

Nieuwe wachtwoordherstelprocedure voor Cisco 8000 en NCS 5500 platform

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Probleem](#)

[Oplossing](#)

[Nieuwe stappen voor wachtwoordherstel](#)

[Samenvatting](#)

Inleiding

Dit document beschrijft een nieuw wachtwoordherstelproces voor Cisco IOS®-XR voor Cisco 8000- en NCS 5500-platforms.

Achtergrondinformatie

Als een gebruiker het basiswachtwoord of de wachtwoorden van alle gebruikers vergeet, wordt het verloren op XR7 LNT-platforms (Cisco 8000, NCS-540L) of eXR-platforms (ASR9K 64-bits, NCS5K, NCS 5500, NCS 540, NCS 560), de router wordt ontoegankelijk voor de gebruiker aangezien inloggen niet mogelijk is zonder de juiste combinatie van gebruikersnaam en wachtwoord. Vandaag de dag kan het herstel van een wachtwoord van een dergelijke router alleen plaatsvinden via een router die opnieuw wordt weergegeven met behulp van de USB-opstartmethode of de iPXE-start van een externe server. Herbeeld van router omvat het opnieuw installeren van routersoftware en het laden van de apparaatconfiguratie. Het opnieuw installeren van software is een tijdrovend proces.

Met ingang van de release 7.3.16 voor Cisco 8000 Series platform en 7.3.3 voor NCS 5500 Series platform is Cisco met een nieuwe methode voor het herstel van wachtwoord gekomen zonder dat u de router opnieuw hoeft in te beelden. Voor een dergelijke methode voor het herstellen van het wachtwoord hoeft de software niet opnieuw te worden geïnstalleerd, waardoor tijd wordt bespaard en het opnieuw instellen van het wachtwoord voor de routerpost mogelijk is. Deze nieuwe wachtwoordterugwinningsmethode is veiligheidsnormen die voldoen aan de oude gebruikersinfo en de gegevens van de gebruiker worden uitgewist voordat het wachtwoordterugwinningsproces wordt gestart.

Probleem

Vandaag de dag is het niet mogelijk om wachtwoorden te herstellen op XR7 LNT-platforms (Cisco 8000, NCS-540L) of eXR-platforms (ASR9K 64-bits, NCS5K, NCS 5500, NCS 540, NCS 560). Het enige beschikbare alternatief om het wachtwoord opnieuw in te stellen is om de router opnieuw te bekijken met behulp van de USB-startmethode of de iPXE-start vanaf een externe server. Dit is een tijdrovend proces omdat het nodig is om routersoftware opnieuw te installeren en de configuratie van het apparaat te laden.

Er is een snellere en beveiligde methode voor het herstellen van het wachtwoord op Cisco XR7- en eXR-platforms nodig.

Oplossing

Met ingang van de release 7.3.16 voor Cisco 8000 Series platform en 7.3.3 voor NCS 5500 Series platform is Cisco met een nieuwe methode voor het herstel van wachtwoord gekomen zonder dat u de router opnieuw hoeft in te beelden. In het Grote Unified Bootloader-menu van de routeprocessor (RP), het opstartscherm, wordt een nieuwe optie - "IOS-XR-Restore" toegevoegd, die expliciet wordt gemaakt voor de wachtwoordherstelprocedure. In de routerconfiguratie wordt een nieuw **opdrachtsysteem** voor het inschakelen van de nieuwe wachtwoordterugzetfunctie gecreëerd. Dit is momenteel een optionele optie en is standaard niet ingeschakeld.

Voorzorgen:

- RP bios bootup GRUB schermoptie **IOS-XR-herstel** wordt gezien ongeacht **de grootte van het opdrachtsysteem** die al dan niet is ingesteld in de routerconfiguratie. Als de opdracht voor **systeemherstel** niet aanwezig is in de routerconfiguratie en er een nieuwe wachtwoordterugwinningsmethode wordt gepoogd door de optie **IOS-XR-herstel van het scherm** van de BoB te selecteren, zal de router het wachtwoordherstelproces beëindigen en met de oude configuratie beginnen. Het is dus verplicht om een **systeem terugzetopdracht** op de router te hebben ingesteld zodat de wachtwoordterugwinningsmethode kan werken.
- De optie voor het herstellen van het wachtwoord is standaard uitgeschakeld.
- De optie voor het herstellen van het wachtwoord moet expliciet worden ingeschakeld via de CLI (Configuration Area Interface). `RP/0/RP0/CPU0:HOSTNAME (configuratie)#systeemherstel.`
- Als de router een wachtwoordherstelprocedure ondergaat, wordt de opdracht **voor de systeemherstel** uitgeschakeld aan het eind van de routerconfiguratie, aangezien alle routerconfiguratie zal worden gewist als onderdeel van de wachtwoordherstelprocedure. De gebruikers moeten de apparaatconfiguratie opnieuw laden en de opdracht voor **systeemherstel** configureren als dit geen onderdeel van de apparaatconfiguratie is.
- Naast het wissen van de routerconfiguratie, zullen alle door de gebruiker gemaakte bestanden, technische bestanden tonen, dumperbestanden worden gewist van zowel disk0 als vaste schijf als onderdeel van de reinigingsprocedure tijdens het herstel van het wachtwoord.
- Deze optie wordt momenteel ondersteund op 7.3.16 en hoger op Cisco 8000, 7.3.3 en hoger op NCS 5500 en voor andere XR7 LNT- en eXR-platforms zal deze optie in toekomstige releases beschikbaar worden gesteld.
- Gebruik de gegeven procedure voor platforms waar beide RP-kaarten in chassis zijn geïnstalleerd. Breng beide RP-kaarten naar het GRUB-menu van de bios. Dan moeten de wachtwoordherstelprocedures op elke RP-kaart één voor één worden uitgevoerd. Dit is een verplichte stap voor dubbele RP-platforms, anders zou dit leiden tot een grotere mate van inconsistentie van de configuratie en het opschonen van bestanden.

Nieuwe stappen voor wachtwoordherstel

Voorwaarden: De nieuwe functie voor het herstellen van het wachtwoord werkt alleen als de CLI deel uitmaakt van de apparaatconfiguratie. Als de CLI niet is geconfigureerd dan zal het nieuwe wachtwoordterugwinningsmechanisme niet werken als gevolg van het ontbreken van een configuratie CLI.

De optie voor het herstellen van het wachtwoord inschakelen:

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

Mogelijk wachtwoordherstel uitschakelen:

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

De wachtwoordherstelprocedure moet alleen via de RP-console worden uitgevoerd.

Stap 1. Breng de RP-kaart naar het GRUB-menu van de bios. Voor platforms waar beide RP-kaarten in chassis zijn geïnstalleerd, moeten beide RP-kaarten naar het GRUB-menu van de bios worden gebracht voordat u de wachtwoordherstelprocedure start. Dit is een verplichte stap. Dit kan worden gedaan door een stroomcyclus van het apparaat en druk vervolgens op de ESC-toets op beide RP-consoles om het GRUB-menu van de bios in te voeren of door elke RP één voor één fysiek opnieuw te plaatsen en druk vervolgens op de **ESC**-toets op de RP-console om het GRUB-menu van de bios in te voeren.

RP0- en RP1-kaart:

```
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- en RP1-kaart:

```
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.
```

Stap 2. Selecteer in de RP0-kaartconsole de **IOS-XR-recovery** optie uit het GRUB-menu en druk op **ENTER**.

RP0-kaart:

```
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.
```

Stap 3. Selecteer de **IOS-XR-hersteloctie** uit het GRUB-menu en druk op Voer in op de RP1-kaartconsole, zodra u het bericht Initiating IOS-XR System recovery ziet op de RP0-kaartconsole. Wacht niet tot de RP0-kaart "Voer root-system gebruikersnaam in". Anders wordt de RP1-kaart automatisch opnieuw geladen en wordt het GRUB-menu van de bios afgesloten. De RP0-kaart zal als actief worden opgestart en de RP1-kaart zal opstarten als een stand-by kaart na het herstelproces.

RP0-kaart:

```

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-kaart:

```

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.

```

Stap 4. Voer op de RP0-kaart een nieuwe basisgebruiker en een nieuw wachtwoord in. Probeer met behulp van de nieuwe gebruikersnaam en het wachtwoord in te loggen op het apparaat.

RP0-kaart:

```

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: █

```

Stap 5. De wachtwoordherstelprocedure is op dit punt voltooid.

De router is nu start met een lege configuratie en met de hoofdgebruikersnaam/het wachtwoord dat in stap 4 is gemaakt. Ga verder met de normale routerconfiguratie of laad een configuratie uit een reservekopiebestand (elke configuratie reservekopie die opgeslagen is op disk0 of vaste schijf zal verloren gaan als onderdeel van de wachtwoordherstelprocedure, dus slaat u de configuratie altijd op een externe server op). Verzekert dat u dit bericht in de logbestanden van de RP0-console ziet voor zowel RP0 als RP1, als een verificatiestap ter bevestiging van het herstel van het wachtwoord en om te controleren of alle oude gebruikersgegevens met succes zijn gereinigd voor beide RP. Als niet, herhaal dan de Voorwaarde Stap en Stappen 1. tot 4. tot u deze berichten op de RP0 console ziet. Als dit bericht niet voor standby RP gezien wordt, moet u de Voorwaarde Stap en Stappen 1. t/m 4 herhalen. alleen voor de standby RP.

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

Samenvatting

Deze nieuwe wachtwoordherstelprocedure kan worden gebruikt om verloren wachtwoorden binnen 10 minuten veilig te resetten op Cisco 8000 Series-platform en het NCS 5500 Series-platform.