Configurazione degli RBAC utente per gli strumenti di backup della configurazione dei dispositivi di rete ossidati o RAID sui dispositivi Cisco Nexus

Sommario

Introduzione

In questo documento viene descritto come configurare gli account utente locali sui dispositivi Cisco Nexus in modo che utilizzino i ruoli RBAC (Role-Based Access Control) limitati ai comandi utilizzati dagli strumenti di backup per la configurazione dei dispositivi di rete ossidati o RAID.

Prerequisiti

Requisiti

Ènecessario disporre dell'accesso ad almeno un account utente in grado di creare altri account utente locali e ruoli RBAC. In genere, questo account utente dispone del ruolo "network-admin" predefinito, ma il ruolo applicabile potrebbe essere diverso per il particolare ambiente di rete e la configurazione.

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione degli account utente in NX-OS
- Come configurare i ruoli RBAC in NX-OS
- Come configurare lo strumento di backup per la configurazione dei dispositivi di rete

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Piattaforma Nexus 9000 NX-OS release 7.0(3)I7(1) o successive

Le informazioni di questo documento riguardano i seguenti strumenti di backup della configurazione dei dispositivi di rete:

- Ossidato v0.26.3
- RANCID v3.9

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

In questa sezione vengono fornite le istruzioni di configurazione per gli strumenti di backup della configurazione dei dispositivi di rete ossidati e RAID.

> **Nota:** Se si utilizza uno strumento di backup della configurazione di un dispositivo di rete diverso, utilizzare le procedure ossidate e RANCID come esempi e modificare le istruzioni in base alla situazione.

Configura account utente e ruolo per ossidato

Come mostrato nel modello NX-OS di Oxidized, Oxidized esegue questo elenco di comandi per impostazione predefinita su qualsiasi dispositivo Cisco Nexus con NX-OS:

- lunghezza terminale 0
- show version
- mostra inventario
- show running-config

Per configurare un account utente autorizzato a eseguire solo questi comandi, eseguire la procedura seguente:

1. Configurare un ruolo RBAC che consenta tali comandi. Nell'esempio seguente, "ossidato" è definito come il nome del ruolo.

```
Nexus# configure terminal
Nexus(config)# role name oxidized
Nexus(config-role)# description Role for Oxidized network device configuration backup tool
Nexus(config-role)# rule 1 permit command terminal length 0
Nexus(config-role)# rule 2 permit command show version
Nexus(config-role)# rule 3 permit command show inventory
Nexus(config-role)# rule 4 permit command show running-config
Nexus(config-role)# end
Nexus#
```

> **Attenzione:** Non dimenticare di aggiungere una regola che autorizza il comando **terminal length 0**, come mostrato nell'esempio precedente. Se questo comando non è consentito, quando esegue il comando **terminal length 0** l'account utente ossidato riceverà un messaggio di errore "% Autorizzazione negata per il ruolo". Se l'output di un comando eseguito da Oxidized supera la lunghezza predefinita del terminale di 24, Oxidized non gestirà correttamente il prompt "—More—" (mostrato di seguito) e genererà un syslog di

avviso "Timeout::Error with msg 'execution exceeded'" (Timeout: errore con l'esecuzione di comandi scaduti nel dispositivo).

```
Nexus# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2019, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source.  This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 08.35
  NXOS: version 7.0(3)I7(6)
--More--    <<<
```

2. Configurare un nuovo account utente che eredita il ruolo configurato nel passaggio 1. Nell'esempio seguente, questo account utente è denominato "ossidato" e la relativa password è "ossidato!123".

```
Nexus# configure terminal
Nexus(config)# username oxidized role oxidized password oxidized!123
Nexus(config)# end
Nexus#
```

3. Accedere manualmente al dispositivo Nexus con il nuovo account utente ossidato e verificare che sia possibile eseguire tutti i comandi necessari senza problemi.
4. Modificare l'origine dati di input di Oxidized in modo che accetti le credenziali dell'account del nuovo account utente Oxidized. Di seguito è riportato un esempio di output di una sorgente CSV con cinque dispositivi Nexus.

```
nexus01.local:192.0.2.1:nxos:oxidized:oxidized!123
nexus02.local:192.0.2.2:nxos:oxidized:oxidized!123
nexus03.local:192.0.2.3:nxos:oxidized:oxidized!123
nexus04.local:192.0.2.4:nxos:oxidized:oxidized!123
nexus05.local:192.0.2.5:nxos:oxidized:oxidized!123
```

Di seguito è riportata la configurazione della fonte ossidata per la fonte CSV sopra indicata.

```
---
source:
  default: csv
  csv:
    file: "/filepath/to/router.db"
    delimiter: !ruby/regexp /:/
    map:
      name: 0
      ip: 1
      model: 2
      username: 3
```

```
password: 4
```

5. Eseguire il comando Oxidized sul file di configurazione e sull'origine dati e verificare che l'output di tutti i comandi venga visualizzato nell'output dei dati configurato. Il comando specifico per fare questo dipenderà dalla vostra implementazione e installazione di Oxidized.

Configura account utente e ruolo per RANCID

Come mostrato nel modello NX-OS di RANCID, per impostazione predefinita RANCID esegue questo elenco di comandi su qualsiasi dispositivo Cisco Nexus con NX-OS:

- terminal no monitor-force
- show version
- show version build-info all
- mostra licenza
- mostra utilizzo licenze
- show license host-id
- mostra stato ridondanza sistema
- mostra orologio di ambiente
- mostra ventola ambiente
- show environment fex all fan
- mostra temperatura ambiente
- mostra potenza ambiente
- mostra avvio
- dir bootflash:
- debug dir:
- dir logflash:
- dir slot0:
- dir usb1:
- dir usb2:
- dir volatile:
- mostra modulo
- show module xbar
- mostra inventario
- show interface transceiver
- show vtp status
- show vlan
- show debug
- show cores vdc-all
- show processes log vdc-all
- show module fex
- mostra fex
- show running-config

Alcuni dei comandi dell'elenco possono essere eseguiti solo da account utente che dispongono del ruolo di amministratore di rete. Anche se il comando è esplicitamente consentito da un ruolo utente personalizzato, gli account utente che dispongono di tale ruolo potrebbero non essere in grado di eseguire il comando e restituiranno un messaggio di errore "%Autorizzazione negata per il ruolo". Questa limitazione è documentata nel capitolo "Configuring User Accounts and RBAC" della guida alla configurazione della sicurezza di ciascuna piattaforma Nexus:

"Indipendentemente dalla regola di lettura/scrittura configurata per un ruolo utente, alcuni comandi possono essere eseguiti solo tramite il ruolo network-admin predefinito."

A seguito di questa limitazione, l'elenco di comandi predefinito di RANCID richiede che il ruolo "network-admin" sia assegnato all'account utente NX-OS utilizzato da RANCID. Per configurare questo account utente, eseguire la procedura seguente:

1. Configurare un nuovo account utente con il ruolo "network-admin". Nell'esempio seguente, questo account utente è denominato "rancid" e ha una password di "rancid!123".
```
Nexus# configure terminal
Nexus(config)# username rancid role network-admin password rancid!123
Nexus(config)# end
Nexus#
```

2. Accedere manualmente al dispositivo Nexus con il nuovo account utente RANCID e verificare che sia possibile eseguire tutti i comandi necessari senza problemi.
3. Modificare il file di configurazione di login di RANCID per utilizzare il nuovo account utente. La procedura per modificare il file di configurazione di accesso varia da un ambiente all'altro, pertanto in questa sezione non vengono forniti dettagli. **Nota:** Il file di configurazione di accesso di RANCID è in genere denominato **.cloginrc**, ma la distribuzione di RANCID potrebbe utilizzare un nome diverso.
4. Eseguire RANCID su un singolo dispositivo Nexus o un set di dispositivi e verificare che tutti i comandi vengano eseguiti correttamente. Il comando specifico per eseguire questa operazione dipende dall'implementazione e dall'installazione di RANCID.

   Nota: Se l'account utente Nexus utilizzato da RANCID non è assolutamente in grado di detenere il ruolo "network-admin" per motivi di sicurezza e se i comandi rilevanti che richiedono questo ruolo non sono necessari nell'ambiente in uso, è possibile rimuovere manualmente tali comandi dall'elenco eseguito da RANCID. Eseguire innanzitutto l'elenco completo dei comandi sopra elencati da un account utente Nexus autorizzato solo a eseguire i comandi sopra indicati. I comandi che richiedono il ruolo "network-admin" restituiranno un messaggio di errore "%Permission negated for the role". È quindi possibile rimuovere manualmente i comandi che hanno restituito il messaggio di errore dall'elenco dei comandi eseguiti da RANCID. La procedura esatta per rimuovere questi comandi non è descritta nel presente documento.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Progetto GitHub ossidato
- Homepage RANCID (Cisco Conflg Differ)

- Capitolo "Configuring User Accounts and RBAC" della guida alla configurazione della sicurezza di Cisco Nexus serie 9000 NX-OS:
  - Release 9.3(x)
  - Release 9.2(x)
  - Release 7.x
  - Release 6.x
- Capitolo "Configuring User Accounts and RBAC" della guida alla configurazione della sicurezza di Cisco Nexus serie 7000 NX-OS:
  - Release 8.x
  - Release 7.x
  - Release 6.x
- Capitolo "Configuring User Accounts and RBAC" della guida alla configurazione della gestione del sistema Cisco Nexus serie 6000 NX-OS
  - Release 7.x
  - Release 6.x
- Capitolo "Configuring User Accounts and RBAC" della Guida alla configurazione della gestione dei sistemi Cisco Nexus serie 5600 NX-OS
  - Release 7.x
- Capitolo "Configuring User Accounts and RBAC" della Guida alla configurazione della gestione dei sistemi Cisco Nexus serie 5500 NX-OS
  - Release 7.x
  - Release 6.x
- Documentazione e supporto tecnico – Cisco Systems