Nexus N5500、5600和N6000角色基础访问控制(RBAC)

目录

简介

本文档介绍如何限制用户使用角色库访问控制(RBAC)访问Nexus 5500、Nexus 5600和Nexus 6000交换机。

RBAC允许您定义已分配用户角色的规则，以限制有权访问交换机管理操作的用户的授权。

您可以创建和管理用户帐户，并分配限制对Nexus 5500、Nexus 5600和Nexus 6000交换机访问的角色。

先决条件

要求

Cisco 建议您了解以下主题：

- Nexus 5500、Nexus 5600、Nexus 6000交换机CLI配置命令
- 思科交换矩阵服务(CFS)。

使用的组件

本文档中的信息基于运行NXOS 5.2(1)N1(9)7.3(1)N1(1)的Nexus 5500、Nexus 5600和Nexus 6000交换机。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

用户要求

以下是需要满足的一些用户要求：

- 只有具有网络管理员角色的用户才能创建角色。
- 只有具有网络管理员角色的用户才能查看show **role的输出**。
- 即使允许用户执行所有show命令，也不允许用户查看**show role**输出，除非为这些用户分配了网络管理员角色。
- 用户帐户必须至少具有一个用户角色。

用户角色

每个角色可以分配给多个用户，每个用户可以是多个角色的一部分。

例如，允许角色A用户发出show命令，允许角色B用户进行配置更改。

如果用户同时被分配到角色A和角色B，则此用户可以发出show命令并更改配置。

Permit access命令优先于deny access命令。

例如，如果您属于拒绝访问配置命令的角色。

但是，如果您也属于有权访问配置命令的角色，则您有权访问配置命令。

有五个默认用户角色：

- network-admin — 完成对整个交换机的读写访问。
- network-operator — 完成对整个交换机的读取访问。
- vdc-admin — 只限VDC的读写访问
- vdc-operator — 仅限VDC的读取访问
- san-admin — 对SAN管理员完成读写访问。

  注意：不能修改/删除默认用户角色。

  注意：show role命令将显示交换机上可用的角色

用户角色规则

规则是角色的基本元素。

规则定义角色允许用户执行的操作。

您可以为以下参数应用规则：

- 命令 — 在正则表达式中定义的命令或命令组。
- 功能 — 适用于NX-OS软件提供的功能的命令。

- 功能组 — 默认或用户定义的功能组。

这些参数会创建分层关系。最基本的控制参数是命令。

下一个控制参数是特征，它表示与特征关联的所有命令。

最后一个控制参数是特征组。该功能组结合了相关功能，使您可以轻松管理规则。

用户指定的规则编号确定应用规则的顺序。

规则按降序应用。

例如，规则1在规则2之前应用，在规则3之前应用，依此类推。

rule命令指定可由特定角色执行的操作。每个规则都包括规则编号、规则类型（允许或拒绝）、

命令类型（例如，配置、show、exec、debug）和可选功能名称（例如，FCOE、HSRP、VTP、接口）。

用户角色分配

基于角色的配置使用思科交换矩阵服务(CFS)基础设施实现高效的数据库管理，并在网络中提供单点配置。

为设备上的功能启用CFS分发时，设备属于CFS区域，该区域包含网络中的其他设备，您也为该功能启用了CFS分发。默认情况下，用户角色功能的CFS分发处于禁用状态。

您必须为要向其分发配置更改的每台设备上的用户角色启用CFS。

在交换机上为用户角色启用CFS分配后，输入的第一个用户角色配置命令会导致交换机NX-OS软件采取以下操作：

1. 在交换机上创建CFS会话。
2. 在为用户角色功能启用CFS的情况下，锁定CFS区域中所有交换机上的用户角色配置。
3. 将用户角色配置更改保存到交换机的临时缓冲区中。

更改将保留在交换机的临时缓冲区中，直到您明确提交将其分发到CFS区域中的设备。

提交更改时，NX-OS软件会执行以下操作：

1. 将更改应用于交换机上的运行配置。
2. 将更新的用户角色配置分发到CFS区域中的其他交换机。
3. 在CFS区域中的设备中解锁用户角色配置。
4. 终止CFS会话。

这些配置是分发的：

- 角色名称和说明
- 角色规则列表

configuration 和 show 命令

	命令	目的
步骤1:	**configure terminal** 示例： switch#configure terminal switch(config)#	进入全局配置模式。
步骤 2	**角色名称** *角色名称* 示例： switch(config)#**角色名UserA** switch(config-role)#	指定用户角色并进入角色配置模式。
第 3 步：	**VLAN策略拒绝** 示例： switch(config-role)#vlan **policy deny** switch(config-role-vlan)#	进入角色vlan策略配置模式。
第 4 步：	**permit vlan** vlan *-id* 示例： switch(config-role-vlan)#permit vlan **1**	指定角色可以访问的VLAN。 根据需要对尽可能多的vlan重复此命令。
第 5 步：	**退出** 示例： switch(config-role-vlan)#exit switch(config-role)#	退出角色vlan策略配置模式。
步骤 6	**show role** 示例： switch(config-role)#**show role**	（可选）显示角色配置。
步骤 7.	**显示角**色{**挂起**|挂**起 — 差异**} 示例： switch(config-role)#show role pending**(show role pending)**	（可选）显示待分发的用户角色配置
步骤 8	**角色提交** 示例： switch(config-role)# **role commit**	（可选）将临时数据库中的用户角色配置更改应用于运行配置，并将
步骤 9	**copy running-config startup-config** 示例： switch#copy running-config startup-config	（可选）将运行配置复制到启动配置。

以下步骤启用角色配置分配：

	命令	目的
步骤1:	switch# config t switch(config)#	进入配置模式。
第二步：	switch(config)# role distribute(switch(config)# **role distribute)** switch(config)#no role distribute **（无角色分配）**	启用角色配置分发。 禁用角色配置分发（默认）。

以下步骤：

	命令	目的
第 1 步	Nexus# **config t**	进入配置模式。

	Nexus(config)#	
步骤 2	Nexus(config)#角**色提交**	提交角色配置更改。

以下步骤放弃角色配置更改：

	命令	**目的**
第 1 步	Nexus# **config t** Nexus(config)#	进入配置模式。
步骤 2	Nexus(config)#角**色中止**	丢弃角色配置更改并清除挂起的配置数据库。

要显示用户帐户和RBAC配置信息，请执行以下任务之一：

命令	**目的**
show role	显示用户角色配置。
show role feature	显示功能列表。
show role feature-group	显示功能组配置。

清除用户角色分配会话

您可以清除持续的思科交换矩阵服务分发会话（如果有）并解锁交换矩阵以获得用户角色功能。

警告：发出此命令时，挂起数据库中的任何更改都将丢失。

	命令	**目的**
第 1 步	switch#清**除角色会话** **示例：** switch# clear role session	清除会话并解锁交换矩阵。
步骤 2	**show role session status** **示例：** switch# show role session status	（可选）显示用户角色CFS会话状态。

配置示例

在本例中，我们将创建具有以下访问权限的用户帐户TAC:

- 访问clear命令
- 访问配置命令
- 访问debug命令
- 访问exec命令
- 访问show命令
- 仅访问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
```

许可要求

产品　许可证要求
NX-OS 用户帐户和RBAC不需要许可证。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。