连结N5500， 5600和N6000角色基础访问控制(RBAC)

目录

简介

本文描述如何限制用户访问连结5500，连结5600，并且连结6000交换机使用角色根据访问控制(RBAC)。

RBAC允许您定义一个已分配用户角色的规则能限制访问交换机管理操作用户的授权。

您能创建和管理用户帐户和分配对连结5500，连结5600和连结的限制访问6000交换机的角色。

先决条件

要求

Cisco 建议您了解以下主题：

- 连结5500，连结5600，连结6000个交换机CLI配置命令
- 思科矩阵服务(CFS)。

使用的组件

本文档中的信息根据连结5500，连结5600和连结运行NXOS 5.2(1)N1(9) 7.3(1)N1(1)的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。

用户需求

这些是需要执行的一些用户需求：

- 有网络Admin角色的只有用户能创建角色。
- 有网络Admin角色的只有用户能查看输出**显示角色**。
- 即使用户允许实行所有显示命令，他们没有允许查看**显示角色**输出，除非这些用户分配网络Admin角色。
- 用户帐户必须有至少一个用户角色。

用户角色

每个角色可以分配到多个用户，并且每个用户可以是多个角色的一部分。

例如，角色A用户允许发出显示命令，并且角色B用户允许做配置更改。

如果用户分配到角色A和角色B，此用户能发出show命令和做对配置的变动。

Permit访问命令采取优先级拒绝访问命令。

例如，如果属于拒绝对配置命令的访问的角色。

然而，如果也属于访问配置命令的角色，您然后有对配置命令的访问。

有五个默认用户角色：

- 网络Admin -对整个交换机的完整读写访问。
- 网络操作员-对整个交换机的完整读访问。
- VDC Admin -对VDC被限制的读写访问
- VDC操作员-对VDC被限制的读访问
- SAN Admin -对SAN管理员的完整读写访问。

  Note:您不能修改/删除默认用户角色。

  Note:**显示角色**命令将显示角色在交换机的联机

用户角色规则

规则是角色的基本元素。

规则定义了什么操作角色允许用户执行。

您能申请规则这些参数：

- command-a请发出命令或在常规表示定义的命令的组。
- 以适用于NX-OS软件提供的功能的命令为特色。
- 以组默认或功能的用户定义的组为特色。

这些参数创建等级关系。多数基本控制控制参数是命令。

下个控制参数是功能，代表与功能的所有associated命令。

最后控制参数是功能组。功能组结合相关功能并且允许您容易地管理规则。

用户指定的规则编号确定规则应用的命令。

规则按顺序降序应用。

例如，规则1在规则2前应用，在规则3前应用，等等。

rule命令指定可以由一个特定角色执行的操作。每个规则包括规则编号，规则类型(permit或拒绝)，

type命令(例如，配置，显示， exec，调试)和可选功能名称(例如， FCOE， HSRP， VTP，接口)。

用户角色分配

基于任务的配置使用思科矩阵服务(CFS)基础设施启用高效数据库管理和提供单点在网络的配置。

当您启用一个功能的CFS分配在您的设备时，设备属于包含在您为功能的CFS分配也启用的网络的CFS区域其它设备。用户角色的默认情况下CFS分配功能禁用。

您必须启用用户角色的CFS在您要分配配置更改的每个设备。

在您启用用户角色的CFS分配在交换机后，第一个用户角色配置命令您输入原因交换机NX-OS软件采取这些行动：

1. 创建交换机的一CFS会话。
2. 在有为用户角色启用的CFS的CFS区域锁定用户角色在所有交换机的配置功能。
3. 保存用户角色配置更改在交换机的一临时缓冲区。

更改在交换机的临时缓冲区坚持，直到您在CFS区域明确地做将被分配的他们对设备。

当您确认更改时， NX-OS软件采取这些行动：

1. 应用对运行的配置的更改在交换机。
2. 分配更新用户角色配置到其他交换机在CFS区域。
3. 在CFS区域取消锁定用户角色配置在设备。
4. 终止CFS会话。

分配这些配置：

- 角色名称和说明
- 规则列表角色的

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。
第二步：	**角色命名角色***NAME* **示例：** switch(config)-**角色名称UserA** 交换机(设置角色) #	指定用户角色并且输入角色配置模式。
第三步：	**VLAN策略拒绝** **示例：** 交换机(设置角色) #**VLAN策略拒绝** 交换机(设置角色VLAN) #	输入角色VLAN策略配置模式。
第四步：	vlan-id **permit vlan** **示例：** 交换机(设置角色VLAN) **# permit vlan 1**	指定角色能访问的VLAN。 重复许多个VLAN的此命令当必要时。
第五步：	**退出** **示例：** 交换机(设置角色VLAN) **#退出** 交换机(设置角色) #	退出角色VLAN策略配置模式。
第六步：	**显示角色** **示例：** 交换机(设置角色) #**显示角色**	(可选)显示角色配置。
步骤 7.	**显示角色{待定 | 待定 diff}** **示例：** 交换机(设置角色) # **show role pending**	(可选)显示用户角色配置待定为分配
步骤 8	**角色进行** **示例：** 交换机(设置角色) #**角色进行**	(可选)应用用户角色配置更改在临时数据库对运行的配置并且分配用户角
步骤 9	**copy running-config startup-config** **示例：** switch- **copy running-config startup-config**	(可选)复制运行的配置对启动配置。

这些步骤启用角色配置分配：

	命令	目的
步骤1:	switch- **config t** switch(config)-	输入配置模式。
第二步：	switch(config)- **role distribute** switch(config)#no **role distribute**	启用角色配置分配。 功能失效角色配置分配(默认)。

这些步骤进行角色配置更改：

	命令	目的
步骤 1	Nexus# **config t** Nexus(config)#	输入配置模式。
步骤 2	Nexus(config)#**角色进行**	做角色配置更改。

这些步骤丢弃角色配置更改：

	命令	目的
步骤 1	Nexus# **config t** Nexus(config)#	输入配置模式。
步骤 2	Nexus(config)#**角色中止**	丢弃角色配置更改并且清除待定配置数据库。

要显示用户帐户和RBAC配置信息，请执行这些任务之一：

命令	目的
显示角色	显示用户角色配置。
显示角色功能	显示功能列表。
显示角色功能组	显示功能组配置。

清除用户角色分配会话

您能清除持续的思科矩阵服务分配会话(若有)和取消锁定用户角色的结构功能。

> **Caution**:当您发出此命令，在待定数据库上的所有变化将丢失。

	命令	目的
步骤 1	switch-**清除角色会话** **示例：** switch-清除角色会话	清除会话并且取消锁定结构。
步骤 2	**显示角色会话状态** **示例：** switch-显示角色会话状态	(可选)显示用户角色CFS会话状态。

配置示例

在本例中，我们创建与这些的用户帐户TAC访问权限：

- 对clear命令的访问
- 对配置命令的访问
- 对debug命令的访问
- 对exec命令的访问
- show命令的访问
- 仅访问对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
```

许可权要求

产品　许可证需求
NX-OS 用户帐户和RBAC不要求许可证。

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。