Configurer RBAC utilisateur pour les outils de sauvegarde de configuration des périphériques réseau Oxidized ou RANCID sur les périphériques Cisco Nexus

Contenu

Introduction

Ce document décrit comment configurer des comptes d'utilisateurs locaux sur des périphériques Cisco Nexus pour utiliser des rôles RBAC (Role-Based Access Control) qui sont limités aux commandes utilisées par les outils de sauvegarde de configuration de périphérique réseau Oxidized ou RANCID.

Conditions préalables

Conditions requises

Vous devez avoir accès à au moins un compte d'utilisateur qui peut créer d'autres comptes d'utilisateur locaux et rôles RBAC. En règle générale, ce compte d'utilisateur possède le rôle d'« administrateur réseau » par défaut, mais le rôle applicable peut être différent pour votre environnement et votre configuration réseau particuliers.

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Comment configurer des comptes d'utilisateurs dans NX-OS
- Configuration des rôles RBAC dans NX-OS
- Configuration de l'outil de sauvegarde de la configuration de votre périphérique réseau

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

- Plate-forme NX-OS version 7.0(3)I7(1) ou ultérieure de la plate-forme Nexus 9000

Les informations de ce document couvrent les outils de sauvegarde de configuration des périphériques réseau suivants :

- Oxide v0.26.3
- RANCID v3.9

Les informations contenues dans ce document ont été créées à partir des périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

Cette section fournit des instructions de configuration pour les outils de sauvegarde de configuration des périphériques réseau Oxidized et RANCID.

> **Note**: Si vous utilisez un autre outil de sauvegarde de configuration de périphérique réseau, utilisez les procédures Oxidized et RANCID comme exemples et modifiez les instructions en fonction de votre situation.

Configurer le compte d'utilisateur et le rôle pour Oxidified

Comme le montre le modèle NX-OS d'Oxidized, Oxidized exécute cette liste de commandes par défaut sur n'importe quel périphérique Cisco Nexus qui exécute NX-OS :

- longueur de terminal 0
- show version
- show inventaire
- show running-config

Pour configurer un compte d'utilisateur autorisé à exécuter uniquement ces commandes, procédez comme suit :

1. Configurez un rôle RBAC qui autorise ces commandes. Dans l'exemple ci-dessous, « oxidized » est défini comme le nom du rôle.

```
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#
```

> **Attention** : N'oubliez pas d'ajouter une règle autorisant la commande **terminal length 0** comme indiqué dans l'exemple ci-dessus. Si cette commande n'est pas autorisée, le compte d'utilisateur Oxidized recevra un message d'erreur "% Permission deny for the role » lorsqu'il exécutera la commande **terminal length 0**. Si la sortie d'une commande exécutée par

Oxidized dépasse la longueur de terminal par défaut de 24, Oxidized ne gère pas avec grâce l'invite "—More—" (illustrée ci-dessous) et déclenche un syslog d'avertissement « Timeout::Error with msg 'exécution expirée'" après avoir exécuté des commandes sur le périphérique.

```
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. Configurez un nouveau compte d'utilisateur qui hérite du rôle que vous avez configuré à l'étape 1. Dans l'exemple ci-dessous, ce compte d'utilisateur est nommé « oxidized » et possède le mot de passe « oxidized !123 ».

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

3. Connectez-vous manuellement au périphérique Nexus avec le nouveau compte d'utilisateur Oxidized et vérifiez que vous pouvez exécuter toutes les commandes nécessaires sans problème.
4. Modifiez la source de données d'entrée d'Oxidized pour accepter les informations d'identification du compte du nouveau compte d'utilisateur Oxidized. L'exemple de sortie d'une source CSV est présenté ci-dessous avec cinq périphériques 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
```

La configuration de source Oxidized appropriée pour la source CSV ci-dessus est présentée ci-dessous.

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

```
map:
  name: 0
  ip: 1
  model: 2
  username: 3
  password: 4
```

5. Exécutez Oxidized avec le fichier de configuration et la source de données et vérifiez que le résultat de toutes les commandes apparaît dans la sortie de données configurée. La commande spécifique pour cela dépendra de votre implémentation et de votre installation d'Oxidized.

Configurer le compte d'utilisateur et le rôle pour RANCID

Comme le montre le modèle NX-OS de RANCID, RANCID exécute cette liste de commandes par défaut sur tout périphérique Cisco Nexus qui exécute NX-OS :

- terminal no monitor-force
- show version
- show version build-info all
- show license
- show license usage
- show license host-id
- show system redundancy status
- show environment clock
- show environment fan
- show environment fex all fan
- show environment températures
- show environment power
- show boot
- dir bootflash:
- dir debug :
- dir logflash:
- dir slot0 :
- dir usb1 :
- dir usb2 :
- dir volatile :
- show module
- show module xbar
- show inventaire
- show interface émetteurs
- show vtp status
- show vlan
- show debug
- show cores vdc-all
- show processes log vdc-all
- show module fex
- show fex
- show running-config

Certaines commandes de cette liste ne peuvent être exécutées que par des comptes d'utilisateurs

qui détiennent le rôle d'utilisateur admin réseau. Même si la commande est explicitement autorisée par un rôle d'utilisateur personnalisé, les comptes d'utilisateurs qui détiennent ce rôle risquent de ne pas pouvoir exécuter la commande et retourneront un message d'erreur "%Permission refusée pour le rôle ». Cette limitation est documentée dans le chapitre « Configuration des comptes d'utilisateurs et RBAC » du Guide de configuration de la sécurité de chaque plate-forme Nexus :

> *« Quelle que soit la règle de lecture-écriture configurée pour un rôle d'utilisateur, certaines commandes ne peuvent être exécutées que via le rôle prédéfini network-admin. »*

En raison de cette limitation, la liste de commandes par défaut de RANCID nécessite que le rôle « network-admin » soit attribué au compte d'utilisateur NX-OS utilisé par RANCID. Pour configurer ce compte d'utilisateur, procédez comme suit :

1. Configurez un nouveau compte d'utilisateur avec le rôle « network-admin ». Dans l'exemple ci-dessous, ce compte d'utilisateur est nommé « rancid » et a le mot de passe « rancid !123 ».

```
Nexus# configure terminal
Nexus(config)# username rancid role network-admin password rancid!123
Nexus(config)# end
Nexus#
```

2. Connectez-vous manuellement au périphérique Nexus avec le nouveau compte utilisateur RANCID et vérifiez que vous pouvez exécuter toutes les commandes nécessaires sans problème.
3. Modifiez le fichier de configuration de connexion de RANCID pour utiliser le nouveau compte d'utilisateur. La procédure de modification du fichier de configuration de connexion varie d'un environnement à l'autre, de sorte que les détails ne sont pas fournis ici. **Note**: Le fichier de configuration de connexion de RANCID est généralement nommé **.cloginrc**, mais votre déploiement de RANCID peut utiliser un nom différent.
4. Exécutez RANCID sur un seul périphérique ou ensemble de périphériques Nexus et vérifiez que toutes les commandes s'exécutent correctement. La commande spécifique pour cela dépend de votre implémentation et installation de RANCID.

   Note: Si le compte d'utilisateur Nexus utilisé par RANCID ne peut absolument pas contenir le rôle « network-admin » pour des raisons de sécurité et si les commandes pertinentes qui nécessitent ce rôle ne sont pas nécessaires dans votre environnement, vous pouvez supprimer manuellement ces commandes de la liste qui est exécutée par RANCID. Tout d'abord, exécutez la liste complète des commandes ci-dessus à partir d'un compte d'utilisateur Nexus qui n'est autorisé qu'à exécuter les commandes mentionnées ci-dessus. Les commandes qui nécessitent le rôle « network-admin » retourneront un message d'erreur "%Permission refusée pour le rôle ». Vous pouvez ensuite supprimer manuellement les commandes qui ont renvoyé le message d'erreur de la liste des commandes exécutées par RANCID. La procédure exacte de suppression de ces commandes n'est pas comprise dans ce document.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Projet GitHub oxydé
- Page d'accueil RANCID (Really Awesome New Cisco Conflg Differ)

- Chapitre « Configuring User Accounts and RBAC » du Guide de configuration de la sécurité NX-OS de la gamme Cisco Nexus 9000 :
  - Version 9.3(x)
  - Version 9.2(x)
  - Version 7.x
  - Version 6.x
- Chapitre « Configuring User Accounts and RBAC » du Guide de configuration de la sécurité NX-OS de la gamme Cisco Nexus 7000 :
  - Version 8.x
  - Version 7.x
  - Version 6.x
- Chapitre « Configuration des comptes d'utilisateurs et RBAC » du Guide de configuration de la gestion du système NX-OS de la gamme Cisco Nexus 6000
  - Version 7.x
  - Version 6.x
- Chapitre « Configuration des comptes d'utilisateurs et RBAC » du Guide de configuration de la gestion du système NX-OS de la gamme Cisco Nexus 5600
  - Version 7.x
- Chapitre « Configuration des comptes d'utilisateurs et RBAC » du Guide de configuration de la gestion du système NX-OS de la gamme Cisco Nexus 5500
  - Version 7.x
  - Version 6.x
- Support et documentation techniques - Cisco Systems