Configure New Password Recovery Procedure on 8000 and NCS5500 Platforms

Contents

Introduction

This document describes a new password recovery process for Cisco IOS® XR for Cisco 8000 and NCS5500 platforms.

Background Information

If a user forgets the root password, or passwords of all users are lost on XR7 LNT platforms (Cisco 8000, NCS-540L), or eXR platforms (ASR9K 64-bit, NCS5K, NCS5500, NCS 540, NCS 560), the router becomes inaccessible for the user as login is not possible without correct username/password combination. Today, password recovery of such router is possible only via router re-image with the use of the USB boot method or iPXE boot from an external server. Re-image of router involves installing router software again afresh and loading the device configuration. Installing software afresh is a time-consuming process.

Starting with 7.3.16 release for Cisco 8000 series platform and 7.3.3 for NCS5500 series platform, Cisco has come up with a new method for password recovery without the need to re-image the router. Such a password recovery method does not require software to be re-installed, thereby saving time and allowing access to the router post password reset. This new password recovery method is security standards compliant as old user info and user runtime data is wiped out before initiation of the password recovery process.

Problem

Today, password recovery on XR7 LNT platforms (Cisco 8000, NCS-540L) or eXR platforms (ASR9K 64-bit, NCS5K, NCS5500, NCS 540, NCS 560) is not possible. The only available alternative to reset the password is to re-image the router with the use of the USB boot method, or iPXE boot from an external server. This is a time-consuming process as it involves installing router software again afresh and loading device configuration. A faster and secure method for password recovery on Cisco XR7 and eXR platforms is needed.

Solution

Starting with 7.3.16 release for Cisco 8000 series platform and 7.3.3 for NCS5500 series platform, Cisco has come up with a new method for password recovery without the need to re-image the router. In the Grand

Unified Bootloader (GRUB) menu of the Route Processor (RP) bootup screen a new option - Cisco IOS XR-Recovery is added which is explicitly created for the password recovery procedure. In the router configuration, a new command **system recovery** is created for the purpose of enabling the new password recovery feature. This is currently an optional feature and is not enabled by default.

Caveats:

- RP bios bootup GRUB screen menu option **Cisco IOS XR-recovery** can be seen irrespective of command **system recovery** configured or not configured in the router configuration. If the **system recovery** command is not present in router configuration, and a new password recovery method is attempted by selecting the bios GRUB screen menu option **Cisco IOS XR-recovery**, then the router can abort the password recovery process and boot with the old configuration. So it is mandatory to have a **system recovery** command configured on the router for the password recovery method to work.
- The password recovery feature is disabled by default.
- The password recovery feature needs to be explicitly enabled via configuration Command Line Interface (CLI). RP/0/RP0/CPU0:HOSTNAME(config)#**system recovery**.

- If the router undergoes a password recovery procedure, then the **system recovery** command can be disabled post router bootup as all router configuration would be wiped out as part of the password recovery procedure. Users need to load the device configuration again and configure the **system recovery** command if it is not part of the device configuration.
- Apart from the deletion of router configuration, all user-created files, show tech files, and dumper files can be wiped out from both disk0 and hard disk as part of the cleanup procedure during password recovery.
- This feature is currently supported on 7.3.16 and later on Cisco 8000, 7.3.3 and later on NCS5500, and for other XR7 LNT and eXR platforms, this feature can be made available in future releases.

- Use the given procedure for platforms where both RP cards are installed in chassis. Bring both RP cards down to the bios GRUB menu. Then, password recovery procedures must be done on each RP card one by one. This is a mandatory step for dual RP platforms, otherwise, it would lead to config and file cleanup inconsistency.

New Password Recovery Steps

Prerequisite: The new password recovery feature works only if the CLI is part of the device configuration. If the CLI is not configured, then the new password recovery mechanism cannot work due to missing config CLI.

Enable password recovery feature:

<#root>

RP/0/RP0/CPU0:HOSTNAME(config)#

system recovery

Disable password recovery feature:

<#root>

RP/0/RP0/CPU0:HOSTNAME(config)#

```
no system recovery
```

Password recovery procedure must be done via RP console only.

Step 1. Bring RP card down to bios GRUB menu. For platforms where both RP cards are installed in chassis, both RP cards must be brought down to the bios GRUB menu before you start the password recovery procedure. This is a mandatory step. This can be done by either a power cycle of the device and then press the **ESC** key on both RP consoles to enter the bios GRUB menu, or by physically re-seating each RP one by one and then press the **ESC** key on the RP console in order to enter the bios GRUB menu.

RP0 and RP1 card:


```
Press Esc for boot options


Cisco 8000(R) Series BIOS Ver 1.22 Primary
Intel(R) Xeon(R) CPU D-1530 @ 2.40GHz
Board Type 0x220 PID 8812 Serial FOX2422PC5N
X86FPGA 1.5.0 TamLib 3.04.12
```

RP0 and RP1 card:


```
Press Esc for boot options
                    GNU GRUB   version 2.02 (LOCKED)

C+----------------------------------------------------------------------+
I| *IOS-XR-latest                                                       |
B|  IOS-XR-fallback                                                     |
X|  IOS-XR-recovery                                                     |
 |                                                                      |
W|                                                                      |
 |                                                                      |
V|                                                                      |
(|                                                                      |
 |                                                                      |
 |                                                                      |
 |                                                                      |
 |                                                                      |
 |                                                                      |
 +----------------------------------------------------------------------+

      Use the ^ and v keys to select which entry is highlighted.
      Press enter to boot the selected OS.
```
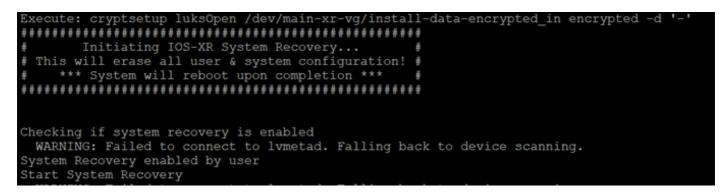
Step 2. On the RP0 card console, select the **IOS XR-recovery** option from the GRUB menu and press **Enter**.

RP0 card:

```
Press Esc for boot options
                    GNU GRUB   version 2.02 (LOCKED)

C+-----------------------------------------------------------------------+
I|  IOS-XR-latest                                                        |
B|  IOS-XR-fallback                                                      |
X| *IOS-XR-recovery                                                      |
 |                                                                       |
W|                                                                       |
 |                                                                       |
V|                                                                       |
(|                                                                       |
 |                                                                       |
 |                                                                       |
 |                                                                       |
 |                                                                       |
 +-----------------------------------------------------------------------+

        Use the ^ and v keys to select which entry is highlighted.
        Press enter to boot the selected OS.
```

Step 3. Select the **Cisco IOS XR-recovery** option from the GRUB menu and press **Enter** on the RP1 card console as soon as you see the Initiating IOS XR System Recovery... message on the RP0 card console. Do not wait until the RP0 card reaches the Enter root-system username prompt, otherwise the RP1 card can auto-reload and exit the bios GRUB menu. The RP0 card can boot up as active and the RP1 card can boot up as a standby card post the recovery process.

RP0 card:


```
Execute: cryptsetup luksOpen /dev/main-xr-vg/install-data-encrypted_in encrypted -d '-'
##################################################
#        Initiating IOS-XR System Recovery...        #
# This will erase all user & system configuration! #
#     *** System will reboot upon completion ***     #
##################################################


Checking if system recovery is enabled
  WARNING: Failed to connect to lvmetad. Falling back to device scanning.
System Recovery enabled by user
Start System Recovery
```

RP1 card:

```
Press Esc for boot options
                        GNU GRUB   version 2.02 (LOCKED)

C+-----------------------------------------------------------------+
I|  IOS-XR-latest                                                  |
B|  IOS-XR-fallback                                                |
X|*IOS-XR-recovery                                                 |
 |                                                                 |
W|                                                                 |
 |                                                                 |
V|                                                                 |
(|                                                                 |
 |                                                                 |
 |                                                                 |
 |                                                                 |
 |                                                                 |
 +-----------------------------------------------------------------+

      Use the ^ and v keys to select which entry is highlighted.
      Press enter to boot the selected OS.
```

Step 4. On the RP0 card, create a new root user and password. Attempt to log in to the device with the use of the new root username and password.

RP0 card:

```
RP/0/RP0/CPU0:Jul  8 04:52:06.168 CEST: ifmgr[361]: %PKT_INFRA-LINK-3-UPDOWN : Interface MgmtEth0/RP0/CPU0/0, changed state to Down
RP/0/RP0/CPU0:Jul  8 04:52:06.170 CEST: ifmgr[361]: %PKT_INFRA-LINK-3-UPDOWN : Interface MgmtEth0/RP0/CPU0/0, changed state to Up

!!!!!!!!!!!!!!!!!!!!! NO root-system username is configured. Need to configure root-system username. !!!!!!!!!!!!!!!!!!!!!

        --- Administrative User Dialog ---

  Enter root-system username: █
```

Step 5. The password recovery procedure is complete at this point.

The router is now booted with a blank configuration and with the root username/password created in step 4. Proceed with normal router configuration, or load a configuration from a backup file (any config backup stored in disk0 or hard disk can be lost as part of the password recovery procedure, hence always save the configuration on an external server). Ensure that you see this message in the RP0 console logs for both RP0 and RP1, as a verification step to confirm password recovery and in order to verify that all old user data cleanup has been completed successfully for both RP. If not, then repeat the Prerequisite Step and Steps 1 to 4 until you see these messages on the RP0 console logs. If this message is not seen for standby RP, then you need to repeat the Prerequisite Step and Steps 1 to 4 for the standby RP only.

```
RP/0/RP0/CPU0:Jul 8 06:13:24.551 CEST: sys_rec[1188]: %SECURITY-SYSTEM_RECOVERY-1-REPORT : System Recov

RP/0/RP1/CPU0:Jul 8 06:15:13.967 CEST: sys_rec[1188]: %SECURITY-SYSTEM_RECOVERY-1-REPORT : System Recov
```

Summary

This new password recovery procedure can be used to securely reset lost passwords on the Cisco 8000 series platform and the NCS5500 series platform in less than 10 minutes.