Nuova procedura di recupero della password sulla piattaforma Cisco 8000 e NCS5500

Sommario

[Introduzione](#)
[Premesse](#)
[Problema](#)
[Soluzione](#)
[Passaggi nuovo recupero password](#)
[Riepilogo](#)

Introduzione

Questo documento descrive un nuovo processo di recupero della password per Cisco IOS®-XR per le piattaforme Cisco 8000 e NCS5500.

Premesse

Se un utente dimentica la password principale o le password di tutti gli utenti vengono perse sulle piattaforme XR7 LNT (Cisco 8000, NCS-540L) o eXR (ASR9K 64-bit, NCS5K, NCS5500, NCS 540, NCS 560), il router diventa inaccessibile per l'utente in quanto l'accesso non è possibile senza la combinazione corretta di nome utente e password. Oggi, il recupero della password di tale router è possibile solo tramite re-image del router con l'uso del metodo di avvio USB o avvio iPXE da un server esterno. La re-immagine del router implica l'installazione del software del router e il caricamento della configurazione del dispositivo. L'installazione di un nuovo software è un processo che richiede molto tempo.

A partire dalla versione 7.3.16 per la piattaforma Cisco serie 8000 e dalla versione 7.3.3 per la piattaforma NCS serie 5500, Cisco ha ideato un nuovo metodo per il recupero della password senza dover creare nuovamente l'immagine del router. Questo metodo di recupero della password non richiede la reinstallazione del software, con un conseguente risparmio di tempo e la possibilità di accedere al router dopo la reimpostazione della password. Questo nuovo metodo di recupero della password è conforme agli standard di sicurezza in quanto le vecchie informazioni utente e i dati di runtime utente vengono cancellati prima dell'avvio del processo di recupero della password.

Problema

Oggi non è possibile recuperare la password su piattaforme XR7 LNT (Cisco 8000, NCS-540L) o eXR (ASR9K a 64 bit, NCS5K, NCS5500, NCS 540, NCS 560). L'unica alternativa disponibile per reimpostare la password consiste nel ricreare l'immagine del router utilizzando il metodo di avvio USB o l'avvio iPXE da un server esterno. Si tratta di un processo che richiede molto tempo in quanto implica l'installazione di nuovo software del router e il caricamento della configurazione del dispositivo.

Ènecessario un metodo più veloce e sicuro per il recupero della password sulle piattaforme Cisco

XR7 e eXR.

Soluzione

A partire dalla versione 7.3.16 per la piattaforma Cisco serie 8000 e dalla versione 7.3.3 per la piattaforma NCS serie 5500, Cisco ha ideato un nuovo metodo per il recupero della password senza dover creare nuovamente l'immagine del router. Nel menu Grand Unified Bootloader (GRUB) della schermata di avvio del Route Processor (RP) viene aggiunta una nuova opzione - "IOS-XR-Recovery" che viene creata esplicitamente per la procedura di recupero della password. Nella configurazione del router, viene creato un nuovo comando **system recovery** per abilitare la nuova funzione di recupero della password. Questa funzionalità è attualmente facoltativa e non è abilitata per impostazione predefinita.

Avvertenze:

- Avvio BIOS RP opzione del menu a schermo GRUB **IOS-XR-recovery** sarà visibile indipendentemente dal comando **system recovery** configurato o non configurato nella configurazione del router. Se il comando **system recovery** non è presente nella configurazione del router e si tenta di utilizzare un nuovo metodo di recupero della password selezionando l'opzione del menu a schermo del BIOS GRUB **IOS-XR-recovery**, il router interromperà il processo di recupero della password e si avvierà con la configurazione precedente. Quindi, per il corretto funzionamento del metodo di recupero della password, è necessario configurare sul router il comando **system recovery**.
- La funzione di recupero della password è disattivata per impostazione predefinita.
- La funzione di recupero della password deve essere abilitata esplicitamente tramite l'interfaccia della riga di comando (CLI) di configurazione.
  RP/0/RP0/CPU0:HOSTNAME(config)**#ripristino del sistema**.

- Se il router viene sottoposto a una procedura di recupero della password, il comando **system recovery** verrà disabilitato dopo l'avvio del router perché tutta la configurazione del router verrà cancellata come parte della procedura di recupero della password. Gli utenti devono caricare di nuovo la configurazione del dispositivo e configurare il comando **system recovery** se non fa parte della configurazione del dispositivo.
- A parte l'eliminazione della configurazione del router, tutti i file creati dall'utente, show tech files, dumper files saranno cancellati sia dal disco0 che dal disco rigido come parte della procedura di pulizia durante il recupero della password.
- Questa funzione è attualmente supportata dalla versione 7.3.16 e successive su Cisco 8000, 7.3.3 e successive su NCS5500 e, per altre piattaforme XR7 LNT e eXR, sarà disponibile nelle versioni future.

- Utilizzare la procedura indicata per le piattaforme in cui entrambe le schede RP sono installate nello chassis. Portare entrambe le schede RP nel menu del BIOS GRUB. Quindi le procedure di recupero della password devono essere eseguite su ciascuna scheda RP uno per uno. Questa operazione è obbligatoria per le piattaforme RP doppie, altrimenti causerebbe incoerenze nella configurazione e nella pulizia dei file.

Passaggi nuovo recupero password

Prerequisito: La nuova funzione di recupero della password funziona solo se la CLI fa parte della configurazione del dispositivo. Se la CLI non è configurata, il nuovo meccanismo di recupero della password non funzionerà a causa della mancanza di config CLI.

Abilita funzionalità di recupero password:

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

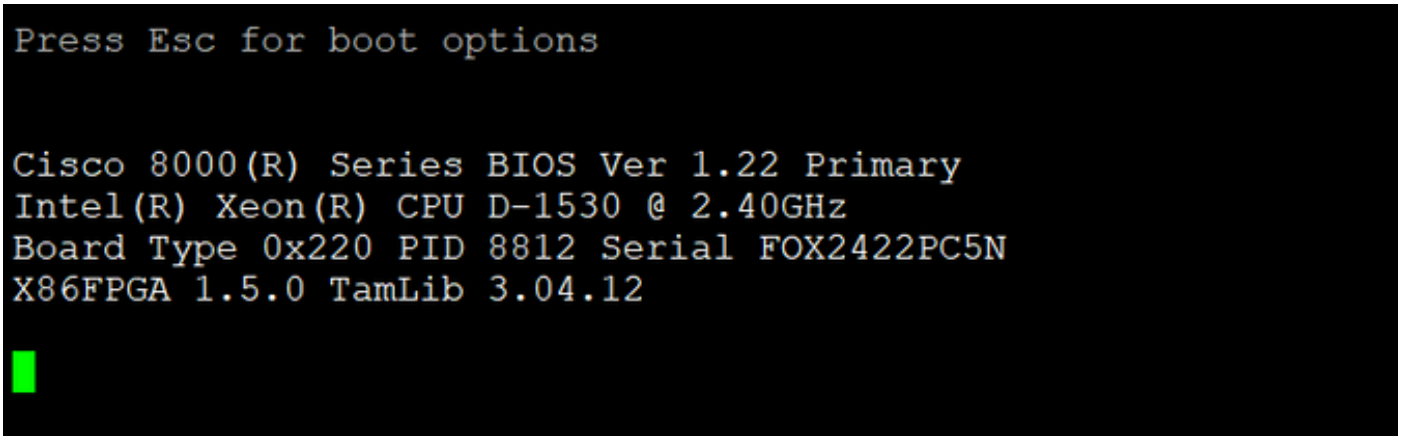
Disabilita funzionalità di recupero password:

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

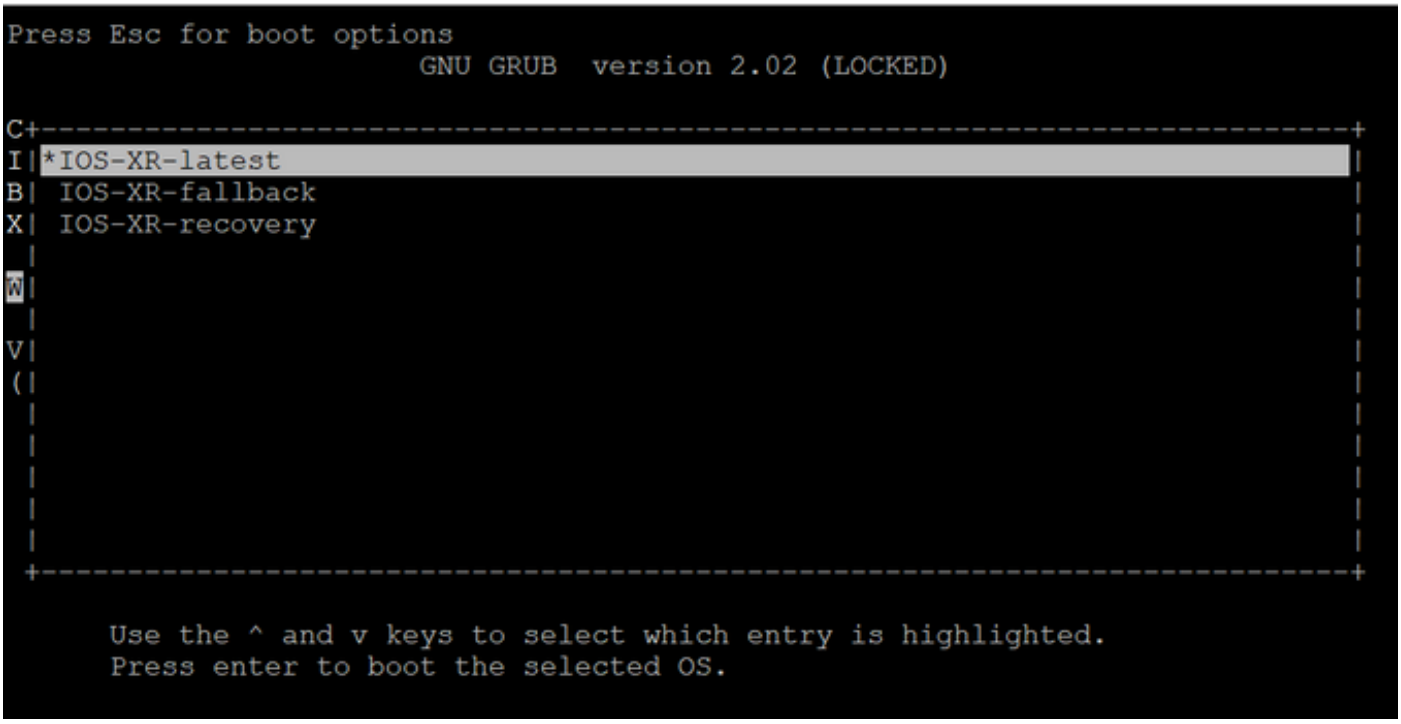
La procedura di recupero della password deve essere eseguita solo tramite la console RP.

Passaggio 1. Riportare la scheda RP nel menu di GRUB del BIOS. Per le piattaforme in cui entrambe le schede RP sono installate nello chassis, prima di avviare la procedura di recupero della password è necessario accedere al menu del BIOS di GRUB. Questa operazione è obbligatoria. A tale scopo, è possibile spegnere e riaccendere il dispositivo e premere ESC su entrambe le console RP per accedere al menu del bios GRUB oppure riposizionare fisicamente ciascun RP uno per uno e quindi premere il tasto **ESC** sulla console RP per accedere al menu del bios GRUB.

RP0 e RP1:

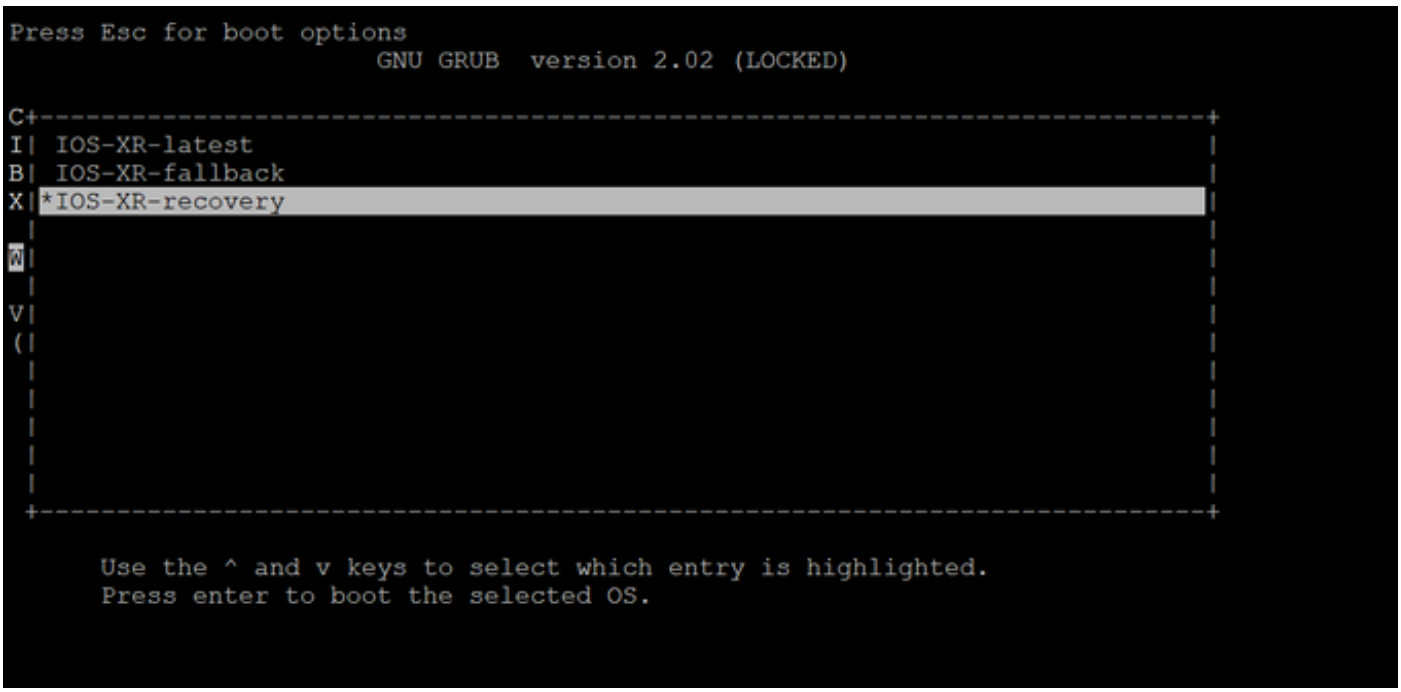


RP0 e RP1:



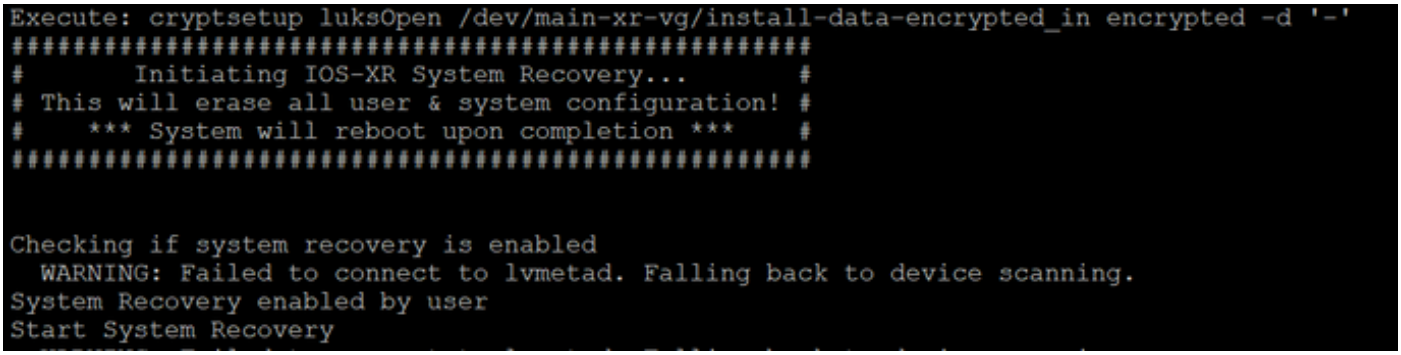
Passaggio 2. Sulla console della scheda RP0, selezionare l'opzione **IOS-XR-recovery** dal menu di GRUB e premere **Invio**.

Scheda RP0:

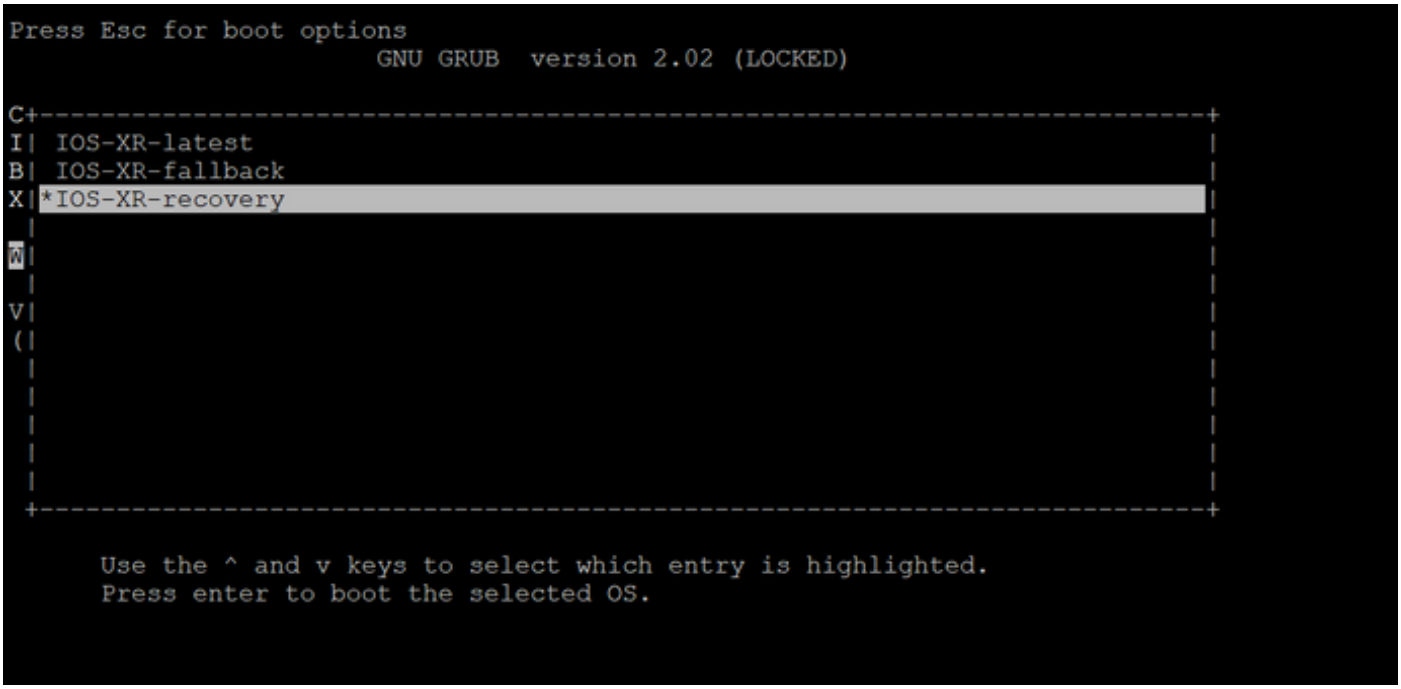


Passaggio 3. Selezionare l'opzione **IOS-XR-recovery** dal menu di GRUB e premere **Invio** sulla console della scheda RP1, non appena viene visualizzato il messaggio Initiating IOS-XR System Recovery... (Avvio del ripristino del sistema IOS-XR in corso) sulla console della scheda RP0. Non attendere che la scheda RP0 raggiunga il prompt "Enter root-system username:" (Immettere il nome utente del sistema radice:), altrimenti la scheda RP1 si ricarica automaticamente e esce dal menu del BIOS di GRUB. La scheda RP0 si avvia come attiva e la scheda RP1 si avvia come scheda di standby dopo il processo di ripristino.

Scheda RP0:

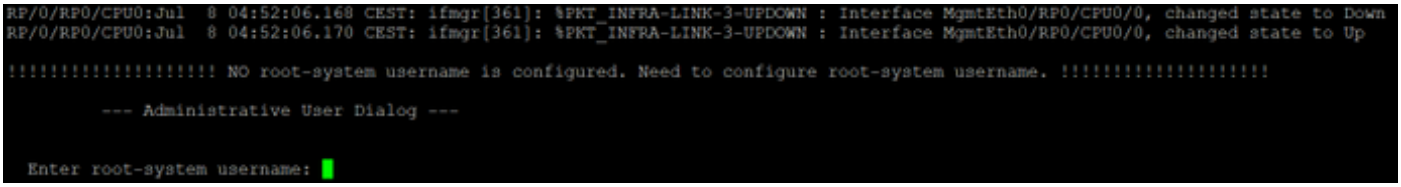


Scheda RP1:



Passaggio 4. Sulla scheda RP0, creare un nuovo utente root e una nuova password. Tentare di accedere al dispositivo utilizzando il nuovo nome utente e la nuova password root.

Scheda RP0:



Passaggio 5. A questo punto, la procedura di recupero della password è completata.

Il router viene ora avviato con una configurazione vuota e con il nome utente/password root creati nel passaggio 4. Procedere con la normale configurazione del router o caricare una configurazione da un file di backup (qualsiasi backup di configurazione archiviato nel disco0 o nel disco rigido andrà perso come parte della procedura di recupero della password, quindi salvare sempre la configurazione su un server esterno). Accertarsi di visualizzare questo messaggio nei log della console RP0 sia per RP0 che per RP1, come passo di verifica per confermare il recupero della password e per verificare che tutta la pulizia dei dati dei vecchi utenti sia stata completata correttamente per entrambi RP. In caso contrario, ripetere i passaggi Prerequisito e da 1 a 4 fino a visualizzare questi messaggi nei log della console RP0. Se questo messaggio non viene visualizzato per l'RP in standby, è necessario ripetere i passi 1 e 4 per l'RP in standby.

```
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
```

Riepilogo

Questa nuova procedura di recupero della password può essere utilizzata per ripristinare in modo sicuro le password perse sulle piattaforme Cisco serie 8000 e NCS serie 5500 in meno di 10 minuti.