Konfigurieren Sie die Benutzer-RBAC für die oxidierten oder RANCID-Netzwerkgerätekonfigurations-Sicherungstools auf Cisco Nexus-Geräten.

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie lokale Benutzerkonten auf Cisco Nexus-Geräten so konfiguriert werden, dass sie RBAC-Rollen (Role-Based Access Control) verwenden, die auf Befehle beschränkt sind, die von Backup-Tools für die Oxidierte oder RANCID-Netzwerkgerätekonfiguration verwendet werden.

Voraussetzungen

Anforderungen

Sie müssen auf mindestens ein Benutzerkonto zugreifen können, das andere lokale Benutzerkonten und RBAC-Rollen erstellen kann. In der Regel verfügt dieses Benutzerkonto über die Standard-Rolle "network-admin". Die entsprechende Rolle kann jedoch je nach Netzwerkumgebung und -konfiguration unterschiedlich sein.

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Konfigurieren von Benutzerkonten in NX-OS
- Konfigurieren von RBAC-Rollen in NX-OS
- Konfigurieren des Backup-Tools für die Konfiguration von Netzwerkgeräten

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und

Hardwareversionen:

- Nexus 9000-Plattform NX-OS 7.0(3)I7(1) oder höher

Die Informationen in diesem Dokument behandeln die folgenden Backup-Tools für die Konfiguration von Netzwerkgeräten:

- Oxidiert v0.26.3
- RANCID v3.9

Die Informationen in diesem Dokument wurden von Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Dieser Abschnitt enthält Konfigurationsanweisungen für die Backup-Tools für die Oxidierte und RANCID-Netzwerkgerätekonfiguration.

> **Hinweis**: Wenn Sie ein anderes Sicherungstool für die Konfiguration von Netzwerkgeräten verwenden, verwenden Sie als Beispiele die Oxidationsverfahren und RANCID-Verfahren, und ändern Sie die Anweisungen entsprechend Ihrer Situation.

Konfigurieren des Benutzerkontos und der Rolle für oxidiertes Gerät

Wie im NX-OS-Modell von Oxidated zu sehen ist, wird diese Befehlsliste standardmäßig auf jedem Cisco Nexus-Gerät ausgeführt, das NX-OS ausführt:

- Anschlusslänge 0
- Anzeigeversion
- Bestand anzeigen
- show running-config

So konfigurieren Sie ein Benutzerkonto, das nur diese Befehle ausführen darf:

1. Konfigurieren Sie eine RBAC-Rolle, die diese Befehle zulässt. Im folgenden Beispiel wird "oxidiert" als Rollenname definiert.

```
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#
```

> **Vorsicht**: Vergessen Sie nicht, eine Regel hinzuzufügen, die den Befehl **Terminal-Länge 0** zulässt, wie im Beispiel oben gezeigt. Wenn dieser Befehl nicht zulässig ist, wird beim Ausführen des Befehls **Terminal length 0** eine Fehlermeldung mit der Fehlermeldung "% Permission weigert for the role" angezeigt, wenn das Benutzerkonto **oxidiert**. Wenn die Ausgabe eines Befehls, der durch Oxidated ausgeführt wird, die standardmäßige

Terminallänge von 24 überschreitet, verarbeitet Oxidated nicht ordnungsgemäß die Eingabeaufforderung "- More—" (weiter unten gezeigt) und löst ein Warnsyslog mit der Meldung "Timeout::Error with msg 'Execution abgelaufen" aus, nachdem es Befehle auf dem Gerät ausführt.

```
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. Konfigurieren Sie ein neues Benutzerkonto, das die in Schritt 1 konfigurierte Rolle übernimmt. Im folgenden Beispiel heißt dieses Benutzerkonto "oxidiert" und hat das Kennwort "oxidiert!123".

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

3. Melden Sie sich mit dem neuen oxidierten Benutzerkonto manuell beim Nexus-Gerät an, und überprüfen Sie, ob Sie alle erforderlichen Befehle fehlerfrei ausführen können.
4. Ändern Sie die Eingabedaten von Oxidized, um die Kontoanmeldeinformationen des neuen oxidierten Benutzerkontos zu akzeptieren. Im Folgenden finden Sie eine Beispielausgabe einer CSV-Quelle mit fünf Nexus-Geräten.

```
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
```

Die relevante oxidierte Quellkonfiguration für die obige CSV-Quelle ist unten aufgeführt.

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

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

5. Führen Sie Oxidated für die Konfigurationsdatei und die Datenquelle aus, und überprüfen Sie, ob die Ausgabe aller Befehle in der konfigurierten Datenausgabe angezeigt wird. Der genaue Befehl dazu hängt von Ihrer Implementierung und Installation von Oxidated ab.

Konfigurieren des Benutzerkontos und der Rolle für RANCID

Wie im NX-OS-Modell von RANCID gezeigt, führt RANCID diese Befehlsliste standardmäßig auf jedem Cisco Nexus-Gerät aus, das NX-OS ausführt:

- Terminal ohne Monitorkraft
- Anzeigeversion
- show version buildinfo all
- Lizenz anzeigen
- Lizenznutzung anzeigen
- show license host-id
- Anzeige des Systemredundanzstatus
- show environment clock
- show environment fan
- show environment alle Fans federn
- Umgebungstemperatur anzeigen
- Anzeige von Umgebungsleistung
- show boot
- dir-Bootflash:
- dir-Debuggen:
- Verzeichnis-Logflash:
- dir-Steckplatz0:
- dir usb1:
- dir usb2:
- Verzeichnis flüchtig:
- Schaumodul
- show module xbar
- Bestand anzeigen
- Show Interface Transceiver
- VTP-Status anzeigen
- Show-VLAN
- Debuggen anzeigen
- show cores vdc all
- show process log vdc all
- show module fex
- FEX anzeigen
- show running-config

Einige der Befehle in dieser Liste können nur von Benutzerkonten ausgeführt werden, die die Rolle "network-admin" besitzen. Selbst wenn der Befehl explizit von einer benutzerdefinierten Benutzerrolle zugelassen wird, können Benutzerkonten, die diese Rolle besitzen, den Befehl möglicherweise nicht ausführen und eine Fehlermeldung mit der Angabe "%Permission verweigert

für die Rolle" zurückgeben. Diese Einschränkung ist im Kapitel "Konfigurieren von Benutzerkonten und RBAC" des Sicherheitskonfigurationsleitfadens jeder Nexus-Plattform dokumentiert:

> *"Unabhängig von der für eine Benutzerrolle konfigurierten Lese- und Schreibregel können einige Befehle nur über die vordefinierte Netzwerkadministratorrolle ausgeführt werden."*

Aufgrund dieser Einschränkung erfordert die standardmäßige Befehlsliste von RANCID, dass die Rolle "network-admin" dem von RANCID verwendeten NX-OS-Benutzerkonto zugewiesen wird. So konfigurieren Sie dieses Benutzerkonto:

1. Konfigurieren Sie ein neues Benutzerkonto mit der Rolle "network-admin". Im folgenden Beispiel heißt dieses Benutzerkonto "rancid" und hat das Kennwort "rancid!123".
```
Nexus# configure terminal
Nexus(config)# username rancid role network-admin password rancid!123
Nexus(config)# end
Nexus#
```
2. Melden Sie sich manuell mit dem neuen RANCID-Benutzerkonto beim Nexus-Gerät an, und überprüfen Sie, ob Sie alle erforderlichen Befehle ohne Probleme ausführen können.
3. Ändern Sie die Anmeldekonfigurationsdatei von RANCID, um das neue Benutzerkonto zu verwenden. Das Verfahren zum Ändern der Anmeldungskonfigurationsdatei ist von Umgebung zu Umgebung unterschiedlich, daher werden hier keine Details angegeben. **Hinweis**: Die Anmelde-Konfigurationsdatei von RANCID heißt in der Regel **.cloginrc**, aber bei der Bereitstellung von RANCID kann ein anderer Name verwendet werden.
4. Führen Sie RANCID für ein einzelnes Nexus-Gerät oder eine Reihe von Geräten aus, und überprüfen Sie, ob alle Befehle erfolgreich ausgeführt werden. Der genaue Befehl dazu hängt von Ihrer Implementierung und Installation von RANCID ab.

   Hinweis: Wenn das von RANCID verwendete Nexus-Benutzerkonto aus Sicherheitsgründen absolut nicht über die Rolle "network-admin" verfügen kann und wenn die relevanten Befehle, die diese Rolle erfordern, in Ihrer Umgebung nicht erforderlich sind, können Sie diese Befehle manuell aus der Liste entfernen, die von RANCID ausgeführt wird. Führen Sie zunächst die vollständige Liste der oben gezeigten Befehle aus einem Nexus-Benutzerkonto aus, das nur die oben genannten Befehle ausführen darf. Die Befehle, die die Rolle "network-admin" erfordern, geben die Fehlermeldung "%Permission verweigert für die Rolle" zurück. Anschließend können Sie die Befehle, die die Fehlermeldung zurückgegeben haben, manuell aus der Liste der von RANCID ausgeführten Befehle entfernen. Das genaue Verfahren zum Entfernen dieser Befehle liegt außerhalb des Anwendungsbereichs dieses Dokuments.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Oxidiertes GitHub-Projekt
- RANCID (wirklich fantastische neue Cisco Conflg-Angebot) Homepage

- Kapitel "Konfigurieren von Benutzerkonten und RBAC" des Cisco Nexus NX-OS Security Configuration Guide der Serie 9000:
  - Version 9.3(x)
  - Version 9.2(x)
  - Version 7.x
  - Version 6.x
- Kapitel "Konfigurieren von Benutzerkonten und RBAC" des Cisco Nexus NX-OS Security Configuration Guide der Serie 7000:
  - Version 8.x
  - Version 7.x
  - Version 6.x
- Kapitel "Konfigurieren von Benutzerkonten und RBAC" des Konfigurationsleitfadens zur Systemverwaltung für die Cisco Nexus Serie 6000
  - Version 7.x
  - Version 6.x
- Kapitel "Konfigurieren von Benutzerkonten und RBAC" des Konfigurationsleitfadens zur Systemverwaltung für die Cisco Nexus Serie 5600
  - Version 7.x
- Kapitel "Konfigurieren von Benutzerkonten und RBAC" des Konfigurationsleitfadens zur Systemverwaltung für die Cisco Nexus Serie 5500
  - Version 7.x
  - Version 6.x
- Technischer Support und Dokumentation - Cisco Systems