Nexus N5500、5600和N6000角色型存取控制(RBAC)

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[使用者要求](#)
[使用者角色](#)
[使用者角色規則](#)
[使用者角色分佈](#)
[配置和Show命令](#)
[清除使用者角色分發會話](#)
[組態範例](#)
[許可要求](#)
[驗證](#)
[疑難排解](#)

簡介

本文說明如何使用角色基礎訪問控制(RBAC)限制使用者訪問Nexus 5500、Nexus 5600和Nexus 6000交換機。

RBAC允許您為分配的使用者角色定義規則，以限制對交換機管理操作具有訪問許可權的使用者的授權。

您可以建立和管理使用者帳戶，並分配限制對Nexus 5500、Nexus 5600和Nexus 6000交換機的訪問許可權的角色。

必要條件

需求

思科建議您瞭解以下主題：

- Nexus 5500、Nexus 5600、Nexus 6000交換機CLI配置命令
- Cisco Fabric Services(CFS)。

採用元件

本文檔中的資訊基於運行NXOS 5.2(1)N1(9)7.3(1)N1(1)的Nexus 5500、Nexus 5600和Nexus 6000交換機。

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。

使用者要求

以下是需要滿足的一些使用者要求：

- 只有具有網路管理員角色的使用者才能建立角色。
- 只有具有網路管理員角色的使用者才能檢視**show role**的輸出。
- 即使允許使用者執行所有show命令，也不允許他們檢視**show role**輸出，除非這些使用者分配了network-admin角色。
- 使用者帳戶必須至少具有一個使用者角色。

使用者角色

可以將每個角色分配給多個使用者，並且每個使用者可以是多個角色的一部分。

例如，允許角色A使用者發出show命令，允許角色B使用者進行配置更改。

如果將使用者同時分配給角色A和角色B，則此使用者可以發出show命令並更改配置。

Permit access命令的優先順序高於deny access命令。

例如，如果您屬於拒絕訪問配置命令的角色。

但是，如果您還屬於有權訪問配置命令的角色，則您便有權訪問配置命令。

有五個預設使用者角色：

- network-admin — 對整個交換機進行完全讀寫訪問。
- network-operator — 對整個交換機進行完全讀取訪問。
- vdc-admin — 限於VDC的讀寫訪問
- vdc-operator — 限於VDC的讀取訪問
- san-admin — 對SAN管理員具有完整的讀寫訪問許可權。

注意：您不能修改/刪除預設使用者角色。

附註：**show role命**令會顯示交換器上可用的角色

使用者角色規則

規則是角色的基本元素。

規則定義角色允許使用者執行的操作。

您可以為這些引數應用規則：

- 命令 — 在正規表示式中定義的命令或命令組。

- 功能 — 適用於NX-OS軟體提供的功能的命令。
- 功能組 — 預設或使用者定義的功能組。

這些引數建立分層關係。最基本的控制引數是命令。

下一個控制引數是特徵，表示與該特徵關聯的所有命令。

最後一個控制引數是特徵組。該功能組結合了相關功能，使您可以輕鬆管理規則。

使用者指定的規則編號決定規則的應用順序。

規則按降序應用。

例如，規則1應用於規則2之前，規則3之前應用，依此類推。

rule命令指定可由特定角色執行的操作。每個規則都包含一個規則編號、一個規則型別（允許或拒絕）、

命令型別（例如configuration、show、exec、debug）和可選功能名稱（例如FCOE、HSRP、VTP、interface）。

使用者角色分佈

基於角色的配置使用Cisco Fabric Services(CFS)基礎設施實現高效的資料庫管理，並在網路中提供單點配置。

當您在裝置上為某個功能啟用CFS分配時，該裝置屬於包含網路中其他裝置的CFS區域，您也為該功能啟用了CFS分配。預設情況下禁用使用者角色功能的CFS分配。

必須在要向其分發配置更改的每個裝置上為使用者角色啟用CFS。

為交換機上的使用者角色啟用CFS分發後，您輸入的第一個使用者角色配置命令會導致交換機NX-OS軟體採取以下操作：

1. 在交換機上建立CFS會話。
2. 在CFS區域中的所有交換機上鎖定使用者角色配置，同時為使用者角色功能啟用CFS。
3. 將使用者角色配置更改儲存到交換機的臨時緩衝區中。

這些更改將保留在交換機上的臨時緩衝區中，直到您明確將其提交給CFS區域中的裝置。

提交更改時，NX-OS軟體將執行以下操作：

1. 將更改應用於交換機上的運行配置。
2. 將更新的使用者角色配置分發到CFS區域中的其他交換機。
3. 在CFS區域中的裝置中解鎖使用者角色配置。
4. 終止CFS會話。

這些配置是分散式的：

- 角色名稱和說明
- 角色規則清單

配置和Show命令

	指令	目的
步驟1.	**configure terminal** 範例： switch# **configure terminal** switch(config)#	進入全域性配置模式。
步驟2.	**角色名稱** *role-name* 範例： switch(config)#角色**名稱** **UserA**	指定使用者角色並進入角色配置模式。
步驟3.	switch(config-role)# **vlan policy deny** 範例： switch(config-role)#vlan **policy deny**	進入角色vlan策略配置模式。
步驟4.	switch(config-role-vlan)# **permit vlan** vlan-*id* 範例： switch(config-role-vlan)# **permit vlan 1**	指定角色可以訪問的VLAN。 根據需要對多個VLAN重複此命令。
步驟5.	switch(config-role-vlan)# **exit** 範例： switch(config-role-vlan)# **exit** switch(config-role)#	退出角色vlan策略配置模式。
步驟6.	**顯示角色** 範例： switch(config-role)# **show role**	（可選）顯示角色配置。
步驟7.	**show role** {**pending** | **pending-diff**} 範例： switch(config-role)#show role **pending**	（可選）顯示待分發的使用者角色配置
步驟8.	**角色提交** 範例： switch(config-role)#role **commit**	（可選）如果您已為使用者角色功能啟用CFS配置分發，則將臨時資料庫
步驟9.	**copy running-config startup-config** 範例： switch# **copy running-config startup-config**	（可選）將運行配置複製到啟動配置。

以下步驟啟用角色配置分發：

	指令	目的
步驟1.	switch# **config t**	進入配置模式。

步驟2.	switch(config)# switch(config)# **role distribute** switch(config)#no **role distribute**	啟用角色配置分發。 禁用角色配置分發（預設）。

以下步驟用於提交角色配置更改：

	指令	**目的**
步驟1	Nexus#**config t** Nexus(config)#	進入配置模式。
步驟2	Nexus(config)# role **commit**	提交角色配置更改。

這些步驟放棄角色配置更改：

	指令	**目的**
步驟1	Nexus#**config t** Nexus(config)#	進入配置模式。
步驟2	Nexus(config)# role **abort**	放棄角色配置更改並清除掛起的配置資料庫。

要顯示使用者帳戶和RBAC配置資訊，請執行以下任務之一：

指令	**目的**
顯示角色	顯示使用者角色配置。
顯示角色功能	顯示功能清單。
show role feature-group	顯示功能組配置。

清除使用者角色分發會話

您可以清除正在進行的思科交換矩陣服務分發會話（如果有），並為使用者角色功能解鎖交換矩陣。

注意：發出此命令時，掛起資料庫中的所有更改都將丟失。

	指令	**目的**
步驟1	switch# **clear role session** **範例：** switch# clear role session	清除會話並解鎖結構。
步驟2	**顯示角色會話狀態** **範例：** switch# show role session status	（可選）顯示使用者角色CFS會話狀態。

組態範例

在本例中，我們將建立具有以下訪問許可權的使用者帳戶TAC:

- 清除命令的訪問許可權
- 存取組態指令
- 對debug命令的訪問
- 訪問exec命令
- 訪問show命令

- 僅訪問VLAN 1-10

```
C5548P-1# config t
Enter configuration commands, one per line.  End with CNTL/Z
C5548P-1(config)# role name Cisco
C5548P-1(config-role)# rule 1 permit command clear
C5548P-1(config-role)# rule 2 permit command config
C5548P-1(config-role)# rule 3 permit command debug
C5548P-1(config-role)# rule 4 permit command exec
C5548P-1(config-role)# rule 5 permit command show
C5548P-1(config-role)# vlan policy deny
C5548P-1(config-role-vlan)# permit vlan 1-10
C5548P-1(config-role-vlan)# end

C5548P-1# show role name Cisco

Role: Cisco
  Description: new role
  vsan policy: permit (default)
  Vlan policy: deny
  Permitted vlans: 1-10
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ----------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ----------------------------------------------------------------
  5       permit  command                         show
  4       permit  command                         exec
  3       permit  command                         debug
  2       permit  command                         config
  1       permit  command                         clear


C5548P-1#
C5548P-1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
C5548P-1(config)# username TAC password Cisco123 role Cisco

C5548P-1(config)# show user-account TAC
user:TAC
        this user account has no expiry date
        roles:Cisco
```

許可要求

產品　許可證要求
NX-OS 使用者帳戶和RBAC不需要許可證。

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。