

Cisco 8000和NCS5500平台上的新密码恢复程序

目录

[简介](#)

[背景信息](#)

[问题](#)

[解决方案](#)

[新密码恢复步骤](#)

[摘要](#)

简介

本文档介绍适用于Cisco 8000和NCS5500平台的Cisco IOS®-XR的新密码恢复过程。

背景信息

如果用户忘记了所有用户的根密码或密码，则XR7 LNT平台（思科8000、NCS-540L）或eXR平台（ASR9K 64位、NCS5K、NCS5500、NCS 540）上会丢失NCS 560），因为没有正确的用户名/密码组合，无法登录，所以用户无法访问路由器。现在，只有通过使用USB引导方法或从外部服务器进行iPXE引导来重新映像路由器，才能恢复此类路由器的口令。重新映像路由器涉及重新安装路由器软件并加载设备配置。重新安装软件是一个非常耗时的过程。

从Cisco 8000系列平台的7.3.16版和NCS5500系列平台的7.3.3版开始，思科提出了一种新的密码恢复方法，无需重新映像路由器。这种密码恢复方法不需要重新安装软件，从而节省时间并允许在重置密码后访问路由器。此新密码恢复方法符合安全标准，因为旧用户信息和用户运行时数据在启动密码恢复过程之前被擦除。

问题

如今，在XR7 LNT平台（思科8000、NCS-540L）或eXR平台（ASR9K 64位、NCS5K、NCS5500、NCS 540、NCS 560）上恢复密码不可能。重置密码的唯一可用替代方案是使用USB引导方法或从外部服务器进行iPXE引导来重新映像路由器。这是一个非常耗时的过程，因为它需要重新安装路由器软件并加载设备配置。

在Cisco XR7和eXR平台上，需要一种更快、更安全的口令恢复方法。

解决方案

从Cisco 8000系列平台的7.3.16版和NCS5500系列平台的7.3.3版开始，思科提出了一种新的密码恢复方法，无需重新映像路由器。在路由处理器(RP)启动屏幕的Grand Unified Bootloader(GRUB)菜单中，添加了新选项“IOS-XR-Recovery”，该选项为口令恢复过程显式创建。在路由器配置中，为了启用新的口令恢复功能，创建了新的命令系统恢复。这当前是可选功能，默认情况下不启用。

注意事项:

- 无论在路由器配置中配置或未配置**命令系统恢复**，都将看到RP bios启动GRUB屏幕菜单选项IOS-XR-recovery。如果路由器配置中**system recovery**命令不存在，并且通过选择bios GRUB屏幕菜单选项**IOS-XR-recovery**尝试了新的口令恢复方法，则路由器将中止口令恢复过程并使用旧配置启动。因此，必须在路由器上**配置系统恢复命令**，使口令恢复方法正常工作。
- 默认情况下禁用密码恢复功能。
- 口令恢复功能需要通过配置命令行界面(CLI)明确启用。
RP/0/RP0/CPU0:HOSTNAME(config)#**系统恢复**。
- 如果路由器执行口令恢复过程，则在路由器启动后将禁用**system recovery**命令，因为所有路由器配置都会作为口令恢复过程的一部分被擦除。如果系统恢复命令不属于设备配置，则用户需要重新加载**设备配置**并配置该命令。
- 除删除路由器配置外，在恢复密码时，除删除路由器配置外，还会从disk0和硬盘上清除用户创建的所有文件、show tech files和dumper文件。
- Cisco 8000、7.3.3及更高版本(NCS5500)以及其他XR7 LNT和eXR平台目前支持此功能，此功能将在未来版本中提供。
- 对于两个RP卡都安装在机箱中的平台，请按照给定步骤操作。将两个RP卡下拉到bios GRUB菜单。然后，必须逐个在每个RP卡上执行密码恢复过程。这是双RP平台的必需步骤，否则会导致配置和文件清理不一致。

新密码恢复步骤

前提条件：新密码恢复功能仅在CLI是设备配置的一部分时才起作用。如果未配置CLI，则新密码恢复机制将因缺少配置CLI而无法工作。

启用密码恢复功能：

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

禁用密码恢复功能：

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

密码恢复过程只能通过RP控制台完成。

步骤1.将RP卡下拉到bios GRUB菜单。对于两个RP卡都安装在机箱中的平台，必须先将两个RP卡都下拉到bios GRUB菜单，然后才能开始密码恢复过程。这是必需步骤。这可以通过以下方式完成：设备重新通电，然后按两个RP控制台上的ESC键进入bios GRUB菜单；或者逐个物理地重新放置每个RP，然后按RP控制台上的**ESC**键进入bios GRUB菜单。

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.
```

步骤2.在RP0卡控制台上，从GRUB菜单中选择IOS-XR-recovery选项，然后按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.
```

步骤4.在RP0卡上，创建新的根用户和密码。尝试使用新的根用户名和密码登录设备。

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: █
```

步骤5.此时密码恢复过程已完成。

现在，路由器使用空白配置和步骤4中创建的根用户名/密码启动。继续正常的路由器配置或从备份文件加载配置（在密码恢复过程中存储在disk0或硬盘的任何配置备份都将丢失，因此始终将配置保存在外部服务器上）。确保您在RP0和RP1的RP0控制台日志中看到此消息，作为确认口令恢复的验证步骤，并验证是否已成功完成两个RP的所有旧用户数据清理。否则，请重复先决条件步骤和步骤1.到4。直到在RP0控制台日志中看到这些消息。如果备用RP未看到此消息，则您需要对备用RP重复先决步骤和步骤1.至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

此新密码恢复过程可用于在10分钟内安全重置Cisco 8000系列平台和NCS5500系列平台上丢失的密码。