Gebruiker RBAC configureren voor de geoxideerde of RANCID-netwerkconfiguratietools op Cisco Nexus-apparaten

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Configureren](#)
[Gebruikersaccount en -rol instellen voor geoxideerd](#)
[Gebruikersaccount en -rol instellen voor RANCID](#)
[Verifiëren](#)
[Probleemoplossing](#)
[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u lokale gebruikersaccounts op Cisco Nexus-apparaten kunt configureren om Rol-Based Access Control (RBAC) rollen te gebruiken die beperkt zijn tot opdrachten die worden gebruikt door de back-uptools van het geoxideerde of RANCID-netwerkapparaat voor de configuratie van het apparaat.

Voorwaarden

Vereisten

U moet toegang hebben tot ten minste één gebruikersaccount waarmee u andere lokale gebruikersrekeningen en RBAC-rollen kunt maken. Meestal houdt deze gebruikersaccount de standaard 'netwerk-beheerder' rol, maar de toepasselijke rol kan verschillen voor de omgeving en configuratie van uw netwerk.

Cisco raadt kennis van de volgende onderwerpen aan:

- Hoe moet u gebruikersaccounts in NX-OS configureren
- Hoe moet u RBAC-rollen instellen in NX-OS
- Het configureren van de back-up van de netwerkapparaatconfiguratie

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Nexus 9000 platform NX-OS release 7.0(3)I7(1) of hoger

De informatie in dit document bestrijkt deze back-uptools voor de configuratie van netwerkapparaten:

- geoxideerd v0,26,3
- RANCID v3.9

De informatie in dit document is gemaakt van apparatuur in een specifieke labomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Dit gedeelte bevat configuratie-instructies voor de back-uptools van het geoxideerde en RANCID-netwerkapparaat.

> Opmerking: Als u een ander back-upgereedschap voor de configuratie van het netwerkapparaat gebruikt, gebruikt u de geoxideerde en RANCID-procedures als voorbeelden en wijzigt u de instructies naar wens voor uw situatie.

Gebruikersaccount en -rol instellen voor geoxideerd

Zoals gezien in het model NX-OS van Oxidized, voert Oxidized deze lijst van opdrachten door standaard uit op een Cisco Nexus apparaat dat NX-OS in werking stelt:

- eindlengte 0
- show version
- inventaris
- toonaangevend in werking stellen

Om een gebruikersaccount te configureren die alleen deze opdrachten mag uitvoeren, voert u deze procedure uit:

1. Configureer een RBAC rol die deze opdrachten toestaat. In het onderstaande voorbeeld wordt "geoxideerd" gedefinieerd als de naam van de rol.

```
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#
```

> **Voorzichtig:** Vergeet niet een regel toe te voegen die de **eindlengte 0** opdracht toestaat zoals in het bovenstaande voorbeeld wordt getoond. Als deze opdracht niet is toegestaan, dan ontvangt de geoxideerde gebruikersaccount een "% Toestemming geweigerd voor de rol" foutmelding wanneer de **eindlengte 0** opdracht wordt uitgevoerd. Als de uitvoer van een opdracht die door Oxidized is uitgevoerd, de standaard eindlengte van 24 overschrijdt, zal Oxidized de "—More—" melding (hieronder aangetoond) niet scherp behandelen en zal een

"Time-out::Fout met msg "executie verlopen" waarschuwingssignaal opvoeren nadat deze opdrachten op het apparaat uitvoert.

```
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. Configureer een nieuwe gebruikersaccount die de rol erft die u in stap 1 hebt ingesteld. In het onderstaande voorbeeld wordt deze gebruikersaccount aangeduid als "geoxideerd" en heeft deze een wachtwoord van "geoxideerd!123".

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

3. Meld u handmatig aan bij het Nexus-apparaat met de nieuwe geoxideerde gebruikersaccount en controleer of u alle benodigde opdrachten zonder probleem kunt uitvoeren.
4. Wijzig de invoerbron van Oxidized om de rekeningnummers van de nieuwe geoxideerde gebruikersaccount te accepteren. De voorbeelduitvoer van een CSV-bron wordt hieronder met vijf Nexus-apparaten weergegeven.

```
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
```

De relevante geoxideerde bronconfiguratie voor de bovenstaande CSV-bron wordt hieronder weergegeven.

```
---
source:
  default: csv
  csv:
    file: "/filepath/to/router.db"
    delimiter: !ruby/regexp /:/
    map:
      name: 0
```

```
ip: 1
model: 2
username: 3
password: 4
```

5. Voert geOxiseerd uit tegen het configuratiebestand en de gegevensbron en controleer of de uitvoer van alle opdrachten in de geconfigureerde gegevensuitvoer voorkomt. De specifieke opdracht om dit te doen zal afhangen van uw implementatie en installatie van geoxideerd.

Gebruikersaccount en -rol instellen voor RANCID

Zoals te zien is in het NX-OS-model van RANCID voert RANCID deze lijst met opdrachten standaard uit op elk Cisco Nexus-apparaat dat NX-OS draait:

- terminal op het bedieningspaneel
- show version
- volledige versie van bouwinformatie tonen
- vergunning tonen
- licentiegebruik tonen
- host-id voor show
- status voor systeemredundantie tonen
- milieuklok tonen
- show environment fan
- show environment fex gehele ventilator
- omgevingstemperatuur tonen
- energie
- tonen
- extra flitser :
- dir debug:
- dir-logflitser:
- sleuf 0:
- dir usb1:
- dir usb2:
- dir-vluchtig:
- demonstratiemodule
- Module xbar tonen
- inventaris
- interfacetransceiver tonen
- vtp-status tonen
- tonen vlan
- vertonen
- tonen kernen vdc-all
- processen-log-vdc-all weergeven
- show Module fex
- show fex
- toonaangevend in werking stellen

Sommige opdrachten in deze lijst kunnen alleen worden uitgevoerd door gebruikersaccounts die de gebruikersrol van de netwerk-beheerder behouden. Zelfs als de opdracht expliciet is toegestaan door een aangepaste gebruikersrol, gebruikersrekeningen die die rol houden zouden de opdracht niet kunnen uitvoeren en zullen een "%Permission die voor de rol" foutbericht wordt

ontkend teruggeven. Deze beperking is gedocumenteerd in het hoofdstuk "Gebruikersrekeningen en RBAC configureren" van de Security Configuration Guide van elk Nexus-platform:

> *"Ongeacht de lezen-schrijf regel die voor een gebruikersrol wordt gevormd, kunnen sommige opdrachten slechts door de vooraf bepaalde netwerk-beheerder rol worden uitgevoerd."*

Als resultaat van deze beperking vereist de standaard commandolijst van RANCID dat de "network-admin" rol wordt toegewezen aan de NX-OS gebruikersaccount die door RANCID wordt gebruikt. Om deze gebruikersaccount te configureren voert u deze procedure uit:

1. Configuratie van een nieuwe gebruikersaccount met de "netwerk-beheerder" rol. In het onderstaande voorbeeld wordt deze gebruikersaccount "ranzig" genoemd en heeft een wachtwoord van "Rancid!123".
```
Nexus# configure terminal
Nexus(config)# username rancid role network-admin password rancid!123
Nexus(config)# end
Nexus#
```

2. Log handmatig in op het Nexus-apparaat met de nieuwe RANCID-gebruikersaccount en controleer of u alle benodigde opdrachten zonder probleem kunt uitvoeren.
3. Aanpassen van RANCID's logconfiguratiebestand om de nieuwe gebruikersaccount te gebruiken. De procedure om het inlogconfiguratiebestand aan te passen varieert van de ene omgeving tot de andere, dus hier worden geen details gegeven. Opmerking: De loginconfiguratie van RANCID wordt doorgaans **cloginrc** genoemd, maar de inzet van RANCID kan een andere naam hebben.
4. Voer RANCID uit tegen één apparaat of set apparaten van de Nexus en controleer of alle opdrachten met succes worden uitgevoerd. De specifieke opdracht om dit te doen is afhankelijk van uw implementatie en installatie van RANCID.

   Opmerking: Als de gebruikersaccount van Nexus die door RANCID wordt gebruikt, om beveiligingsredenen de "netwerk-beheerder"-rol absoluut niet kan aanhouden en als de opdrachten die deze rol vereisen, niet nodig zijn in uw omgeving, kunt u deze opdrachten handmatig uit de lijst verwijderen die door RANCID wordt uitgevoerd. Start eerst de volledige lijst met opdrachten die hierboven zijn aangegeven vanuit een Nexus-gebruikersaccount die alleen de hiervoor genoemde opdrachten mag uitvoeren. De opdrachten die de rol "network-admin" vereisen, geven een "%Permission terug die wordt ontkend voor de rol" foutmelding. U kunt vervolgens handmatig de opdrachten verwijderen die de foutmelding weergeven in de lijst met opdrachten die door RANCID zijn uitgevoerd. De exacte procedure om deze opdrachten te verwijderen, is niet binnen het bereik van dit document.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Probleemoplossing

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Geoxideerd GigabitHub-project
- RANCID (Echt nieuw Cisco Conflg Differ)-startpagina

- Het hoofdstuk "Gebruikersrekeningen en RBAC configureren" van Cisco Nexus 9000 Series NX-OS security configuratiegids:
  - release 9.3(x)
  - release 9.2(x)
  - release 7.x
  - release 6.x
- "Gebruikersrekeningen en RBAC configureren" hoofdstuk van Cisco Nexus 7000 Series NX-OS security configuratiegids:
  - release 8.x
  - release 7.x
  - release 6.x
- Het hoofdstuk "Gebruikersrekeningen en RBAC configureren" van Cisco Nexus 6000 Series NX-OS systeembeheerdershandleiding
  - release 7.x
  - release 6.x
- Het hoofdstuk "Gebruikersrekeningen en RBAC configureren" van Cisco Nexus 5600 Series NX-OS systeembeheerdershandleiding
  - release 7.x
- Het hoofdstuk "Gebruikersrekeningen en RBAC configureren" van Cisco Nexus 5500 Series NX-OS systeembeheerdershandleiding
  - release 7.x
  - release 6.x
- Technische ondersteuning en documentatie – Cisco Systems