

# Cisco 8000和NCS5500平台上的新密碼恢復過程

## 目錄

[簡介](#)

[背景資訊](#)

[問題](#)

[解決方案](#)

[新密碼恢復步驟](#)

[摘要](#)

## 簡介

本文檔介紹適用於Cisco 8000和NCS5500平台的Cisco IOS®-XR的新密碼恢復過程。

## 背景資訊

如果使用者忘記了根密碼，或者所有使用者的密碼在XR7 LNT平台(Cisco 8000、NCS-540L)或eXR平台 ( ASR9K 64位、NCS5K、NCS5500、NCS 540、NCS 560 ) 上丟失，則使用者將無法登入，因為如果沒有正確的使用者名稱/密碼組合，將無法登入。目前，只能通過使用USB引導方法或從外部伺服器啟動iPXE來重新映像路由器，才能恢復此類路由器的密碼。重新映像路由器涉及重新安裝路由器軟體並載入裝置配置。重新安裝軟體是一個耗時的過程。

從Cisco 8000系列平台的7.3.16版和NCS5500系列平台的7.3.3版開始，思科提出了一種無需重新映像路由器即可恢復口令的新方法。這種口令恢復方法不需要重新安裝軟體，從而節省了時間並允許在口令重置後訪問路由器。這種新的密碼恢復方法符合安全標準，因為舊使用者資訊和使用者運行時資料在密碼恢復過程啟動之前被擦除。

## 問題

目前，在XR7 LNT平台(Cisco 8000、NCS-540L)或eXR平台 ( ASR9K 64位、NCS5K、NCS5500、NCS 540、NCS 560 ) 上無法進行密碼恢復。重置密碼的唯一可用替代方法是使用USB引導方法或從外部伺服器啟動iPXE來重新映像路由器。這是一個耗時的過程，因為它涉及重新安裝路由器軟體並載入裝置配置。

在Cisco XR7和eXR平台上需要更快且安全的密碼恢復方法。

## 解決方案

從Cisco 8000系列平台的7.3.16版和NCS5500系列平台的7.3.3版開始，思科提出了一種無需重新映像路由器即可恢復口令的新方法。在路由處理器(RP)啟動螢幕的Grand Unified Bootloader(GRUB)選單中，新增了一個新選項 — 「IOS-XR-Recovery」，該選項是為密碼恢復過程顯式建立的。在路由器配置中，會建立一個新命令**system recovery**，用於啟用新的口令恢復功能。此功能目前為選用功能，預設不會啟用。

## 注意事項:

- RP bios啟動GRUB螢幕選單選項**IOS-XR-recovery**將被看到，無論路由器配置中是否配置了**系統恢復**命令。如果路由器配置中沒有**system recovery**命令，並且通過選擇bios GRUB螢幕選單選項**IOS-XR-recovery**嘗試新的口令恢復方法，則路由器將中止口令恢復過程並使用舊配置啟動。因此，必須在路由器上配置**system recovery**命令才能使密碼恢復方法正常工作。
- 密碼復原功能預設會停用。
- 需要通過配置命令列介面(CLI)顯式啟用密碼恢復功能。  
RP/0/RP0/CPU0:HOSTNAME(config)#**系統恢復**。
- 如果路由器執行口令恢復過程，則在路由器啟動後，**system recovery**命令將被禁用，因為作為口令恢復過程的一部分，所有路由器配置將被清除。如果裝置配置中不包含此命令，使用者需要重新載入裝置配置並配置**system recovery**命令。
- 除了刪除路由器配置外，在密碼恢復過程中，所有使用者建立的檔案、show tech files和轉儲檔案都將從disk0和硬碟上擦除。
- Cisco 8000、7.3.3及更高版本目前在NCS5500上支援7.3.16及更高版本上的此功能，對於其他XR7 LNT和eXR平台，未來版本中會提供此功能。
- 對於兩個RP卡都安裝在機箱中的平台，請使用給定的過程。將兩個RP卡下至bios GRUB選單。然後，必須在每個RP卡上逐一執行密碼恢復過程。這是雙RP平台的強制步驟，否則將導致配置和檔案清理不一致。

## 新密碼恢復步驟

必備條件:只有當CLI是裝置配置的一部分時，新的口令恢復功能才起作用。如果未配置CLI，則由於缺少配置CLI，新的密碼恢復機制將無法工作。

啟用密碼恢復功能：

```
RP/0/RP0/CPU0:HOSTNAME(config)#system recovery
```

禁用密碼恢復功能：

```
RP/0/RP0/CPU0:HOSTNAME(config)#no system recovery
```

密碼恢復過程只能通過RP控制檯完成。

步驟1.將RP卡放入bios GRUB選單。對於兩個RP卡都安裝在機箱中的平台，在開始密碼恢復過程之前，必須將兩個RP卡都放入bios GRUB選單。這是強制步驟。這可以通過以下方法完成：裝置重新通電，然後按兩個RP控制檯上的ESC鍵進入bios GRUB選單；或者逐個物理地重新安放每個RP，然後在RP控制檯上按ESC鍵進入bios GRUB選單。

RP0和RP1卡：

```
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和RP1卡：

```
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.
```

步驟2.在RP0卡控制檯上，從GRUB選單中選擇IOS-XR-recovery選項，然後按Enter。

RP0卡：

```

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

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

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

```

步驟3.從GRUB選單中選擇**IOS-XR-recovery**選項，然後在RP1卡控制檯上看到RP0卡控制檯上的「Initiating IOS-XR System Recovery.. ( 啟動IOS-XR系統恢復..... )」消息後立即按**Enter**。不要等待RP0卡到達「Enter root-system username :」提示，否則RP1卡將自動重新載入並退出bios GRUB選單。恢復過程後，RP0卡將啟動為主用卡，RP1卡將啟動為備用卡。

RP0卡：

```

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 lvmtool. Falling back to device scanning.
System Recovery enabled by user
Start System Recovery

```

RP1卡：

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

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

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

步驟4.在RP0卡上建立新的根使用者和密碼。嘗試使用新的root使用者名稱和密碼登入裝置。

RP0卡：

```
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: █
```

步驟5.此時密碼復原程式已完成。

現在，路由器使用空白配置啟動，並且使用步驟4中建立的根使用者名稱/密碼啟動。請繼續執行正常的路由器配置或從備份檔案載入配置（在密碼恢復過程中，儲存在disk0或硬碟中的任何配置備份都將丟失，因此請始終在外部伺服器上儲存配置）。確保在RP0和RP1的RP0控制檯日誌中看到此消息，作為確認密碼恢復的驗證步驟，並驗證兩個RP的所有舊使用者資料清理是否已成功完成。如果沒有，則重複先決條件步驟和步驟1。到4。直到RP0控制檯日誌中看到這些消息。如果看不到待命RP的此消息，則需要僅對待命RP重複先決條件步驟和步驟1到4。

```
RP/0/RP0/CPU0:Jul 8 06:13:24.551 CEST: sys_rec[1188]: %SECURITY-SYSTEM_RECOVERY-1-REPORT :
System Recovery at 06:10:19 CEST Thu Jul 08 2021 was successful
```

```
RP/0/RP1/CPU0:Jul 8 06:15:13.967 CEST: sys_rec[1188]: %SECURITY-SYSTEM_RECOVERY-1-REPORT :
System Recovery at 06:11:23 CEST Thu Jul 08 2021 was successful
```

## 摘要

此新的密碼恢復過程可用於在10分鐘內安全地重置Cisco 8000系列平台和NCS5500系列平台上丟失的密碼。