cisco IOS XR EXEC mode to display core dump context information of NCS 1004.

   Example

   ```
   RP/0/RP0/CPU0:ios# show context
   Mon Sep 27 17:21:59.219 UTC

   node: node0_RP0_CPU0
   ------------------------------------------------------------------
   No context
   ```

   Note

   The command output is empty during system upgrade.

2. Enter the **admin** command to access system admin EXEC mode.
3. Use the **show context** command in system admin EXEC mode to display core dump context information of NCS 1004.

   Example

   ```
   sysadmin-vm:0_RP0# show context
   Mon Sep  27 17:22:19.351 UTC+00:00
   ***********************************************************
   Location : 0/RP0
   ***********************************************************
   No context
   ```

If the output shows "No context" in both modes, the system does not have core dumps and operates normally.

Verify core files

Use this procedure to check for core files on NCS 1004 to identify any system issues that may require attention.

The **run** command allows you to execute shell commands to check for core files on NCS 1004. Core files show system crashes or process failures and might require investigation.

Procedure

1. Use the **run** command in Cisco IOS XR EXEC mode. Then, navigate to the disk location to check for core files.

Example

```
RP/0/RP0/CPU0:ios# run
Mon Sep 27 17:29:11.163 UTC
[xr-vm_node0_RP0_CPU0:~]$cd /misc/disk1/
[xr-vm_node0_RP0_CPU0:/misc/disk1]$ls -lrt *.tgz
```

This command enters the shell environment and lists any compressed core files (with the .tgz extension) in the /misc/disk1/ directory.

2. Enter the **admin** command to access system admin EXEC mode.
3. Use the **run** command in system admin EXEC mode. Then, navigate to the disk location to check for core files.

Example

```
sysadmin-vm:0_RP0# run
Mon Sep  27 17:31:10.365 UTC+00:00

[sysadmin-vm:0_RP0:~]$cd /misc/disk1/
[sysadmin-vm:0_RP0:~]$ls -lrt *.tgz
```

This command checks for compressed core files in the system admin environment.

If core files are not listed, the system is operating normally without recent crashes or process failures.

4 Create User Profiles and Assign Privileges

Topics:

Provides instructions for configuring user profiles, groups, and access control rules to manage administrative privileges on the NCS 1004. These procedures allow administrators to enforce security policies through command and data restrictions while establishing reliable disaster-recovery credentials for emergency system access.

User profiles and privileges are authentication, authorization, and accounting (AAA) configurations that control access to System Admin configurations on the NCS 1004.

To create user profiles and assign privileges, you must

- create user profiles with usernames and passwords for authentication,
- specify command rules that define which commands users can execute,
- specify data rules that control access to configuration data elements, and
- apply these rules to user groups.

User authentication and authorization

You can use a username and a password for authentication. On successful authentication, you can execute commands and access data elements that are based on the command rules and data rules. Users who are part of a user group have access privileges to the system as defined in the command rules and data rules for that user group.

Use the **show run aaa** command in the System Admin Config mode to view existing AAA configurations.

Topics covered in this chapter

This chapter covers these topics:

- **Create a user profile**: Create individual user accounts with authentication credentials.
- **Create a user group**: Organize users into groups for easier privilege management.
- **Create command rules**: Define which commands users can read and execute.
- **Create data rules**: Control user access to configuration data elements.
- **Change disaster-recovery username and password**: Configure emergency access credentials.

Create a user profile

Use this procedure to create a user profile to provide restricted access to the System Admin console based on assigned privileges.

Users are included in a user group and assigned specific privileges, which provide restricted access to the commands and configurations in the System Admin console.

NCS 1004 supports up to 1,024 user profiles.

> **Note**
>
> System Admin users are different from XR users. Therefore, the username and password of a System Admin user cannot be used to access the XR, and the other way round.

As an XR user, you can access the System Admin by entering the **admin** command in the XR EXEC mode. NCS 1004 does not prompt you to enter any username and password. As an XR user, you have full access to the System Admin console.

Procedure

1. Enter the **admin** command to access System Admin EXEC mode.

   Example

   ```
   RP/0/RP0/CPU0:ios# admin
   ```

2. Enter the **config** command to access System Admin config mode.

   Example

   ```
   sysadmin-vm:0_RP0# config
   ```

3. Enter the **aaa authentication users user** *user_name* command to create a new user and enter user configuration mode.

   Example

   ```
   sysadmin-vm:0_RP0#(config)# aaa authentication users user us1
   ```

4. Enter the **password** *password* command to specify the user password for user authentication.

   Example

   ```
   sysadmin-vm:0_RP0#(config-user-us1)# password pwd1
   ```

5. Enter the **uid** *user_id_value* command to specify the user ID.

Example

```
sysadmin-vm:0_RP0#(config-user-us1)# uid 100
```

Enter any 32-bit integer.

6. Enter the **gid** *group_id_value* command to specify the group ID.

Example

```
sysadmin-vm:0_RP0#(config-user-us1)# gid 50
```

Enter any 32-bit integer.

7. Enter the **ssh_keydir** *ssh_keydir* command to specify the SSH key directory.

Example

```
sysadmin-vm:0_RP0#(config-user-us1)# ssh_keydir dir1
```

Specify any alphanumeric value.

8. Enter the **homedir** *homedir* command to specify the home directory.

Example

```
sysadmin-vm:0_RP0#(config-user-us1)# homedir dir2
```

Specify any alphanumeric value.

9. Enter the **commit** or **end** command to save the configuration.

   The **commit** command saves the configuration changes and remains within the configuration session.

   The **end** command prompts you to take one of these actions:

   - **Yes**: saves configuration changes and exits the configuration session.
   - **No**: exits the configuration session without committing the configuration changes.
   - **Cancel**: remains in the configuration session without committing the configuration changes.

What to do next

After creating a user profile, complete these tasks:

- Create a user group that includes the user profile that is created in this task. See Create a user group on page 75 for details.
- Create command rules that apply to the user group. See Create command rules on page 76 for details.
- Create data rules that apply to the user group. See Create data rules on page 79 for details.

Create a user group

Use this procedure to create a user group to associate command rules and data rules that are enforced on all users in the group.

NCS 1004 supports up to 32 user groups.

Before you begin

Create a user profile on page 73

Procedure

1. Enter the **admin** command to access System Admin EXEC mode.

   Example

   ```
   RP/0/RP0/CPU0:ios# admin
   ```

2. Enter the **config** command to access System Admin config mode.

   Example

   ```
   sysadmin-vm:0_RP0# config
   ```

3. Enter the **aaa authentication groups group** *group_name* command to create a new user group and enter group configuration mode.

   Example

   ```
   sysadmin-vm:0_RP0#(config)# aaa authentication groups group gr1
   ```

   Note

   The system creates the user group 'root-system' automatically when you create the root user. The root user is a member of this group. Users added to this group receive root user permissions.

4. Enter the **users** *user_name* command to specify the name of the user that must be part of the user group.

   Example

   ```
   sysadmin-vm:0_RP0#(config-group-gr1)# users us1
   ```

   You can specify multiple usernames that are enclosed within double quotes. For example, `users "user1 user2 ..."`.

5. Enter the **gid** *group_id_value* command to specify the group ID.

Example

```
sysadmin-vm:0_RP0#(config-group-gr1)# gid 50
```

Enter any 32-bit integer.

6. Enter the **commit** or **end** command to save the configuration.

   The **commit** command saves the configuration changes and remains within the configuration session.

   The **end** command prompts you to take one of these actions:

   - **Yes**: saves configuration changes and exits the configuration session.
   - **No**: exits the configuration session without committing the configuration changes.
   - **Cancel**: remains in the configuration session without committing the configuration changes.

What to do next

After creating a user group, complete these tasks:

- Create command rules. See Create command rules on page 76 for details.
- Create data rules. See Create data rules on page 79 for details.

Create command rules

Use this procedure to create command rules to permit or deny users in a user group from using certain commands.

Use this procedure to create command rules that control which commands users can read and execute.

Command rules are guidelines you can define for a user group to permit or deny access to specific commands. You can associate command rules with a user group and apply them to all users in that group.

You can create a command rule by specifying whether to permit or deny an operation on a command.

This table lists the possible operation and permission combinations.

Operation	Accept permission	Reject permission
Read (R)	Displays command on the CLI when you enter "?" from the CLI	Does not display command on the CLI when you enter "?" from the CLI
Execute (X)	Executes command from the CLI	Cannot execute command from the CLI
Read and execute (RX)	Displays command on the CLI and can execute command	Command is not visible or executable from the CLI

Permissions are set to reject by default.

Each command rule is identified by an associated number. When you apply multiple command rules to a user group, the command rule with a lower number takes precedence. For example, cmdrule5 permits read access, while cmdrule10 rejects read access. When both these command rules are applied to the same user group, users in this group get read access because cmdrule 5 takes precedence.

For example, you can create a command rule to deny read and execute permissions for the **show platform** command.

Before you begin

Create a user group. For details, see Create a user group on page 75.

Procedure

1. Enter the **admin** command to access System Admin EXEC mode.

   Example

   ```
   RP/0/RP0/CPU0:ios# admin
   ```

2. Enter the **config** command to access System Admin config mode.

   Example

   ```
   sysadmin-vm:0_RP0# config
   ```

3. Enter the **aaa authorization cmdrules cmdrule** *command_rule_number* command to create a command rule.

   Example

   ```
   sysadmin-vm:0_RP0#(config)# aaa authorization cmdrules cmdrule 1100
   ```

   This command specifies a numeric value as the command rule number. You can enter a 32-bit integer.

   Important

   Do not use numbers 1-1000 because they are reserved by Cisco.

   This command creates a new command rule if it does not already exist. It then enters the command rule configuration mode. In this example, command rule 1100 is created.

   > **Note**
   >
   > By default, the system creates cmdrule 1 when the root-system user is created. This command rule provides accept permission to read and execute operations for all commands. Therefore, the root user has no restrictions that are imposed on it, unless cmdrule 1 is modified.

4. Enter the **command** *command_name* command to specify the command for which permission is controlled.

   Example

   ```
   sysadmin-vm:0_RP0#(config-cmdrule-1100)# command "show platform"
   ```

   Entering an asterisk (*) for the command applies the rule to all commands.

5. Enter the **ops** command to specify the operation for which permission must be set.

Example

```
sysadmin-vm:0_RP0#(config-cmdrule-1100)# ops rx
```

- `r`: read
- `x`: execute
- `rx`: read and execute

6. Enter the **action {accept | accept_log | reject}** command to specify whether users are permitted or denied the use of the operation.

   Example

   ```
   sysadmin-vm:0_RP0#(config-cmdrule-1100)# action reject
   ```

   This command specifies whether users are permitted or denied the use of the operation:

   - `accept`: Users are permitted to perform the operation.
   - `accept_log`: Users are permitted to perform the operation and every access attempt is logged.
   - `reject`: Users are restricted from performing the operation.

7. Enter the **group** *user_group_name* command to specify the user group to which the command rule applies.

   Example

   ```
   sysadmin-vm:0_RP0#(config-cmdrule-1100)# group gr1
   ```

8. Enter the **context** *connection_type* command to specify the connection type to which this rule applies.

   Example

   ```
   sysadmin-vm:0_RP0#(config-cmdrule-1100)# context *
   ```

   The connection type can be `netconf` (Network Configuration Protocol), `cli` (Command Line Interface), or `xml` (Extensible Markup Language). Entering an asterisk (*) applies the command rule to all connection types.

9. Enter the **commit** or **end** command to save the configuration.

   The **commit** command saves the configuration changes and remains within the configuration session.

   The **end** command prompts you to take one of these actions:

   - **Yes**: saves configuration changes and exits the configuration session.
   - **No**: exits the configuration session without committing the configuration changes.
   - **Cancel**: remains in the configuration session without committing the configuration changes.

What to do next

Create data rules. See Create data rules on page 79 for details.

Create data rules

Use this procedure to create data rules to permit or deny users in a user group from accessing and modifying configuration data elements.

Use this procedure to create data rules that control user access to configuration data elements.

Data rules determine whether users in a user group can access and modify configuration data elements. Data rules are linked to a user group and apply to all users within that group.

Each data rule is identified by an associated number. When a user group has multiple data rules, the rule with the lowest number takes precedence.

To create data rules, you must complete these subtasks:

1. Configure the data rule parameters
2. Apply data rule to user group

Before you begin

Create a user group. For details, see Create a user group on page 75.

Procedure

1. Configure the data rule parameters. See Configure data rule parameters on page 79 for details.
2. Apply data rule to user group. See Apply data rule to user group on page 81 for details.

Configure data rule parameters

Use this procedure to configure the basic parameters for a data rule including the rule number, keypath, operations, and action.

Use this procedure to create a data rule and configure its basic parameters.

This is the first subtask for creating data rules. In this subtask, you create the data rule, specify the data element keypath, define the operations, and set the permission action.

Before you begin

Create a user group. For details, see Create a user group on page 75.

Procedure

1. Enter the **admin** command to access the System Admin EXEC mode.

   Example

   ```
   RP/0/RP0/CPU0:ios# admin
   ```

2. Enter the **config** command to access the System Admin config mode.

   Example

   ```
   sysadmin-vm:0_RP0# config
   ```

3. Enter the **aaa authorization datarules datarule** *data_rule_number* command to create a data rule.

   Example

   ```
   sysadmin-vm:0_RP0#(config)# aaa authorization datarules datarule 1100
   ```

   This command specifies a numeric value as the data rule number. You can enter a 32-bit integer.

   Important

   Do not use numbers between 1 to 1000 because they are reserved by Cisco.

   This command creates a new data rule and enters the data rule configuration mode. In the example, data rule 1100 is created.

   > **Note**
   >
   > The system creates data rule 1 by default when the root-system user is created. This data rule provides accept permission to read, write, and execute operations for all the configuration data. As a result, the root user has no restrictions unless data rule 1 is modified.

4. Enter the **keypath** *keypath* command to specify the key path of the data element.

   Example

   ```
   sysadmin-vm:0_RP0#(config-datarule-1100)# keypath /aaa/disaster-recovery
   ```

   The key path is an expression defining the location of the data element. Entering an asterisk (*) as the keypath makes the command rule apply to all the configuration data.

5. Enter the **ops** *operation* command to specify the operation for which permission is set.

   Example

   ```
   sysadmin-vm:0_RP0#(config-datarule-1100)# ops rw
   ```

   Use these letters to identify various operations:

   - `c`: create
   - `d`: delete
   - `u`: update
   - `w`: write (a combination of create, update, and delete)
   - `r`: read
   - `x`: execute

6. Enter the **action {accept | accept_log | reject}** command to specify whether users may perform the operation.

Example

```
sysadmin-vm:0_RP0#(config-datarule-1100)# action reject
```

This command specifies whether to permit or deny users to perform the operation:

- `accept`: permit users to perform the operation.
- `accept_log`: permit users to perform the operation and log every access attempt.
- `reject`: restrict users from performing the operation.

What to do next

Apply the data rule to a user group. For details, see Apply data rule to user group on page 81.

Apply data rule to user group

Use this procedure to apply the configured data rule to a user group and specify the connection context and namespace.

Use this procedure to apply a data rule to a user group and finalize the configuration.

This is the second subtask for creating data rules. In this subtask, you apply the data rule to a user group. You also specify the connection context and namespace, and then commit the configuration.

Before you begin

Configure data rule parameters. For details, see Configure data rule parameters on page 79.

Procedure

1. Enter the **group** *user_group_name* command to specify the user group to which the data rule applies.

   Example

   ```
   sysadmin-vm:0_RP0#(config-datarule-1100)# group gr1
   ```

   You can also specify multiple group names.

2. Enter the **context** *connection_type* command to specify the connection type to which this rule applies.

   Example

   ```
   sysadmin-vm:0_RP0#(config-datarule-1100)# context *
   ```

   The connection type can be `netconf` (Network Configuration Protocol), `cli` (Command Line Interface), or `xml` (Extensible Markup Language). Enter an asterisk (*), which indicates that the command applies to all connection types.

3. Enter the **namespace** *namespace* command to specify the namespace.

   Example

   ```
   sysadmin-vm:0_RP0#(config-datarule-1100)# namespace *
   ```

   Enter asterisk * to indicate that the data rule is applicable to all the namespace values.

4. Enter the **commit** or **end** command to save the configuration.

   The **commit** command saves the configuration changes and remains within the configuration session.

   The **end** command prompts you to take one of these actions:

   - **Yes**: saves configuration changes and exits the configuration session.
   - **No**: exits the configuration session without committing the configuration changes.
   - **Cancel**: remains in the configuration session without committing the configuration changes.

Change disaster-recovery user name and password

Use this procedure to change the disaster-recovery user name and password to provide emergency access to the System Admin console.

Use this procedure to configure or change the disaster-recovery user name and password for emergency access scenarios.

After you start NCS 1004, define the root-system user name and password. You can use this user name and password for disaster recovery in System Admin mode. You can change the user name and password if needed.

The disaster-recovery user name and password can be used in these scenarios:

- Access the system when the AAA database is corrupted.
- Access the system through the management port when the System Admin console is not working.
- Use the disaster-recovery user name and password in System Admin to create new users if you forget the regular user name and password.

The AAA database is the default source for authentication in System Admin.

> **Note**
>
> You can have only one disaster-recovery user name and password at any time.

Before you begin

Create a user profile. For details, see Create a user profile on page 73.

Procedure

1. Enter the **admin** command to access the System Admin EXEC mode.

   Example

   ```
   RP/0/RP0/CPU0:ios# admin
   ```

2. Enter the **config** command to access the System Admin config mode.

Example

```
sysadmin-vm:0_RP0# config
```

3. Enter the **aaa disaster-recovery username** *username* **password** *password* command to specify the disaster-recovery user name and password.

   Example

   ```
   sysadmin-vm:0_RP0#(config)# aaa disaster-recovery username us1 password pwd1
   ```

   You must select an existing user as the disaster-recovery user.

   In the example, 'us1' is the disaster-recovery user and the password is 'pwd1'. You can enter the password as a plain-text string or as an MD5 digest.

   To use the disaster recovery user name, you must enter it as *username*`@localhost`.

4. Enter the **commit** or **end** command to save the configuration.

   The **commit** command saves the configuration changes and remains within the configuration session.

   The **end** command prompts you to take one of these actions:

   - **Yes**: saves configuration changes and exits the configuration session.
   - **No**: exits the configuration session without committing the configuration changes.
   - **Cancel**: remains in the configuration session without committing the configuration changes.

5 Perform System Upgrade and Install Feature Packages

Topics:

Provides instructions for upgrading Cisco NCS 1004, managing software packages, and performing necessary firmware updates. It also includes compatibility matrices and health check configurations to help users ensure system readiness.

You can execute the system upgrade and package installation processes using the **install** commands on NCS 1004. The processes involve adding and activating the ISO images (*.iso*) and feature packages (*.rpm*) on NCS 1004. You can accesss these files from a network server and then activate on NCS 1004. If the installed package or SMU causes any issue, you can uninstall it.

Note

We recommend that you collect the output of **show tech-support ncs1004** command before performing operations such as a reload or CPU OIR on NCS 1004. The command provides information about the state of the system before reload or before the CPU OIR operation is performed. This information is useful in debugging.

Note

The output of the examples in the procedures is not from the latest software release. The output will change for any explicit references to the current release.

The topics covered in this chapter are:

Software and firmware compatibility matrix

This section provides the FPGA firmware version for each NCS 1004 hardware type across all supported Cisco IOS XR releases, from Release 7.0.0 through Release 26.1.1.

Use these tables to determine which FPGA firmware version corresponds to each hardware type for a given software release. Cross-reference these values before planning a software upgrade or downgrade.

> **Note**
>
> FPGA firmware compatibility is not applicable for NCS1K-FTA.

Table 2: FPGA firmware compatibility for R7.x.x

Hardware type	FPGA	R7.0.0	R7.0.1	R7.1.1	R7.1.2	R7.2.1	R7.3.1	R7.3.2	R7.5.1	R7.5.2	R7
NCS1K4-1.2T-L-K9	LC_CPU_MOD_FW	70.00	70.10	11.49	71.23	72.10	73.10	73.20	75.10	75.20	77
	LC_OPT_MOD_FW	1.06	1.09	1.13	1.14	1.15	1.18	1.25	1.25	1.25	1.3
NCS1K4-1.2T-K9	LC_CPU_MOD_FW	70.00	70.10	11.49	71.23	72.10	73.10	73.20	75.10	75.20	77
	LC_OPT_MOD_FW	1.06	1.09	1.13	1.14	1.15	1.18	1.25	1.25	1.25	1.3
NCS1K4-2-QDD-C-K9	LC_CPU_MOD_FW	NA	NA	NA	NA	NA	73.10	73.20	75.10	75.20	77
	LC_OPT_MOD_FW	NA	NA	NA	NA	NA	1.18	1.26	1.26	1.26	1.3
NCS1K4-2-QDD-CK9L	LC_CPU_MOD_FW	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
	LC_OPT_MOD_FW	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
NCS1K4- 1.2TL-K9	LC_CPU_MOD_FW	NA	NA	NA	NA	72.10	73.10	73.20	75.10	75.20	77
	LC_OPT_MOD_FW	NA	NA	NA	NA	1.15	1.18	1.25	1.25	1.25	1.2

NCS1K4- OTN-XP	LC_CPU_MOD_FW	NA	NA	NA	NA	72.10	73.10	73.20	75.10	75.20	77
	LC_DP_MOD_FW	NA	NA	NA	NA	6.10	10.10	11.10	11.10	12.10	12
	Sub-type 10G-GREY-MXP 40x10G-4x100G-MXP										
	LC_DP_MOD_FW	NA	NA	NA	NA	6.10	10.10	11.10	11.10	11.10	11
	Sub-type 4x100G-MXP-400G-TXP										
	LC_DP_MOD_FW	NA	NA	NA	NA	NA	NA	4.10	3.10	3.10	3.
	LC_DP_MOD_FW	NA	NA	NA	NA	NA	NA	4.10	3.10	4.10	4.
	Sub-type 400GE-TXP-DD										
	LC_DP_MOD_FW	NA	NA	NA	NA	NA	NA	NA	NA	2.10	2.
	Sub-type FC-MXP OTUCn-REGEN										
	LC_DP_MOD_FW	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
	Sub-type 2x100GE-TXP-MXP										
	LC_CFP2_PORT_0	NA	NA	NA	NA	NA	1.10	1.52	1.52	1.60	1.6
	LC_CFP2_PORT_0	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
	Sub-type 2x100GE-TXP-MXP										
	LC_CFP2_PORT_1	NA	NA	NA	NA	NA	1.10	1.52	1.52	1.60	1.6
	LC_QSFPDD_PORT_9	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	61.2013	61.2221	61.
LC_QSFPDD_PORT_11	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	61.2013	61.2221	61.2221	61.

NCS1K4-QXP-K9	LC_CPU_MOD_FW	NA	NA	NA	NA	NA	NA	NA	NA	NA	77
	LC_QSFPDD_PORT_0	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	61.
	LC_QSFPDD_PORT_2	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	61.
	LC_QSFPDD_PORT_4	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	61.
	LC_QSFPDD_PORT_6	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	61.
	LC_QSFPDD_PORT_8	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	61.
	LC_QSFPDD_PORT_10	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	61.
	LC_QSFPDD_PORT_0	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.
	LC_QSFPDD_PORT_10	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.
	LC_QSFPDD_PORT_14	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.
	LC_QSFPDD_PORT_4	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.13011	70.
NCS1004	BP_FPGA	1.25	1.25	1.25	1.25	1.25	1.25	1.25	1.25	1.25	1.2
	XGE_FLASH	18.04	18.04	18.04	18.04	18.04	18.04	18.04	18.04	18.04	18

Table 3: FPGA firmware compatibility for controller card for R7.x.x

Hardware type	FPGA	R7.0.0	R7.0.1	R7.1.1	R7.1.2	R7.2.1	R7.3.1	R7.3.2	R7.5.1	R7.5.2	R7.7.1
NCS1K4-CNTLR-K9	BIOS	4.10	4.20	4.20	4.30	4.30	4.70	5.06	5.30	5.50	5.80
	CSB_IMG	0.200	0.200	0.200	0.200	0.200	0.200	0.200	0.200	0.200	0.200
	TAM_FW	36.08	36.08	36.08	36.08	36.08	36.08	36.08	36.08	36.08	36.08
	CPU_FPGA	1.14	1.14	1.14	1.14	1.14	1.14	1.14	1.14	1.14	1.14
	CPU_SSD	NA	NA	NA	NA	NA	NA	NA	NA	75.00	75.00
	POWMAN_CFG	NA	NA	NA	NA	NA	NA	NA	NA	3.40	3.40
NCS1K4-CNTLR-B-K9	CPU_SSD	NA	NA	NA	NA	NA	NA	NA	NA	NA	1.00

Table 4: FPGA firmware compatibility for power supply unit for R7.x.x

Hardware type	FPGA	R7.0.0	R7.0.1	R7.1.1	R7.1.2	R7.2.1	R7.3.1	R7.3.2	R7.5.1	R7.5.2	R7.7.1	R7.8.1
NCS1K4-2KW-AC	PO-PriMCU	2.70	2.70	2.70	2.70	2.70	2.70	2.70	2.70	2.70	2.70	2.70
NCS1K4-AC-PSU	PO-PriMCU	2.70	2.70	2.70	2.70	2.70	2.70	2.70	2.70	2.70	2.70	2.70
NCS1K4-DC-PSU	PO-PriMCU	1.12	1.12	1.12	1.12	1.12	1.12	1.12	1.12	1.12	1.12	1.12

Table 5: FPGA firmware compatibility for R24.x.x, R25.x.x, and R26.x.x

Hardware type	FPGA	R24.1.1	R24.3.1	R25.3.1	R25.4.1	R26.1.1
NCS1K4-1.2T-L-K9	LC_CPU_MOD_FW	241.10	243.10	253.10	254.100	261.1
	LC_OPT_MOD_FW	1.38	1.38	1.38	1.38	1.38

NCS1K4-1.2T-K9	LC_CPU_MOD_FW	241.10	243.10	253.10	254.100	261.1
	LC_OPT_MOD_FW	1.38	1.38	1.38	1.38	1.38
NCS1K4-2-QDD-C-K9	LC_CPU_MOD_FW	241.10	243.10	253.10	254.100	261.1
	LC_OPT_MOD_FW	1.38	1.38	1.38	1.38	1.38
NCS1K4-2-QDD-CK9L	LC_CPU_MOD_FW	241.10	243.10	253.10	254.100	261.1
	LC_OPT_MOD_FW	1.38	1.38	1.38	1.38	1.38
NCS1K4-1.2TL-K9	LC_CPU_MOD_FW	241.10	243.10	253.10	254.100	261.1
	LC_OPT_MOD_FW	1.38	1.38	1.38	1.38	1.38
NCS1K4-OTN-XP	LC_CPU_MOD_FW	241.10	243.10	253.10	254.100	261.1
	LC_DP_MOD_FW	3.10	15.10	17.10	17.10	17.10
	Sub-type					
	10G-GREY-MXP					
	40x10G-4x100G-MXP					
	LC_DP_MOD_FW	12.10	12.10	14.10	14.10	14.10
	Sub-type					
	4x100G-MXP-400G-TXP					
	LC_DP_MOD_FW	12.10	3.10	3.10	3.10	3.10
	LC_DP_MOD_FW	4.10	4.10	4.10	4.10	4.10
	Sub-type					
	400GE-TXP-DD					
	LC_DP_MOD_FW	5.10	5.10	7.10	7.10	7.10
	Sub-type					
	FC-MXP					
	OTUCn-REGEN					
	LC_DP_MOD_FW	1.10	1.10	1.10	1.10	1.10
	Sub-type					
	2x100GE-TXP-MXP					
	LC_CFP2_PORT_0	1.46	1.80	1.80	1.80	1.46
	LC_CFP2_PORT_0	38.27397	38.27397	38.27397	38.27397	38.27397
	Sub-type					
	2x100GE-TXP-MXP					
	LC_CFP2_PORT_1	1.46	1.46	1.46	1.46	1.46
	LC_QSFPDD_PORT_9	61.2332	61.2332	61.2332	61.2332	61.2332
	LC_QSFPDD_PORT_11	61.2332	61.2332	61.2332	61.2332	61.2332

NCS1K4-QXP-K9	LC_CPU_MOD_FW	241.10	243.10	243.10	243.10	261.10
	LC_QSFPDD_PORT_0	70.13011	70.13011	70.13011	70.13011	70.13011
	LC_QSFPDD_PORT_2	70.13011	70.13011	70.13011	70.13011	70.13011
	LC_QSFPDD_PORT_4	61.2332	70.13011	70.13011	70.13011	70.13011
	LC_QSFPDD_PORT_6	61.2332	61.2332	61.2332	61.2332	70.13011
	LC_QSFPDD_PORT_8	61.2332	61.2332	61.2332	61.2332	70.13011
	LC_QSFPDD_PORT_10	61.2332	61.2332	61.2332	61.2332	70.13011
	LC_QSFPDD_PORT_0	70.13011	70.13011	70.13011	70.13011	70.13011
	LC_QSFPDD_PORT_10	70.13011	70.13011	70.13011	70.13011	70.13011
	LC_QSFPDD_PORT_14	70.13011	70.13011	70.13011	70.13011	70.13011
	LC_QSFPDD_PORT_4	70.13011	70.13011	70.13011	70.13011	70.13011
NCS1004	BP_FPGA	1.25	1.25	1.25	1.25	1.25
	XGE_FLASH	18.04	18.04	18.04	18.04	18.04

Table 6: FPGA firmware compatibility for controller card for R24.x.x, R25.x.x, and R26.x.x

Hardware type	FPGA	R24.1.1	R24.3.1	R25.3.1	R25.4.1	R26.1.1
NCS1K4-CNTLR-K9	BIOS	6.20	6.40	7.00	7.20	7.20
	CSB_IMG	0.200	0.200	0.200	0.200	0.200
	TAM_FW	36.08	36.08	36.08	36.08	36.08
	CPU_FPGA	1.14	1.14	1.14	1.14	1.14
	CPU_SSD	75.00	75.00	75.00	75.00	120
	POWMAN_CFG	3.40	3.40	3.40	3.40	3.40
NCS1K4-CNTLR-B-K9	CPU_SSD	1.00	1.00	1.00	1.00	1.00

Table 7: FPGA firmware compatibility for power supply unit for R24.x.x , R25.x.x,and R26.x.x

Hardware type	FPGA	R24.1.1	R24.3.1	R25.3.1	R25.4.1	R26.1.1
NCS1K4-2KW-AC	PO-PriMCU	2.70	2.70	2.70	2.70	2.70
NCS1K4-AC-PSU	PO-PriMCU	2.70	2.70	2.70	2.70	2.70
NCS1K4-DC-PSU	PO-PriMCU	1.12	1.12	1.12	1.12	1.12

System upgrade

This section explains the concept of system upgrades for NCS 1004, including their key functions and considerations.

A system upgrade is a maintenance procedure that

- replaces the Cisco IOS XR operating system image with a newer version,

- upgrades both the XR and the System Admin operating systems simultaneously, and
- initiates the process from XR mode using **install** commands.

System upgrade installs the base package, which includes the Cisco IOS XR Core Bundle and Manageability Package. Install the ISO image using **install** commands.

Additional reference information

For more information on upgrading the system and the RPMs, see *Cisco IOS XR Flexible Packaging Configuration Guide for Cisco NCS 1000 Series*.

Note

- Software downgrade from Release 7.2.1 to Release 7.1.1 affects traffic.
- Before you upgrade from Release 7.3.1 and later, or downgrade to Release 7.3.1 and earlier, configure minimum and maximum values for chromatic dispersion (CD) on the trunk optical controller of the OTN-XP card to maintain traffic flow. Use the **controller optics** *R/S/I/P* [**cd-max** *cd-max* | **cd-min** *cd-min*] command to configure minimum and maximum chromatic dispersion values. See Command Reference for Cisco NCS 1004 for the range of CD values.

Note

From Release 25.4.1, to run the **install replace** command for a software upgrade, if a public IP address is connected to management port 1, you must configure **linux networking** for management port 1.

This is a sample Linux networking configuration on management port 1.

```
linux networking
 vrf default
  address-family ipv4
   default-route software-forwarding
   source-hint management-route interface MgmtEth0/RP0/CPU0/1
   source-hint default-route interface MgmtEth0/RP0/CPU0/1
 !
```

View supported software upgrade or downgrade versions

Use this procedure to verify supported upgrade and downgrade paths on NCS 1004 using the **show install upgrade-matrix** commands, and to configure pre and post-upgrade installation health checks.

Determine which release versions NCS 1004 supports for upgrade or downgrade from the currently running release, validate a specific source-to-target release path before attempting the upgrade, and configure health checks to automatically verify system readiness before and after installation.

Table 8: Feature History Table

Feature Name	Release Information	Description
Supported Software Upgrade or Downgrade IOS XR Versions	Cisco IOS XR Release 7.5.1	You can determine whether a software version can be upgraded or downgraded to another version using this functionality. Before an actual upgrade or downgrade process, you can also view the hardware or software limitations that could cause the upgrade or downgrade to fail. This feature helps you plan successful software upgrades or downgrades. This feature introduces the **show install upgrade-matrix** command.

Table 9: Feature History

Feature Name	Release Information	Feature Description
Pre and Post-Upgrade Install Health Checks using Profile	Cisco IOS XR Release 7.8.1	This feature allows you to create profiles that define the actions performed during pre and post-upgrade installation checks. You can configure the default actions for: • Pre-upgrade check failure • Upgrade failure • Revert after post-installation check failure

Use the **show install upgrade-matrix** command to list all releases from which the currently running release can be reached by a direct upgrade or downgrade.

Use the **show install upgrade-matrix from** *release-version* command to validate whether a specific release-to-release path is supported. The command output shows YES if the path is supported and NO if it is not.

Note

The **show install upgrade-matrix** command is available from Release 7.9.1. The **from** keyword option is available from Release 7.10.1.

Procedure

1. Use the **show install upgrade-matrix** command to list all supported upgrade and downgrade paths from the currently running release.

Example

```
RP/0/RP0/CPU0:ios#show install upgrade-matrix
Fri Aug 18 11:25:15.571 UTC
Upgrade Matrix for ncs1004-mini-x-7.10.1 image:
    From Release    Upgrade    Downgrade
    7.9.1             YES       NO
    7.10.1            YES       YES
    24.1.1            NO        YES
```

2. Use the **show install upgrade-matrix from** *release-version* command to validate whether a specific release-to-release upgrade or downgrade path is supported.

Example

```
RP/0/RP0/CPU0:ios#show install upgrade-matrix from 7.9.1
Fri Aug 18 11:27:50.215 UTC
From Release 7.9.1:
    To 7.10.1:  Upgrade supported: YES
                Downgrade supported: NO
```

The command output shows YES if the path is supported and NO if it is not.

You have verified the supported upgrade and downgrade paths for NCS 1004.

List all supported paths

This example shows the supported upgrade and downgrade paths for the currently running release.

```
RP/0/RP0/CPU0:ios#show install upgrade-matrix
Fri Aug 18 11:25:15.571 UTC
Upgrade Matrix for ncs1004-mini-x-7.10.1 image:
    From Release    Upgrade    Downgrade
    7.9.1             YES       NO
    7.10.1            YES       YES
    24.1.1            NO        YES
```

Validate a specific path

This example validates whether an upgrade from Release 7.9.1 to the current running release is supported.

```
RP/0/RP0/CPU0:ios#show install upgrade-matrix from 7.9.1
Fri Aug 18 11:27:50.215 UTC
From Release 7.9.1:
    To 7.10.1:  Upgrade supported: YES
                Downgrade supported: NO
```

show install upgrade-matrix from (unsupported path)

This example shows the output when the specified upgrade path is not supported.

```
RP/0/RP0/CPU0:ios#show install upgrade-matrix from 7.6.1
Fri Aug 18 11:30:22.415 UTC
From Release 7.6.1:
    To 7.10.1:  Upgrade supported: NO
                Downgrade supported: NO
Info: Direct upgrade or downgrade between 7.6.1 and 7.10.1 is not supported.
      Please upgrade via intermediate release.
```

show install upgrade-matrix for Release 24.x.x

```
RP/0/RP0/CPU0:ios#show install upgrade-matrix
Fri Aug 18 11:25:15.571 UTC
Upgrade Matrix for ncs1004-mini-x-24.1.1 image:
    From Release    Upgrade    Downgrade
    7.10.1            YES       NO
    24.1.1            YES       YES
    24.2.1            NO        YES
```

Software upgrade and downgrade matrix

This section lists the supported upgrade and downgrade paths for NCS 1004 across releases from Release 7.0.0 through Release 26.1.1, for use when planning a software upgrade or downgrade.

Use this table to determine the release versions of NCS 1004 that support direct upgrade or downgrade. Cross-reference the source and target release versions before planning a software upgrade or downgrade.

Table 10: NCS 1004 software upgrade and downgrade matrix

Upgrade Path		Downgrade Path	
Source Release	**Destination Release**	**Source Release**	**Destination Release**
• R7.3.2 • R7.5.1 • R7.5.2 • R7.7.1 • R7.8.1 • R7.9.1	R7.10.1	R7.10.1	• R7.9.1 • R7.8.1 • R7.7.1 • R7.5.2 • R7.5.1 • R7.3.2
• R7.8.1 • R7.9.1 • R7.10.1 • R24.1.1	R24.3.1	R24.3.1	• R24.1.1 • R7.10.1 • R7.9.1 • R7.8.1
• R25.3.1 • R24.3.1 • R24.1.1 • R71.0.1 • R7.9.1 • R7.8.1 • R7.7.1	R25.4.1	R25.4.1	• R25.3.1 • R24.3.1 • R24.1.1 • R71.0.1 • R7.9.1 • R7.8.1 • R7.7.1

Upgrade Path		Downgrade Path	
Source Release	**Destination Release**	**Source Release**	**Destination Release**
• R25.4.1 • R25.3.1 • R24.3.1 • R24.1.1 • R7.10.1 • R7.9.1 • R7.8.1 • R7.3.2	R26.1.1	R26.1.1	• R25.4.1 • R25.3.1 • R24.3.1 • R24.1.1 • R7.10.1 • R7.9.1 • R7.8.1 • R7.3.2

NCS 1004 software packages

This section explains how Cisco IOS XR software is packaged on NCS 1004, the package naming convention, and the standard packages available for installation.

A package is a software component that

- installs a specific set of NCS 1004 features or functions,
- follows the naming convention `<platform>-<pkg>-<pkg version>-<release version>.<architecture>.rpm`, and
- can be installed individually or as part of an SMU patch.

Standard packages for NCS 1004

This table lists the standard packages available for NCS 1004.

Table 11: Standard packages for NCS 1004

Feature set	Filename	Description
Composite Package		
Cisco IOS XR Core Bundle + Manageability Package	ncs1004-mini-x-24.1.1.iso	Contains required core packages, such as the operating system, Admin, Base, Forwarding, SNMP Agent, FPD, Alarm Correlation, NETCONF-YANG, Telemetry, XML parser, and HTTP server packages.
Individually Installable Optional Packages		
Cisco IOS XR Security Package	ncs1004-k9sec-1.0.0.0-r2411.x86_64.rpm	Provides support for encryption, decryption, IP Security (IPsec), Secure Socket Layer (SSL), and public key infrastructure (PKI).

Feature set	Filename	Description
OpenROADM	ncs1004-tp-sw-1.0.0.0-r2411.x86_64.rpm	To configure OpenROADM, install the ncs1004-tp-sw-1.0.0.0-r732.rpm package.
OTN-XP	ncs1004-sysadmin-otn-xp-dp-24.1.1-r2411.x86_64.rpm	Install this package on the OTN-XP card to bring up the system with the OTN-XP card.
Pre and post-upgrade installation health checks	ncs1004-healthcheck-1.0.0.0-r2411.x86_64.rpm	Install this package to configure health checks before and after upgrades.

Install and uninstall workflow

This section explains the ordered sequence of install operations—add, activate, and commit—and the reverse sequence used to uninstall packages on NCS 1004.

The install and uninstall workflow is an ordered sequence of operations that

- adds, activates, and commits packages during installation, and
- deactivates, removes, and commits packages during uninstallation.

Related procedures

To install a package, see Install packages. To uninstall a package, see Uninstall packages. Each topic includes a flowchart depicting the workflow for that operation.

Install packages

Use this procedure to add an ISO image, RPM packages, or SMUs to the NCS 1004 repository and activate them to perform a system upgrade or feature installation.

Complete this task to upgrade the system or install a patch. You can perform the system upgrade using an ISO image file and the patch installation using packages and SMUs. This task also enables you to install .tar files. The .tar file contains multiple packages and SMUs merged into a single file. A single .tar file can contain up to sixty four individual files. The packaging format defines one RPM per component, without dependency on card type.

Note

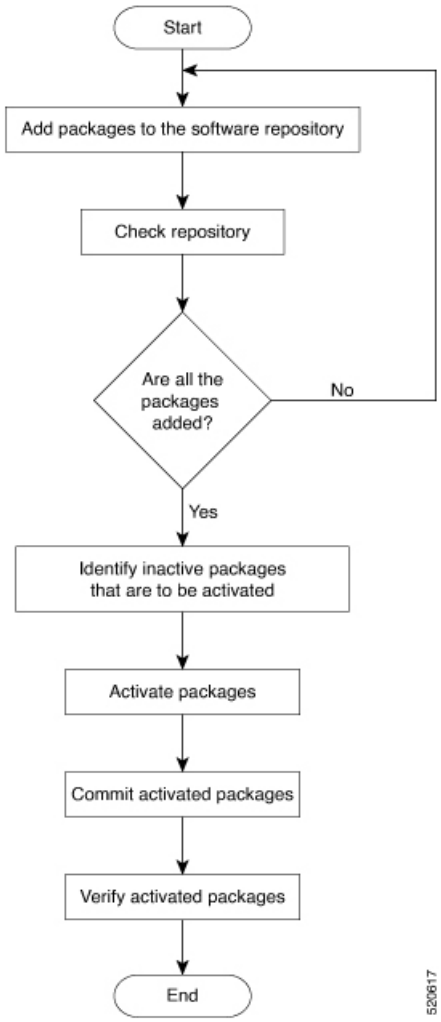
To install a System Admin package or an XR package, run the **install** commands in System Admin EXEC mode or XR EXEC mode respectively. All the **install** commands are applicable in both these modes.

Note

Two FPDs (Field-Programmable Devices) are available for the OTN-XP card: LC_CPU_MOD_FW and LC_DP_MOD_FW. LC_CPU_MOD_FW is available as part of the boot ISO image. Install the ncs1004-sysadmin-otn-xp-dp-*.rpm data path FPD package on the OTN-XP line card using this procedure to bring up the system with the OTN-XP card.

This flowchart demonstrates the process for installing the package.

Figure 1: Installing packages workflow



Before you begin

- Configure and connect to the management port. You can access the installable file through the management port. For information about configuring the management port, see Configure the management interface.
- Copy the package to be installed either to the NCS 1004 hard disk or to a network server that NCS 1004 can access.
- When the ncs1004-k9sec package is not installed, use only FTP or TFTP to copy files or during the **install add** operation.

Procedure

1. Use one of these commands to add the package to the repository.
   - **install add source** *<tftp transfer protocol>/package_path filename1 filename2 ...*
   - **install add source** *<ftp or sftp transfer protocol>//user@server:/package_path filename1 filename2 ...*

   Example

   ```
   RP/0/RP0/CPU0:ios#install add source harddisk: ncs1004-mini-x-7.2.1
   ncs1004-k9sec-2.1.0.0-r721.x86_64.rpm
   ```

   ```
   Thu Feb  7 11:10:51.867 UTC
   Feb 07 11:10:53 Install operation 25 started by root:
    install add source harddisk: ncs1004-mini-x-7.2.1
   ncs1004-k9sec-2.1.0.0-r721.x86_64.rpm
   Feb 07 11:10:55 Install operation will continue in the background
   Thu Feb  7 11:10:51 Install operation 25 finished successfully
   ```

   Add the respective packages as appropriate. This command unpacks software files from the package and adds them to the software repository. The operation runs in asynchronous mode – the **install add** command runs in the background and the EXEC prompt is returned immediately.

   Note

   Install operation over IPv6 is not supported.

2. (Optional) Use the **show install request** command to display the operation ID of the add operation and its status.

   Example

   ```
   RP/0/RP0/CPU0:ios#show install request
   ```

   You can use the operation ID later to run the **activate** command.

3. Use the **show install repository** command to display packages added to the repository.

   Example

   ```
   RP/0/RP0/CPU0:ios#show install repository
   ```

   ```
   6 package(s) in XR repository:
       ncs1004-mini-x-7.0.1
       ncs1004-mini-x-7.2.1
   ```

```
    ncs1004-mpls-2.0.0.0-r711
    ncs1004-k9sec-2.1.0.0-r721.x86_64
    ncs1004-xr-7.2.1
    ncs1004-mpls-te-rsvp-2.1.0.0-r711
```

Packages appear only after the **install add** operation is complete.

4. Use the **show install inactive** command to display inactive packages present in the repository.

   Example

```
RP/0/RP0/CPU0:ios#show install inactive
```

```
6 inactive package(s) found:
    ncs1004-mini-x-7.0.1
    ncs1004-mini-x-7.2.1
    ncs1004-mpls-2.0.0.0-r711
    ncs1004-k9sec-2.1.0.0-r721.x86_64
    ncs1004-xr-7.2.1
    ncs1004-mpls-te-rsvp-2.1.0.0-r711
```

   You can activate only inactive packages.

5. Use the **install activate** *package_name* command to set the package configurations to active on NCS 1004.

   Example

```
RP/0/RP0/CPU0:ios#install activate ncs1004-mini-x-7.2.1
ncs1004-k9sec-2.1.0.0-r721.x86_64
```

```
Thu Feb  7 11:25:09.229 UTC
Feb 07 11:25:10 Install operation 26 started by root:
  install activate pkg ncs1004-mini-x-7.2.1 ncs1004-k9sec-2.1.0.0-r721.x86_64
Feb 07 11:25:10 Package list:
Feb 07 11:25:10     ncs1004-mini-x-7.2.1 ncs1004-k9sec-2.1.0.0-r721.x86_64
Feb 07 11:25:17 Install operation will continue in the background
Feb 07 11:25:10 Install operation 26 finished successfully
```

   New features and software fixes take effect. This operation runs in asynchronous mode. The **install activate** command runs in the background, and the EXEC prompt is returned.

Note

To activate an RPM of a lower version after a higher version is already active, use the force option. You can do this in two ways:

- Add the RPM with the lower version to the repository and then force the activation:

```
install add source repository ncs1004-xr-7.2.1
install activate ncs1004-xr-7.2.1 force
```

- Use the **install update** command:

```
install update source repository ncs1004-xr-7.2.1
```

If you use the operation ID, all the packages added in the specified operation are activated together. For example, if five packages are added in operation 8, running **install activate id 8** activates all five packages together.

6. Use the **show install active** command to display packages that are active.

Example

```
RP/0/RP0/CPU0:ios#show install active
```

```
Mon Mar 11 07:31:12.302 UTC
Node 0/RP0/CPU0 [RP]
  Boot Partition: xr_lv19
  Active Packages: 5
    ncs1004-mini-x-7.2.1
    ncs1004-mpls-2.0.0.0-r711
    ncs1004-k9sec-2.1.0.0-r721.x86_64
    ncs1004-xr-7.2.1
    ncs1004-mpls-te-rsvp-2.1.0.0-r711
```

7. Use the **install commit system** command to commit the newly active software.

Example

```
RP/0/RP0/CPU0:ios#install commit system
```

```
Thu Feb  7 11:34:04.207 UTC
Feb 07 11:34:05 Install operation 27 started by root:
  install commit system
Feb 07 11:34:06 Install operation will continue in the background
Feb 07 11:34:19 Install operation 27 finished successfully
```

> **Note**
>
> If you perform a manual or automatic system reload without completing the transaction with the **install commit** command during a system update, the system reverts to its state prior to the install transaction, including any configuration changes. Only the log is preserved for debugging. This action clears all configuration rollback points. You cannot roll back to or view any commits made before the install rollback event. New commits made after the install rollback event start from commit ID "1000000001".

Table 12: Install packages: related commands

Related command	Purpose
show install log	Displays the log information for the install process. Use this information for troubleshooting in case of installation failure.
show install package	Displays the details of the packages added to the repository. Use this command to identify individual components of a package.
install prepare	Makes preactivation checks on an inactive package to prepare it for activation.
show install prepare	Displays the list of packages that have been prepared and are ready for activation.

The packages are installed, activated, and committed on NCS 1004. New features and fixes become available, and the repository displays the active and inactive packages.

What to do next

- After performing a system upgrade, upgrade FPDs using the **upgrade hw-module location all fpd all** command from Cisco IOS XR mode. Monitor the FPD upgrade progress using the **show hw-module fpd** command.
- Reload NCS 1004 if BIOS, BP_SSD, and CPU_SSD are in RLOAD REQ state. Use the **hw-module location 0/RP0 reload** command.
- Verify the installation using the **install verify packages** command.
- Uninstall the packages or SMUs if their installation causes issues on NCS 1004. See Uninstall packages.

> **Note**
>
> ISO images cannot be uninstalled. However, you can perform a system downgrade by installing an older ISO version.

Install prepared packages

Use this procedure to prepare packages before activation, which detects corrupted files early and reduces downtime during the activation phase on NCS 1004.

Complete this task to upgrade the system and install packages by using the prepare operation.

You can perform a system upgrade or feature upgrade by activating the ISO image file, packages, and SMUs. It is possible to prepare these installable files before activation. During the preparation phase, preactivation checks are made. The system also loads the components of the installable files onto the NCS 1004 setup. The preparation process runs in the background, and NCS 1004 is fully usable during this time. When the prepare phase completes, the prepared files are activated instantaneously.

The advantages of preparing before activation are:

- If the installable file is corrupted, the preparation process fails, providing an early warning. A corrupted file that is activated directly may cause NCS 1004 to malfunction.
- Directly activating an ISO image takes considerable time, and NCS 1004 is unavailable during this period. If you prepare the image first, it runs asynchronously. When you activate the prepared image, activation takes less time, which reduces downtime.

Procedure

1. Add the required ISO image and packages to the repository.
   For more information, see Install packages.
2. Use the **show install repository** command to verify that the required installable files are available in the repository.

   Example

   ```
   RP/0/RP0/CPU0:ios#show install repository
   Fri Mar 15 11:31:53.352 IST
   12 package(s) in XR repository:
       ncs1004-mpls-1.0.0.0-r241146I.x86_64
       ncs1004-k9sec-1.0.0.0-r2411.x86_64
       ncs1004-xr-24.1.1.46I
       ncs1004-healthcheck-1.0.0.0-r241146I.x86_64
       ncs1004-mpls-te-rsvp-1.0.0.0-r2411.x86_64
       ncs1004-xr-24.1.1
       ncs1004-mini-x-24.1.1.46I
       ncs1004-mpls-1.0.0.0-r2411.x86_64
       ncs1004-mini-x-24.1.1
       ncs1004-healthcheck-1.0.0.0-r2411.x86_64
       ncs1004-k9sec-1.0.0.0-r241146I.x86_64
       ncs1004-mpls-te-rsvp-1.0.0.0-r241146I.x86_64
   ```

   Packages appear only after the **install add** operation is complete.
3. Use one of these commands to prepare the packages:
   - **install prepare** *package_name*
   - **install prepare id** *operation_id*

   Example

   ```
   RP/0/RP0/CPU0:ios#install prepare ncs1004-mini-x-7.2.1
   ncs1004-k9sec-2.1.0.0-r721.x86_64
   ```

   Or

   ```
   RP/0/RP0/CPU0:ios#install prepare id 8
   ```

   The preparation process runs in asynchronous mode. The **install prepare** command runs in the background and the EXEC prompt is returned.

If you use the operation ID, all packages added in the specified operation are prepared together. For example, if five packages are added in operation 8, running **install prepare id 8** prepares all five packages together.

4. Use the **show install prepare** command to verify that all the required packages appear in the output.

   Example

   ```
   RP/0/RP0/CPU0:ios#show install prepare
   ```

5. Use the **install activate** *package_name* command to activate the prepared packages.

   Example

   ```
   RP/0/RP0/CPU0:ios#install activate ncs1004-mini-x-7.2.1
   ncs1004-k9sec-2.1.0.0-r721.x86_64
   ```

   All prepared packages are activated together. This action applies the package configurations on NCS 1004.

6. Use the **show install active** command to display the packages that are active.
7. Use the **install commit system** command to commit the recently activated software.

   Example

   ```
   RP/0/RP0/CPU0:ios#install commit system
   ```

Table 13: Install prepared packages: related commands

Related command	Purpose
show install log	Displays the log information for the install process. Use this information for troubleshooting in case of install failure.
show install package	Displays the details of the packages added to the repository. Use this command to identify individual components of a package.
install prepare clean	Clears the prepare operation and removes the packages from the prepared state.

Prepared packages are activated immediately with minimal downtime. The system detects any corrupted files before activation to prevent issues.

What to do next

- After performing a system upgrade, upgrade FPDs using the **upgrade hw-module location all fpd all** command from Cisco IOS XR mode. Monitor the FPD upgrade progress using the **show hw-module fpd** command.
- Reload NCS 1004 if BIOS, BP_SSD, and CPU_SSD are in RLOAD REQ state. Use the **hw-module location 0/RP0 reload** command.
- Verify the installation using the **install verify packages** command.
- Uninstall the packages or SMUs if their installation causes issues on NCS 1004. See Uninstall packages.

> **Note**
>
> ISO images cannot be uninstalled. However, you can perform a system downgrade by installing an older ISO version.

Uninstall packages

Use this procedure to deactivate and remove a package from the NCS 1004 software repository when you need to revert a feature installation or roll back a patch.

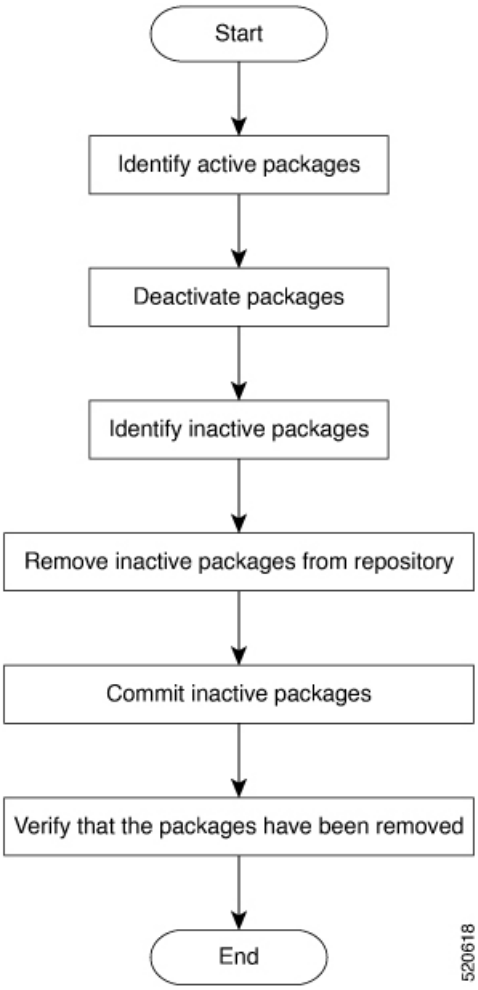
Complete this task to uninstall a package when you want to remove features or revert a patch.

Packages added in XR mode cannot be uninstalled from System Admin mode, and the other way round.

> **Note**
>
> Installed ISO images cannot be uninstalled. Additionally, kernel SMUs that install a third-party SMU on host, XR mode, and System Admin mode cannot be uninstalled. However, a subsequent installation of an ISO image or kernel SMU overwrites the existing installation.

This flowchart demonstrates how to uninstall a package.

Figure 2: Uninstalling packages workflow



Procedure

1. Use the **show install active** command to display the active packages.

   Example

   ```
   RP/0/RP0/CPU0:ios#show install active
   Mon Mar 11 07:31:12.302 UTC
   Node 0/RP0/CPU0 [RP]
     Boot Partition: xr_lv19
     Active Packages: 5
       ncs1004-mini-x-7.2.1
       ncs1004-mpls-2.0.0.0-r711
       ncs1004-k9sec-2.1.0.0-r721.x86_64
       ncs1004-xr-7.1.1
       ncs1004-mpls-te-rsvp-2.1.0.0-r711
   ```

   You can deactivate only active packages.

2. Use one of these commands to deactivate the package:

   - **install deactivate** *package_name*
   - **install deactivate id** *operation_id*

Example

```
RP/0/RP0/CPU0:ios#install deactivate ncs1004-k9sec-2.1.0.0-r721.x86_64
```

Or

```
RP/0/RP0/CPU0:ios#install deactivate id 8
```

All features and software patches associated with the package are deactivated. You can specify multiple package names to deactivate them simultaneously.

If you use the operation ID, all packages added in the specified operation are deactivated together. You do not have to deactivate the packages individually.

3. Use the **show install inactive** command to display the inactive packages.

Example

```
RP/0/RP0/CPU0:ios#show install inactive
Mon Mar 11 08:07:46.504 UTC
1 inactive package(s) found:
    ncs1004-k9sec-2.1.0.0-r721.x86_64
```

The deactivated packages are now listed as inactive packages. You can remove only inactive packages from the repository.

4. Use the **install remove** *package_name* command to remove the inactive packages from the repository.

Example

```
RP/0/RP0/CPU0:ios#install remove ncs1004-k9sec-2.1.0.0-r721.x86_64
```

Use the **install remove** command with the **id** *operation-id* keyword and argument to remove all packages added for the specified operation ID.

5. Use the **install commit system** command to commit the newly active software.

Example

```
RP/0/RP0/CPU0:ios#install commit system
```

6. Use the **show install repository** command to display the packages available in the repository.

Example

```
RP/0/RP0/CPU0:ios#show install repository
Mon Mar 11 08:11:55.780 UTC
4 package(s) in XR repository:
     ncs1004-xr-7.2.1 version=7.2.1 [Boot image]
     ncs1004-mini-x-7.2.1
     ncs1004-mpls-2.0.0.0-r711
     ncs1004-mpls-te-rsvp-2.1.0.0-r711
```

The removed package does not appear in the output.

The selected package and its associated features or patches are fully deactivated and removed from the NCS 1004 software repository.

What to do next

Install the required packages. See Install packages.

FPD automatic upgrade

This section explains the FPD automatic upgrade feature, its limitations across hardware types and releases, and the expected FPD status after a software upgrade.

FPD automatic upgrade is a system capability that

- upgrades FPD firmware versions of all the components to the latest version along with software activation,
- ensures all the FPD components show CURRENT status after the software upgrade, and
- retains the upgraded FPD version even when the software image is rolled back to the original version.

From Release 7.9.1, FPD automatic upgrade is enabled by default. You can manually disable it using the **fpd auto-upgrade disable** command. Before upgrading from a release earlier than Release 7.9.1 to Release 7.9.1, clear any existing FPD configuration using the **no fpd auto-upgrade** command to ensure that the automatic upgrade is active after the upgrade.

Feature history

Limitations and exclusions

Table 14: Feature history

Feature name	Release information	Feature description
Automatic FPD upgrade	Cisco IOS XR Release 7.9.1	The automatic FPD upgrade functionality is now enabled by default. It upgrades the FPD components' firmware version to the latest version. This enhancement eliminates the need to explicitly enable the functionality using the **fpd auto-upgrade enable** command. As a result, the software upgrade is simplified, and the system always maintains the latest state of the FPD firmware version.

> **Note**
>
> From Release 25.4.1, the automatic FPD upgrade process is supported in 1.2T, 1.2TL, QDD, and QXP line cards. It is not supported in the OTN-XP line card.

> **Note**
>
> FPD automatic upgrade is supported for the BP_SSD and CPU_SSD FPDs only if the SSDs are programmed with the latest firmware. FPD automatic upgrade for BP_SSD and CPU_SSD works without manual intervention when upgrading from Release 7.5.2 to a later release. If upgrading from a release earlier than Release 7.5.2 to Release 7.5.2, SSDs use the old firmware. In this scenario, manually upgrade BP_SSD and CPU_SSD FPDs, even if FPD automatic upgrade is enabled.

> **Note**
>
> FPD automatic upgrade is not supported on the LC_DP_MOD_FW FPD of the OTN-XP card because the upgrade affects traffic.

> **Note**
>
> FPD automatic upgrade is not supported for POWMAN_CFG. During a system upgrade to Release 7.5.2 or a later release, manually upgrade POWMAN_CFG if it is not running the latest version. Manually upgrading POWMAN_CFG does not affect traffic.

Enable FPD automatic upgrade

Use this procedure to enable the FPD automatic upgrade feature on NCS 1004 and verify that it is active.

Enable FPD automatic upgrade so that FPD firmware components are upgraded to the latest version during software activation. This eliminates manual intervention.

Procedure

1. Use the **fpd auto-upgrade enable** command to enable FPD automatic upgrade.

   Example

```
RP/0/RP0/CPU0:ios# configure
RP/0/RP0/CPU0:ios(config)# fpd auto-upgrade enable
```

```
RP/0/RP0/CPU0:ios(config)# commit
RP/0/RP0/CPU0:ios(config)# end
```

2. Use the **show running-config | inc fpd** command to verify whether FPD automatic upgrade is enabled.

   Example

```
RP/0/RP0/CPU0:ios# show running-config | inc fpd
Thu Feb  7 10:43:44.822 UTC
Building configuration...
fpd auto-upgrade enable
```

   The output confirms that FPD automatic upgrade is enabled when `fpd auto-upgrade enable` appears in the running configuration.

FPD automatic upgrade is enabled. During the next software activation, all supported FPD components are upgraded automatically and display the CURRENT status in the **show hw-module fpd** output.

show hw-module fpd output with FPD automatic upgrade enabled

This example shows all the FPDs in CURRENT status after a software upgrade with FPD automatic upgrade enabled.

```
RP/0/RP0/CPU0:ios# show hw-module fpd
Mon Nov 11 16:25:24.365 UTC
Auto-upgrade: Enabled
                                                                                FPD
Versions

==============
Location   Card type             HWver FPD device       ATR Status    Running
   Programd
-------------------------------------------------------------------------------
0/0        NCS1K4-1.2T-K9        2.0   LC_CPU_MOD_FW        CURRENT   240.44
   240.44
0/0        NCS1K4-1.2T-K9        1.0   LC_OPT_MOD_FW        CURRENT     1.38
     1.38
0/1        NCS1K4-1.2TL-K9       2.0   LC_CPU_MOD_FW        CURRENT   240.44
   240.44
0/1        NCS1K4-1.2TL-K9       1.0   LC_OPT_MOD_FW        CURRENT     1.38
     1.38
0/RP0      NCS1K4-CNTLR-K9       5.0   CSB_IMG           S  CURRENT     0.260
     0.200
0/RP0      NCS1K4-CNTLR-K9       5.0   TAM_FW               CURRENT    36.08
    36.08
0/RP0      NCS1K4-CNTLR-K9       3.14  BIOS              S  CURRENT     6.60
     6.60
0/RP0      NCS1K4-CNTLR-K9       1.4   BP_SSD               CURRENT   130.00
   130.00
0/RP0      NCS1K4-CNTLR-K9       5.0   CPU_FPGA             CURRENT     3.14
     3.14
0/RP0      NCS1K4-CNTLR-K9       1.4   CPU_SSD              CURRENT   130.00
   130.00
0/RP0      NCS1K4-CNTLR-K9       3.18  POWMAN_CFG           CURRENT     3.40
     3.40
0/PM0      NCS1K4-AC-PSU         0.1   PO-PriMCU            CURRENT     2.70
     2.70
0/SC0      NCS1004               2.0   BP_FPGA              CURRENT     1.25
     1.25
```

```
0/SC0      NCS1004              2.0   XGE_FLASH            CURRENT    18.04
    18.04
```

Manual POWMAN_CFG upgrade during FPD automatic upgrade

FPD automatic upgrade does not support POWMAN_CFG. If POWMAN_CFG displays NEED UPGD after a software upgrade, perform a manual upgrade. The provided output shows the **show hw-module fpd** command results before the manual upgrade.

```
RP/0/RP0/CPU0:ncs1004-129# show hw-module fpd
Tue Nov 21 15:55:27.689 UTC
Auto-upgrade: Disabled
                                                                              FPD
Versions

==============
Location   Card type             HWver FPD device       ATR Status    Running
   Programd
-----------------------------------------------------------------------------------
0/0        NCS1K4-2-QDD-C-K9     1.0   LC_CPU_MOD_FW        NEED UPGD  80.10
    80.10
0/0        NCS1K4-2-QDD-C-K9     1.0   LC_OPT_MOD_FW        CURRENT     1.38
     1.38
0/2        NCS1K4-1.2TL-K9       3.0   LC_CPU_MOD_FW        CURRENT    75.20
    75.20
0/2        NCS1K4-1.2TL-K9       1.0   LC_OPT_MOD_FW        CURRENT     1.38
     1.38
0/3        NCS1K4-1.2TL-K9       3.0   LC_CPU_MOD_FW        CURRENT    75.20
    75.20
0/3        NCS1K4-1.2TL-K9       1.0   LC_OPT_MOD_FW        CURRENT     1.38
     1.38
0/RP0      NCS1K4-CNTLR-K9       5.0   CSB_IMG           S  CURRENT     0.200
     0.200
0/RP0      NCS1K4-CNTLR-K9       5.0   TAM_FW               CURRENT    36.08
    36.08
0/RP0      NCS1K4-CNTLR-K9       1.14  BIOS              S  CURRENT     5.50
     5.50
0/RP0      NCS1K4-CNTLR-K9       5.4   BP_SSD               CURRENT    75.00
    75.00
0/RP0      NCS1K4-CNTLR-K9       5.0   CPU_FPGA             CURRENT     1.14
     1.14
0/RP0      NCS1K4-CNTLR-K9       5.4   CPU_SSD              CURRENT    75.00
    75.00
0/RP0      NCS1K4-CNTLR-K9       3.18  POWMAN_CFG           CURRENT     3.40
     3.40
0/PM0      NCS1K4-DC-PSU         0.1   PO-PriMCU            CURRENT     1.12
     1.12
0/PM1      NCS1K4-DC-PSU         0.1   PO-PriMCU            CURRENT     1.12
     1.12
0/SC0      NCS1004               2.0   BP_FPGA              CURRENT     1.25
     1.25
0/SC0      NCS1004               2.0   XGE_FLASH            CURRENT    18.04
    18.04
```

To upgrade POWMAN_CFG manually:

1. Initiate the FPD upgrade:

```
RP/0/RP0/CPU0:ios# upgrade hw-module location 0/RP0 fpd POWMAN_CFG
```

POWMAN_CFG moves to RLOAD REQ state:

```
0/RP0      NCS1K4-CNTLR-K9       3.18  POWMAN_CFG           RLOAD REQ   2.50
      2.50
```

2. Reload the route processor (RP) to complete the upgrade:

```
sysadmin-vm:0_RP0# hw-module location 0/RP0 reload noprompt
```

After reload, POWMAN_CFG shows CURRENT status and the upgrade is complete.

NCS 1004 SSD FPD upgrade support

This section explains SSD FPD upgrade support on NCS 1004, including when the NOT READY status appears in **show hw-module fpd** output and what it means for your system.

SSD FPD upgrade support is a capability that

- enables the chassis SSD FPD (BP_SSD) and controller SSD FPD (CPU_SSD) to be upgraded to newer firmware versions, and
- reports a NOT READY status in the **show hw-module fpd** output for SSD FPDs when the system runs a release earlier than the one that first qualified each SSD model.

If you run the **show hw-module fpd** command in releases earlier than those supporting each chassis SSD (BP_SSD) and controller SSD (CPU_SSD), the output displays NOT READY for the STATUS column of BP_SSD and CPU_SSD. The NOT READY status does not affect the FPD's function.

SSD FPD status in supported and unsupported releases

These examples show how the **show hw-module fpd** command output differs depending on whether the running release supports the installed SSD model.

SSD FPD status in a supported release

Command

```
RP/0/RP0/CPU0:ios#show hw-module fpd
```

In this output, the STATUS of BP_SSD and CPU_SSD is CURRENT, indicating that the chassis and controller SSD FPDs are running the current release firmware.

Output

```
Wed Jun 4 05:37:09.037 UTC

Auto-upgrade: Enabled
                                                                              FPD
Versions

==============
Location   Card type             HWver FPD device       ATR Status    Running
   Programd
-------------------------------------------------------------------------------
0/0        NCS1K4-2-QDD-C-K9     1.0   LC_CPU_MOD_FW          CURRENT    80.10
     80.10
0/0        NCS1K4-2-QDD-C-K9     1.0   LC_OPT_MOD_FW          CURRENT     1.38
      1.38
0/1        NCS1K4-2-QDD-C-K9     1.0   LC_CPU_MOD_FW          CURRENT    80.10
     80.10
```

```
0/1         NCS1K4-2-QDD-C-K9      1.0   LC_OPT_MOD_FW          CURRENT     1.38
      1.38
0/RP0       NCS1K4-CNTLR-B-K9      4.0   CSB_IMG             S  CURRENT     0.200
     0.200
0/RP0       NCS1K4-CNTLR-B-K9      4.0   TAM_FW                 CURRENT     36.08
     36.08
0/RP0       NCS1K4-CNTLR-B-K9      1.14  BIOS                S  RLOAD REQ   4.70
      4.70
0/RP0       NCS1K4-CNTLR-B-K9      5.4   BP_SSD                 CURRENT     75.00
     75.00
0/RP0       NCS1K4-CNTLR-B-K9      4.0   CPU_FPGA               CURRENT     1.14
      1.14
0/RP0       NCS1K4-CNTLR-B-K9      5.4   CPU_SSD                CURRENT     75.00
     75.00
0/RP0       NCS1K4-CNTLR-B-K9      3.18  POWMAN_CFG             CURRENT     3.40
      3.40
0/PM1       NCS1K4-AC-PSU          0.1   PO-PriMCU              CURRENT     2.70
      2.70
0/SC0       NCS1004                2.0   BP_FPGA                CURRENT     1.25
      1.25
0/SC0       NCS1004                2.0   XGE_FLASH              CURRENT     18.04
     18.04
```

SSD FPD status in an unsupported release

Command

```
RP/0/RP0/CPU0:ios#show hw-module fpd
```

In this output, the STATUS of BP_SSD and CPU_SSD is NOT READY, indicating that the chassis and controller SSD FPDs are running firmware from an unsupported release.

Output

```
Wed Jun  4 05:37:09.037 UTC

Auto-upgrade:Enabled
                                                                                FPD
Versions

==============
Location   Card type              HWver FPD device       ATR Status    Running
   Programd
-------------------------------------------------------------------------------
0/0         NCS1K4-2-QDD-C-K9      1.0   LC_CPU_MOD_FW          CURRENT     80.10
     80.10
0/0         NCS1K4-2-QDD-C-K9      1.0   LC_OPT_MOD_FW          CURRENT     1.38
      1.38
0/1         NCS1K4-2-QDD-C-K9      1.0   LC_CPU_MOD_FW          CURRENT     80.10
     80.10
0/1         NCS1K4-2-QDD-C-K9      1.0   LC_OPT_MOD_FW          CURRENT     1.38
      1.38
0/RP0       NCS1K4-CNTLR-B-K9      4.0   CSB_IMG             S  CURRENT     0.200
     0.200
0/RP0       NCS1K4-CNTLR-B-K9      4.0   TAM_FW                 CURRENT     36.08
     36.08
0/RP0       NCS1K4-CNTLR-B-K9      1.14  BIOS                S  RLOAD REQ   4.70
      4.70
0/RP0       NCS1K4-CNTLR-B-K9      0.0   BP_SSD                 NOT READY
       0.00
0/RP0       NCS1K4-CNTLR-B-K9      4.0   CPU_FPGA               CURRENT     1.14
      1.14
```

```
0/RP0       NCS1K4-CNTLR-B-K9      0.0    CPU_SSD                 NOT READY
       0.00
0/RP0       NCS1K4-CNTLR-B-K9      3.18   POWMAN_CFG              CURRENT      3.40
      3.40
0/PM1       NCS1K4-AC-PSU          0.1    PO-PriMCU               CURRENT      2.70
      2.70
0/SC0       NCS1004                2.0    BP_FPGA                 CURRENT      1.25
      1.25
0/SC0       NCS1004                2.0    XGE_FLASH               CURRENT     18.04
     18.04
```

Verify SSD model name and release

Use this procedure to identify the SSD model name and firmware version on NCS 1004 so that you can verify whether an FPD upgrade is supported in your target release.

Ensure the installed SSD model is qualified for firmware upgrade in the target release by checking its model and firmware version.

Before upgrading SSD FPDs, you must verify that your SSD model and firmware are supported for upgrade in the target release. Compare your results with the SSD FPD upgrade matrix to confirm compatibility.

Procedure

1. Use the **admin** command to enter the administrator mode.

   Example

   ```
   RP/0/RP0/CPU0:ios#admin
   Wed Jun  4 11:47:09.156 UTC
   Last login: Thu May 29 11:59:29 2025 from 192.0.0.4

   root connected from 192.0.0.4 using ssh on sysadmin-vm:0_RP0
   sysadmin-vm:0_RP0#
   ```

2. Use the **show smart-monitor | inc "SmartCtl|\Model:|\Firm"** command to check the SSD model name and firmware version.

   Example

   ```
   sysadmin-vm:0_RP0#show smart-monitor | inc "SmartCtl|\Model:|\Firm"
   ```

   The output displays the SSD model name and firmware version. The **SmartCtl info for sda** block provides the controller SSD FPD information. The **SmartCtl info for sdb** block provides the chassis SSD FPD information.

   Output example

   ```
   Tue Jun 24 06:44:19.927 UTC
   ======== SmartCtl info for sda ========
   Device Model:     Micron_5100_MTFDDAK240TCB
   Firmware Version: D0MU075
   ======== SmartCtl info for sdb ========
   Device Model:     Micron_5100_MTFDDAV240TCB
   Firmware Version: D0MU075
   ```

3. Verify the SSD model name against the release in which the upgrade is supported in the SSD FPD upgrade matrix.

You have verified whether the installed SSD model and firmware on NCS 1004 are eligible for FPD upgrade in your target release.

SSD FPD upgrade matrix

This section lists the SSD models qualified for FPD upgrade on NCS 1004, together with the required firmware version and the minimum Cisco IOS XR release that supports each model.

Use these tables to determine which SSD models are qualified for FPD upgrade and the minimum Cisco IOS XR release required. Cross-reference the SSD model name you identified using the Verify SSD model name and release procedure.

Table 15: Upgrade matrix for controller SSD FPDs

SSD model name	FPD version	FPD upgrade supported from release
SOLIDIGM SSDSC2KB240GZ	130	25.x.x and later
Micron_5400_MTFDDAK240TGA	0.2	24.1.1
INTEL SSDSC2KB240GZ	120	7.10.1, 24.1.1
INTEL SSDSC2KB240GZ	111	7.10.1
INTEL SSDSC2KB240G8	132	7.5.2
Micron_5100_MTFDDAK240TCB	51	7.5.2
Micron_5300_MTFDDAK240TDS	0.1	7.5.2

Table 16: Upgrade matrix for chassis SSD FPDs

SSD model name	FPD version	FPD upgrade supported from release
SOLIDIGM SSDSCKKB240GZ	130	25.x.x and later
Micron_5400_MTFDDAV240TGA	0.2	24.1.1
INTEL SSDSCKKB240GZ	120	7.10.1, 24.1.1
INTEL SSDSCKKB240GZ	111	7.10.1
INTEL SSDSCKKB240G8	132	7.5.2
Micron_5100_MTFDDAV240TCB	51	7.5.2
Micron_5300_MTFDDAV240TDS	0.1	7.5.2

Upgrade firmware

Use this procedure to upgrade FPD firmware on NCS 1004 after a software upgrade.

You must upgrade the FPD firmware of the route processor and the line cards after upgrading to the latest software release. This task also provides instructions for upgrading the FPD firmware of SSDs located on the chassis SSD (BP_SSD) and the route processor SSD (CPU_SSD). This upgrade is supported from R7.5.2.

Table 17: Feature history

Feature name	Release information	Feature description
FPD upgrade support for SSDs	Cisco IOS XR Release 7.5.2	The FPDs of the SSDs on the chassis and on the route processor can now be upgraded. This feature allows you to maintain the FPD versions of SSDs with the latest firmware, including enhancements and bug fixes. If an FPD upgrade is required, the **One Or More FPDs Need Upgrade Or Not In Current State** alarm is raised on the route processor.

Note

The Provisioning In Progress alarm is raised on the slice or line card during the FPD upgrade and automatically clears after the upgrade completes. This alarm does not affect traffic.

Note

Follow this sequence to upgrade the FPDs of the OTN-XP card:

1. LC_CPU_MOD_FW
2. LC_DP_MOD_FW
3. LC_CFP2_PORT_<0/1>

From Release 7.5.2, the FPDs of the SSDs on the chassis and the route processor can be upgraded. FPD upgrades of BP_SSD and CPU_SSD do not impact traffic.

Procedure

1. Use the **show hw-module fpd** command to check the status of the FPDs.

   Verify the status of the FPDs of the line cards in these examples.

   Example

```
RP/0/RP0/CPU0:ios# show hw-module fpd

Fri May 29 11:17:52.980 UTC
```

```
                                                                    FPD Versions

=================

Location   Card type             HWver FPD device       ATR Status   Running
 Programd

--------------------------------------------------------------------------------

0/0        NCS1K4-1.2T-K9        2.0   LC_CPU_MOD_FW        CURRENT   21.19
  21.19

0/0        NCS1K4-1.2T-K9        1.0   LC_OPT_MOD_FW        CURRENT    2.04
   2.04

0/1        NCS1K4-OTN-XP         3.0   LC_CPU_MOD_FW        NEED UPGD 21.18
  21.18

0/1        NCS1K4-OTN-XP         3.0   LC_DP_MOD_FW         CURRENT    6.10
   6.10

0/2        NCS1K4-OTN-XP         3.0   LC_CPU_MOD_FW        NEED UPGD 21.18
  21.18

0/2        NCS1K4-OTN-XP         3.0   LC_DP_MOD_FW         CURRENT    6.10
   6.10

0/3        NCS1K4-OTN-XP         3.0   LC_CPU_MOD_FW        NEED UPGD 21.18
  21.18

0/3        NCS1K4-OTN-XP         3.0   LC_DP_MOD_FW         CURRENT    6.10
   6.10

0/RP0      NCS1K4-CNTLR-K9       4.0   CSB_IMG           S  CURRENT    0.200
   0.200

0/RP0      NCS1K4-CNTLR-K9       4.0   TAM_FW               CURRENT   36.08
  36.08

0/RP0      NCS1K4-CNTLR-K9       1.14  BIOS              S  CURRENT    4.30
   4.30

0/RP0      NCS1K4-CNTLR-K9       4.0   CPU_FPGA             CURRENT    1.14
   1.14

0/PM0      NCS1K4-DC-PSU         0.1   PO-PriMCU            CURRENT    1.12
   1.12

0/PM1      NCS1K4-DC-PSU               PO-PriMCU            NOT READY


0/SC0      NCS1004               2.0   BP_FPGA              CURRENT    1.25
   1.25

0/SC0      NCS1004               2.0   XGE_FLASH            CURRENT   18.04
  18.04
```

From R7.5.2, you can verify the status of the FPDs of the SSDs in this example.

Example

```
RP/0/RP0/CPU0:ios# show hw-module fpd
Thu Oct  7 12:44:43.532 UTC

Auto-upgrade:Disabled
                                                                        FPD Versions


=================

Location   Card type            HWver FPD device       ATR Status   Running
 Programd

--------------------------------------------------------------------------------

0/0        NCS1K4-2-QDD-C-K9     1.0   LC_CPU_MOD_FW        CURRENT    21.31
     21.31
0/0        NCS1K4-2-QDD-C-K9     1.0   LC_OPT_MOD_FW        CURRENT     1.26
      1.26
0/1        NCS1K4-2-QDD-C-K9     0.0   LC_CPU_MOD_FW        CURRENT    21.31
     21.31
0/1        NCS1K4-2-QDD-C-K9     1.0   LC_OPT_MOD_FW        CURRENT     1.26
      1.26
0/2        NCS1K4-2-QDD-C-K9     1.0   LC_CPU_MOD_FW        CURRENT    21.31
     21.31
0/2        NCS1K4-2-QDD-C-K9     1.0   LC_OPT_MOD_FW        CURRENT     1.26
      1.26
0/3        NCS1K4-2-QDD-C-K9     0.0   LC_CPU_MOD_FW        CURRENT    21.31
     21.31
0/3        NCS1K4-2-QDD-C-K9     1.0   LC_OPT_MOD_FW        CURRENT     1.26
      1.26
0/RP0      NCS1K4-CNTLR-K9       4.0   CSB_IMG           S  CURRENT     0.200
     0.200
0/RP0      NCS1K4-CNTLR-K9       4.0   TAM_FW               CURRENT    36.08
     36.08
0/RP0      NCS1K4-CNTLR-K9       1.14  BIOS              S  CURRENT     5.30
      5.30
0/RP0      NCS1K4-CNTLR-K9       5.4   BP_SSD               NEED UPGD  71.00
     71.00
0/RP0      NCS1K4-CNTLR-K9       4.0   CPU_FPGA             CURRENT     1.14
      1.14
0/RP0      NCS1K4-CNTLR-K9       5.4   CPU_SSD              NEED UPGD  71.00
     71.00
0/PM1      NCS1K4-AC-PSU         0.1   PO-PriMCU            NEED UPGD   2.51
      2.51
0/SC0      NCS1004               2.0   BP_FPGA              CURRENT     1.25
      1.25
0/SC0      NCS1004               2.0   XGE_FLASH            CURRENT    18.04
     18.04
```

2. Use the **upgrade hw-module** command to upgrade the FPDs.

Example

This example shows how to upgrade the FPD image of a line card.

```
RP/0/RP0/CPU0:ios# upgrade hw-module location all fpd all
```

This command upgrades the FPDs of line cards. The FPD upgrade process for line cards may take three to five minutes. After the upgrade, the device automatically reloads. When the process completes, all FPDs, including BIOS, display the CURRENT status.

Example

From R7.5.2, this example shows how to upgrade the FPD image of BP_SSD.

```
RP/0/RP0/CPU0:ios# upgrade hw-module location 0/RP0 fpd BP_SSD
```

Example

From R7.5.2, this example shows how to upgrade the FPD image of CPU_SSD.

```
RP/0/RP0/CPU0:ios# upgrade hw-module location 0/RP0 fpd CPU_SSD
```

3. Use the **show hw-module fpd** command to verify the FPD status after the upgrade.

Example

```
RP/0/RP0/CPU0:ios# show hw-module fpd
Fri May 29 11:30:24.492 UTC

Auto-upgrade:Disabled
                                                                                FPD
 Versions

==============
Location   Card type             HWver FPD device       ATR Status    Running
   Programd
-------------------------------------------------------------------------------
0/0       NCS1K4-2-QDD-C-K9 1.0   LC_CPU_MOD_FW             CURRENT    21.31
     21.31
0/0       NCS1K4-2-QDD-C-K9 1.0   LC_OPT_MOD_FW             CURRENT     1.26
      1.26
0/1       NCS1K4-2-QDD-C-K9 0.0   LC_CPU_MOD_FW             CURRENT    21.31
     21.31
0/1       NCS1K4-2-QDD-C-K9 1.0   LC_OPT_MOD_FW             CURRENT     1.26
      1.26
0/2       NCS1K4-2-QDD-C-K9 1.0   LC_CPU_MOD_FW             CURRENT    21.31
     21.31
0/2       NCS1K4-2-QDD-C-K9 1.0   LC_OPT_MOD_FW             CURRENT     1.26
      1.26
0/3       NCS1K4-2-QDD-C-K9 0.0   LC_CPU_MOD_FW             CURRENT    21.31
     21.31
0/3       NCS1K4-2-QDD-C-K9 1.0   LC_OPT_MOD_FW             CURRENT     1.26
      1.26
0/RP0     NCS1K4-CNTLR-K9   1.14  BIOS              S        RLOAD REQ   5.10
      5.10
0/RP0     NCS1K4-CNTLR-K9   5.4   BP_SSD                    RLOAD REQ   71.00
     71.00
0/RP0     NCS1K4-CNTLR-K9   4.0   CPU_FPGA                    CURRENT
1.14      1.14
0/RP0     NCS1K4-CNTLR-K9   5.4   CPU_SSD                   RLOAD REQ   71.00
     71.00
0/PM1     NCS1K4-AC-PSU     0.1   PO-PriMCU                   CURRENT
2.70      2.70
0/SC0     NCS1004           2.0   BP_FPGA                   CURRENT     1.25
      1.25
```

```
0/SC0     NCS1004           2.0   XGE_FLASH                 CURRENT    18.04
     18.04
```

4. Use the **hw-module location 0/RP0 reload** command to reload NCS 1004 if FPDs show RLOAD REQ status.

   After reload, verify the FPD status. If the upgrade fails, the status shows UPGD_FAIL. If the upgrade succeeds, the status shows CURRENT.

   Example

```
RP/0/RP0/CPU0:ios# show hw-module fpd
Fri May 29 11:35:24.492 UTC

Auto-upgrade:Disabled
                                                                              FPD
 Versions

==============
Location   Card type             HWver FPD device       ATR Status    Running
   Programd
-----------------------------------------------------------------------------------
0/0       NCS1K4-2-QDD-C-K9 1.0   LC_CPU_MOD_FW             CURRENT    21.31
     21.31
0/0       NCS1K4-2-QDD-C-K9 1.0   LC_OPT_MOD_FW             CURRENT     1.26
      1.26
0/1       NCS1K4-2-QDD-C-K9 0.0   LC_CPU_MOD_FW             CURRENT    21.31
     21.31
0/1       NCS1K4-2-QDD-C-K9 1.0   LC_OPT_MOD_FW             CURRENT     1.26
      1.26
0/2       NCS1K4-2-QDD-C-K9 1.0   LC_CPU_MOD_FW             CURRENT    21.31
     21.31
0/2       NCS1K4-2-QDD-C-K9 1.0   LC_OPT_MOD_FW             CURRENT     1.26
      1.26
0/3       NCS1K4-2-QDD-C-K9 0.0   LC_CPU_MOD_FW             CURRENT    21.31
     21.31
0/3       NCS1K4-2-QDD-C-K9 1.0   LC_OPT_MOD_FW             CURRENT     1.26
      1.26
0/RP0     NCS1K4-CNTLR-K9   1.14  BIOS              S       CURRENT     5.30
      5.30
0/RP0     NCS1K4-CNTLR-K9   5.4   BP_SSD                    CURRENT    75.00
     75.00
0/RP0     NCS1K4-CNTLR-K9   4.0   CPU_FPGA                  CURRENT     1.14
      1.14
0/RP0     NCS1K4-CNTLR-K9   5.4   CPU_SSD                   CURRENT    75.00
     75.00
0/PM1     NCS1K4-AC-PSU     0.1   PO-PriMCU                 CURRENT     2.70
      2.70
0/SC0     NCS1004           2.0   BP_FPGA                   CURRENT     1.25
      1.25
0/SC0     NCS1004           2.0   XGE_FLASH                 CURRENT    18.04
     18.04
```

> **Note**
>
> FPD upgrades from Release 7.0.1 to later releases do not affect traffic. The upgrade of LC_OPT_MOD_FW FPD during the transition from R7.0.0 to R7.0.1 impacts traffic

> **Note**
>
> FPD upgrade of LC_CPU_MOD_FW does not affect traffic. However, upgrading the LC_DP_MOD_FW FPD does impact traffic.

All FPDs on NCS 1004, including line cards and SSDs, are upgraded and show the CURRENT status. The device operates with the latest firmware, ensuring reliability and compatibility.

6 Implement Audit Monitoring

Topics:

Provides instructions for configuring audit monitoring and logging on the NCS 1004 to track system events and security-relevant changes. By implementing these features, administrators can enhance network compliance and security through centralized analysis of audit logs forwarded to a remote syslog server.

This chapter explains the audit monitoring and logging capabilities available on NCS 1004 and how to configure audit monitoring.

Feature name	Release information	Description
Audit logging and monitoring	Cisco IOS XR 25.3.1	You can enable audit logging and monitoring on the NCS 1004. You can also configure predefined rule groups that allow NCS 1004 to monitor activities, log events, and, when necessary, forward audit logs to a remote syslog server for centralized analysis and incident response. This feature helps enhance security and compliance on your network. CLI: These new commands are introduced: • **linux security audit monitor** *group-keyword* • **show linux security audit monitor status** • **linux security audit logging syslog** • • **logging** *remote-server-ipv4/ipv6/remote-server-ip* • **show linux security audit logging syslog**

Audit logging

This topic explains how audit logs and audit rules work together to automatically record security-relevant events, facilitate compliance monitoring, and enable administrators to track system changes for investigation and reporting purposes.

Audit logging is a security and compliance feature that

- operates according to defined audit rules, automatically creating audit logs whenever specified actions or changes occur on the router
- integrates with the Linux Audit Daemon to monitor and log relevant security events across the router, and
- allows forwarding of audit logs to a remote syslog server.

Linux audit daemon is a user-space component of the Linux auditing system that

- tracks and logs system calls, file accesses, user actions, and other events as specified by audit rules, and
- provides administrators with insights to detect suspicious behavior and maintain system integrity.

An audit rule is a configuration that

- specifies which files, directories, or system events should be monitored
- determines the conditions for monitoring, and
- forms the foundation of an audit logging system.

An Audit log is a chronological record that

- is automatically generated when a monitored event, as defined by an audit rule, occurs, and
- typically includes details such as the event type, timestamp, user or process involved, and affected resources.

Audit rules and audit logs for security monitoring

Administrators define audit rules to track changes to sensitive files, monitor system calls, and observe other critical activities. By customizing audit rules, organizations can align monitoring with their unique security and compliance requirements.

Audit rules establish what to watch, while audit logs capture and document every relevant occurrence, ensuring a complete and actionable history of system activity.

For example, an audit rule that monitors changes to the **/etc/passwd** file creates an audit log entry each time this file is modified.

Audit logging is not to be confused with system logging. While audit logging records security-relevant events, such as user actions and changes to sensitive files, system logging (syslog) captures general system events like service status updates, routine errors, or informational messages.

Audit log storage

- NCS 1004 stores audit logs locally at **/var/log/audit/audit.log**, unless you enable log forwarding.
- By default, the system rotates up to five audit log files, each up to 8 MB in size.

How audit logging works

This process describes how audit logging operates in network devices, the components involved, and the stages of monitoring and log forwarding.

Summary

These are the key components involved in this feature:

- Network Administrator: The user who initiates configurations via CLI.
- Linux audit daemon: The process that monitors system activity according to the installed rules and writes audit event logs.
- Local rsyslog daemon: The process that forwards logs to a remote syslog server.
- Remote syslog server: The external server that maintains the logs generated by the router.

The Linux audit daemon is the core service that actually performs event monitoring and logging, based on the audit rules configured by the administrator. It operates at the operating system level on each node, such as line cards and processors.

Workflow

These stages describe how audit monitoring and logging works.

1. The network administrator enables audit monitoring via CLI.
2. The router software receives the configurations. It applies the relevant audit rules and ensures these rules are distributed to all appropriate nodes.
3. On each node, the Linux audit daemon actively monitors system events as defined by the audit rules and writes the logs to a local log file at **/var/log/audit/audit.log**.
4. If the network administrator has enabled log forwarding, the audit logs are sent to the local rsyslog daemon. The rsyslog daemon then forwards the logs to a remote syslog server.

Guidelines for audit logging

Use these guidelines for audit logging configuration, resource usage, log security, and log forwarding on NCS 1004.

Granularity of audit rules

- You can enable or disable audit rules only at the group level, not individually within a group.
- Regularly review the status of audit rules and audit log forwarding to ensure monitoring remains effective.

Resource usage on NCS 1004

Use caution when enabling all rule groups, especially those that monitor frequent events. Enabling all groups may increase CPU, memory, or disk usage. Enable only the groups required for compliance or security needs.

Security of audit logs and syslog servers

- Allow only users with appropriate administrative privileges to configure or view Linux security audit settings.
- Protect access to audit logs and syslog servers to prevent unauthorized access or tampering.

Log forwarding to remote syslog servers

- Confirm that the remote syslog server is reachable and properly configured before enabling log forwarding.
- NCS 1004 forwards audit logs to remote syslog servers in unencrypted plain text. Use only trusted network segments for remote syslog servers.

Configure audit logging

Use this procedure to configure and monitor audit logs for specific system events by enabling audit rule groups, verifying their status, and optionally forwarding logs to a remote syslog server for centralized monitoring.

Follow this task to configure and monitor audit logs for specific system events by enabling the relevant audit rule groups.

Procedure

1. Run the **linux security audit monitor** *<group-keyword>* command to enable a group of audit rules.

   Example

```
RP/0/RP0/CPU0:ios# configure
RP/0/RP0/CPU0:ios(config)# linux security audit monitor xr-software
RP/0/RP0/CPU0:ios(config)# linux security audit monitor user-group-config-files
RP/0/RP0/CPU0:ios(config)# commit
```

2. Run the **show linux security audit monitor status** command to verify the general status of all active audit rule groups.

   Example

```
RP/0/RP0/CPU0:ios# show linux security audit monitor status
Wed Aug 20 16:16:23.518 IST
key name: xr-software                  status: enabled
rules:
-a always,exit -F arch=b64 -F dir=/pkg/bin -F perm=wa -k xr_bin_changes
-a always,exit -F arch=b64 -F dir=/pkg/sbin -F perm=wa -k xr_sbin_changes
-a always,exit -F arch=b64 -F dir=/pkg/lib -F perm=wa -k xr_lib_changes
------------------------------------------------------------
key name: user-group-config-files      status: enabled
rules:
-a always,exit -F arch=b64 -F path=/etc/passwd -F perm=wa -k passwd_changes
-a always,exit -F arch=b64 -F path=/etc/shadow -F perm=wa -k shadow_changes
-a always,exit -F arch=b64 -F path=/etc/group -F perm=wa -k group_changes
-a always,exit -F arch=b64 -F path=/etc/sudoers -F perm=wa -k sudoers_changes
------------------------------------------------------------
```

3. (Optional) Run the **linux security audit logging syslog** command to enable forwarding of audit rules.

   Example

```
RP/0/RP0/CPU0:ios# configure
RP/0/RP0/CPU0:ios(config)# linux security audit logging syslog
RP/0/RP0/CPU0:ios(config)# commit
```

4. (Optional) Run the **logging** *remote-server-ip* **vrf** *vrf-name* command to configure the remote syslog server.

   Example

```
RP/0/RP0/CPU0:ios# configure
RP/0/RP0/CPU0:ios(config)# logging 10.0.1.2 vrf default severity info port
default facility local6
RP/0/RP0/CPU0:ios(config)# commit
```

5. (Optional) Run the **show linux security audit logging syslog** command to verify whether audit log forwarding is enabled and to view the configured remote syslog server.

Example

```
RP/0/RP0/CPU0:ios# show linux security audit logging syslog
Wed Aug 20 16:16:44.553 IST
status: enabled
syslog-server(s):
ipaddr: 10.0.1.2 vrf: vrf-default port: 514
ipaddr: 10.0.1.9 vrf: vrf-default port: 514
```