在Cisco Nexus裝置上配置使用者RBAC以使用氧化或變質網路裝置配置備份工具

目錄

簡介

本檔案介紹如何在Cisco Nexus裝置上配置本地使用者帳戶，以使用僅限於氧化或變質網路裝置配置備份工具使用的命令的基於角色的訪問控制(RBAC)角色。

必要條件

需求

您必須擁有至少一個可以建立其他本地使用者帳戶和RBAC角色的使用者帳戶的訪問許可權。通常情況下，此使用者帳戶擁有預設的「network-admin」角色，但是對於您的特定網路環境和配置，適用的角色可能不同。

思科建議您瞭解以下主題：

- 如何在NX-OS中配置使用者帳戶
- 如何在NX-OS中配置RBAC角色
- 如何配置網路裝置配置備份工具

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Nexus 9000平台NX-OS版本7.0(3)I7(1)或更高版本

本檔案中的資訊涵蓋了以下網路裝置組態備份工具：

- 氧化v0.26.3
- RANCID v3.9

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

本節提供Oxidiated和RANCID網路裝置配置備份工具的配置說明。

> **附註**：如果您使用不同的網路裝置配置備份工具，請以氧化和變質過程為例，並根據您的具體情況修改說明。

配置氧化使用者的使用者帳戶和角色

如在Oxidiated的NX-OS模型中,Oxidiated在運行NX-OS的任何Cisco Nexus裝置上預設執行以下命令清單：

- 終端長度0
- 顯示版本
- 顯示庫存
- show running-config

要配置僅允許執行這些命令的使用者帳戶，請執行以下步驟：

1. 配置允許這些命令的RBAC角色。在下面的示例中，「oxidiated」被定義為角色名稱。

```
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#
```

> **注意**：不要忘記新增允許**terminal length 0**命令的規則，如上例所示。如果不允許使用此命令，則在執行終端長度0命令時，Oxidied使用者帳戶將收到「% Permission denied for the role」錯**誤消**息。如果Oxidiated執行的命令的輸出超過預設終端長度24,Oxidiated將不優雅地處理「 — More — 」提示（如下所示），並在裝置上執行命令後發出「Timeout::Error with msg 'execution expired'」警告系統日誌。

```
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. 配置一個新使用者帳戶，該使用者帳戶繼承您在步驟1中配置的角色。在下面的示例中，該使用者帳戶名為"oxidied"，其密碼為"oxidiated!123"。

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

3. 使用新的Oxidied使用者帳戶手動登入到Nexus裝置，並驗證您可以執行所有必要的命令而沒有出現問題。
4. 修改Oxidied的輸入資料來源以接受新Oxidied使用者帳戶的帳戶憑據。CSV源的輸出示例如下所示，包含五個Nexus裝置。

```
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
```

   上述CSV源的相關氧化源配置如下所示。

```
---
source:
  default: csv
  csv:
    file: "/filepath/to/router.db"
    delimiter: !ruby/regexp /:/
    map:
      name: 0
      ip: 1
      model: 2
      username: 3
      password: 4
```

5. 對配置檔案和資料來源執行Oxidiated，並驗證所有命令的輸出是否出現在配置的資料輸出中。具體操作命令取決於您實施和安裝Oxidiated。

為RANCID配置使用者帳戶和角色

如RANCID的NX-OS模型所示，RANCID預設在運行NX-OS的任何Cisco Nexus裝置上執行此命令清單：

- terminal no monitor-force
- 顯示版本
- show version build-info all
- 顯示許可證
- 顯示許可證使用情況
- show license host-id
- 顯示系統冗餘狀態
- 顯示環境時鐘

- 顯示環境風扇
- show environment fex all fan
- 顯示環境溫度
- 顯示環境功率
- show boot
- dir bootflash:
- dir debug:
- dir logflash:
- dir slot0:
- dir usb1:
- dir usb2:
- dir volatile:
- show module
- show module xbar
- 顯示庫存
- show interface transceiver
- show vtp status
- show vlan
- show debug
- show cores vdc-all
- show processes log vdc-all
- show module fex
- show fex
- show running-config

此清單中的某些命令只能由具有network-admin使用者角色的使用者帳戶執行。即使自定義使用者角色明確允許該命令，擁有該角色的使用者帳戶也可能無法執行該命令，並返回「%拒絕該角色的許可權」錯誤消息。每個Nexus平台的安全配置指南的「配置使用者帳戶和RBAC」一章中記錄了此限制:

無論為使用者角色配置了讀寫規則，某些命令都只能通過預定義的network-admin角色執行。

由於此限制，RANCID的預設命令清單要求將「network-admin」角色分配給RANCID使用的NX-OS使用者帳戶。要配置此使用者帳戶，請執行以下步驟：

1. 配置具有「network-admin」角色的新使用者帳戶。在下面的示例中，此使用者帳戶名為「rancid」，密碼為「rancid!123」。

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

2. 使用新的RANCID使用者帳戶手動登入到Nexus裝置，並驗證您能夠順利執行所有必要的命令。
3. 修改RANCID的登入配置檔案以使用新使用者帳戶。修改登入配置檔案的過程因環境而異，因此此處不提供詳細資訊。 **附註**：RANCID的登入配置檔案通常命名為**.cloginrc**，但您的RANCID部署可能使用不同的名稱。
4. 對單個Nexus裝置或一組裝置執行RANCID，並驗證所有命令是否成功執行。具體操作命令取決於您的RANCID實施和安裝。

附註：如果RANCID使用的Nexus使用者帳戶出於安全原因絕對不能擁有「network-admin」

角色，並且您的環境中不需要需要此角色的相關命令，則您可以手動從RANCID執行的清單中刪除這些命令。首先，從只允許運行上述命令的Nexus使用者帳戶執行上面顯示的命令完整清單。需要「network-admin」角色的命令將返回「%Permission denied for the role」錯誤消息。然後，您可以手動從RANCID執行的命令清單中刪除返回錯誤消息的命令。移除這些命令的準確程式不在本檔案的範圍之內。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 氧化GitHub專案
- RANCID(Really Excellent New Cisco Conflg Different)首頁
- Cisco Nexus 9000系列NX-OS安全配置指南的「配置使用者帳戶和RBAC」一章：
  - 版本9.3(x)
  - 版本9.2(x)
  - 版本7.x
  - 版本6.x
- Cisco Nexus 7000系列NX-OS安全配置指南的「配置使用者帳戶和RBAC」一章：
  - 版本8.x
  - 版本7.x
  - 版本6.x
- Cisco Nexus 6000系列NX-OS系統管理配置指南的「配置使用者帳戶和RBAC」一章
  - 版本7.x
  - 版本6.x
- Cisco Nexus 5600系列NX-OS系統管理配置指南的「配置使用者帳戶和RBAC」一章
  - 版本7.x
- Cisco Nexus 5500系列NX-OS系統管理配置指南的「配置使用者帳戶和RBAC」一章
  - 版本7.x
  - 版本6.x
- 技術支援與文件 - Cisco Systems