在Nexus上使用RADIUS的ACS有限用户访问配置示例

目录

简介

本文档介绍如何为Nexus用户提供受限访问，以便他们只能使用思科安全访问控制服务器(ACS)作为RADIUS服务器输入受限命令。例如，您可能希望用户能够登录到特权或配置模式，并且只能输入接口命令。为此，必须在所使用的RADIUS服务器上为用户创建自定义角色。

先决条件

要求

RADIUS服务器（本例中的ACS）和Nexus必须能够相互联系并执行身份验证。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ACS版本5.x
- Nexus 7000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。

配置

在Nexus上配置自定义角色

要创建只为interface命令提供读/写访问权限的角色，请输入：

```
switch(config)# role name Limited-Access
switch(config-role)# rule 1 permit read-write feature interface
```

其他允许访问规则使用以下语法定义：

```
switch(config-role)# rule 1 permit read-write feature snmp
switch(config-role)# rule 2 permit read-write feature snmp
TargetParamsEntry
switch(config-role)# rule 3 permit read-write feature snmp
TargetAddrEntry
```

配置Nexus进行身份验证和授权

1. 要在具有完全回退权限的交换机上创建本地用户，请输入**username**命令：

   ```
   Switch(config)#username admin privilege 15 password 0 cisco123!
   ```

2. 要提供RADIUS服务器(ACS)的IP地址，请输入：

   ```
   switch# conf terminal
   switch(config)# Radius-server host 10.10.1.1 key cisco123
   authenticationaccounting
   switch(config)# aaa group server radius RadServer
   switch(config-radius)#server 10.10.1.1
   switch(config-radius)# use-vrf Management
   ```

   注：密钥必须与此Nexus设备的RADIUS服务器上配置的共享密钥匹配。

3. 要测试RADIUS服务器可用性，请输入**test aaa**命令：

   ```
   switch# test aaa server Radius 10.10.1.1 user1 Ur2Gd2BH
   ```

   测试身份验证应会失败，并且服务器会拒绝，因为它尚未配置。但是，它确认服务器可访问。

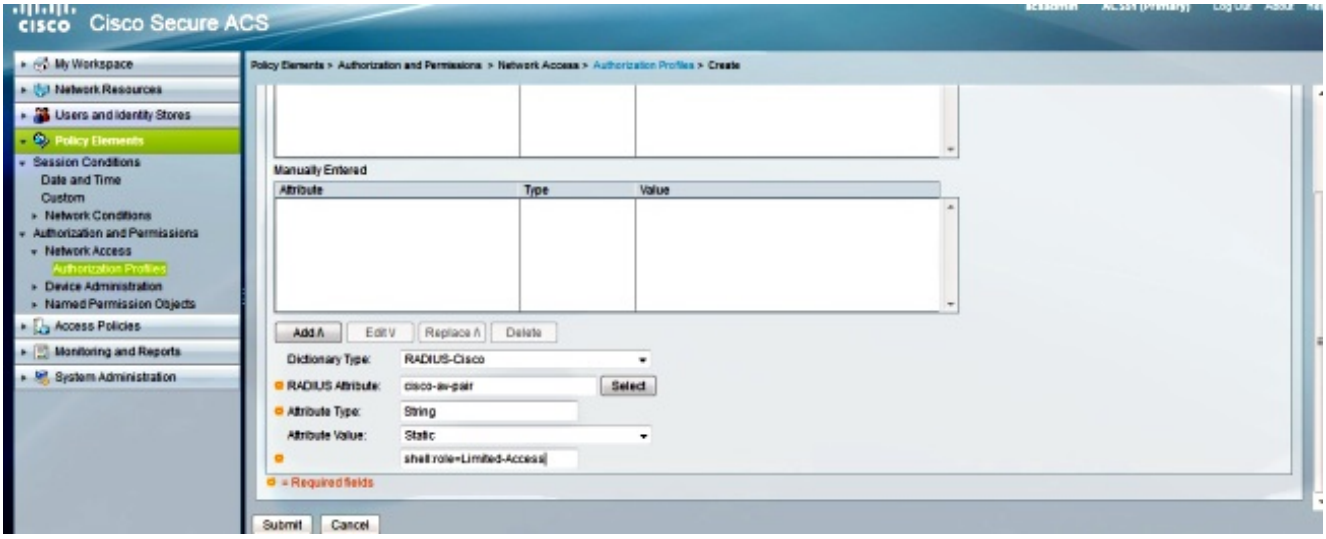
4. 要配置登录身份验证，请输入：

   ```
   Switch(config)#aaa authentication login default group Radserver
   Switch(config)#aaa accounting default group Radserver
   Switch(config)#aaa authentication login error-enable
   ```

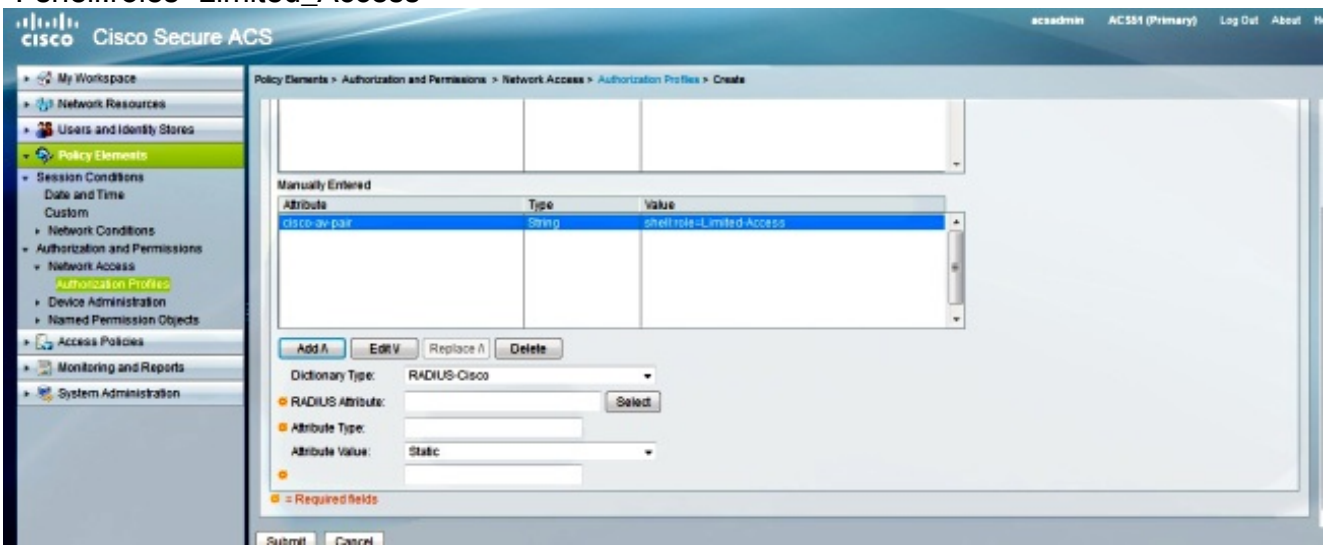
   您无需担心本地回退方法，因为如果RADIUS服务器不可用，Nexus会自行回退到本地。

ACS配置

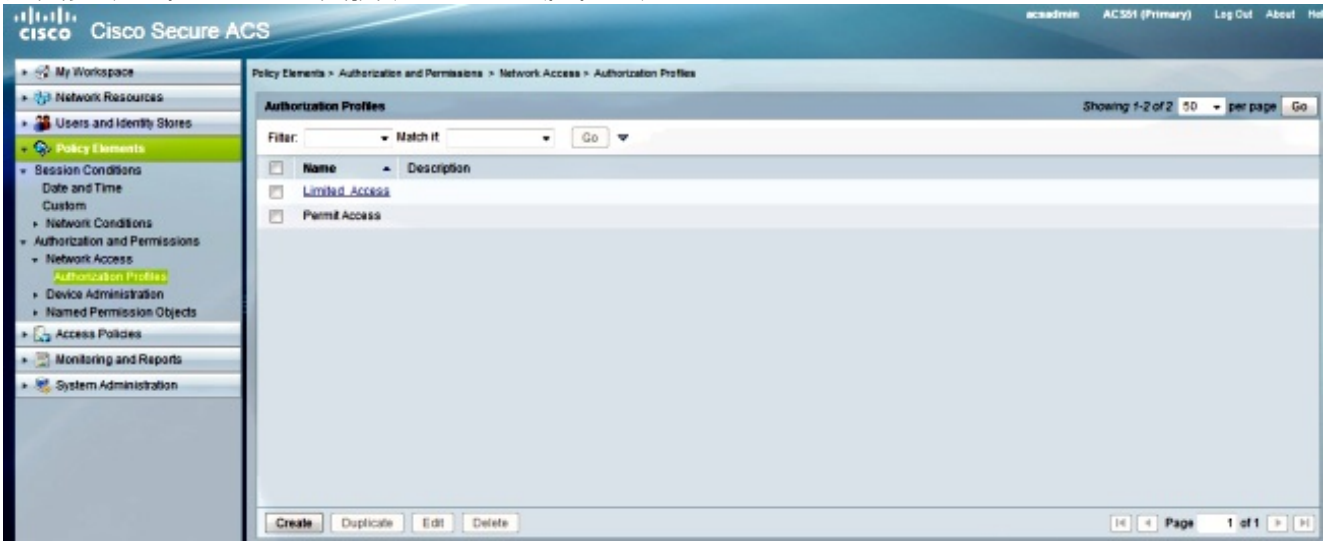
1. 导航到**Policy Elements > Authentication and Permissions > Network Access > Authorization Profile**以创建授权配置文件。



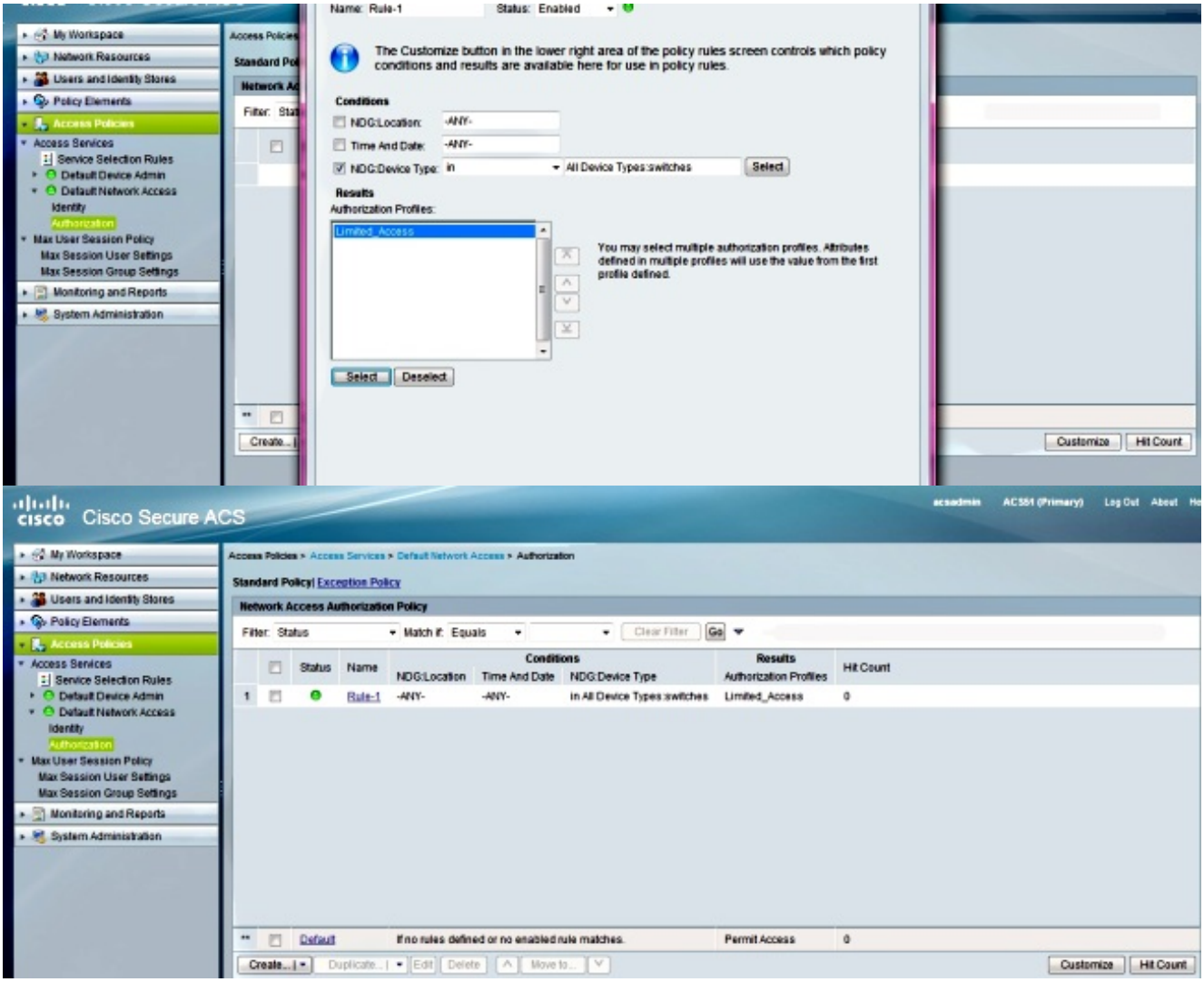
2. 输入配置文件的名称。
3. 在**Custom Attributes**选项卡下，输入以下值：
   词典类型：Radius-Cisco属性：cisco-av-pair要求：必填值
   ：shell:roles=Limited_Access



4. 提交更改以便为Nexus交换机创建基于属性的角色。



5. 创建新的授权规则或在正确的访问策略中编辑当前规则。默认情况下，RADIUS请求由网络访问策略处理。
6. 在**Conditions**区域中，选择适当的条件。在**Results**区域中，选择**Limited_Access**配置文件。



7. Click **OK**.

验证

使用本部分可确认配置能否正常运行。

Nexus角色验证

在Nexus上输入**show role**命令以显示定义的角色和配置的访问规则。

```
switch# show role  (Displays all the roles and includes
custom roles that you have created and their permissions.)

Role: network-admin

Description: Predefined network admin role has access to all
commands on the switch.
------------------------------------------------------------------
Rule Perm Type Scope Entity
------------------------------------------------------------------
1 permit read-write

Role:Limited_Access
Description: Predefined Limited_Access role has access to these commands.
```

```
-------------------------------------------------------------------
Rule Perm Type Scope Entity
-------------------------------------------------------------------
1 permit read-write feature Interface
```

Nexus用户角色分配验证

使用在ACS上配置的用户名和密码登录Nexus。登录后，输入**show user-account**命令以验证测试用户是否具有Limited_Access角色：

```
switch# show user-account
user:admin
this user account has no expiry date
roles:network-admin

user:Test
this user account has no expiry date
roles:Limited_Access
```

确认用户访问角色后，切换到配置模式并尝试输入接口命令以外的命令。应拒绝用户访问。

命令输出解释程序工具（仅限注册用户）支持某些 **show 命令。**使用输出解释器工具来查看 show 命令输出的分析。

- **show role** — 显示角色定义和配置的访问规则。
- **show user-account** — 显示用户帐户详细信息并包括角色分配。

故障排除

本节提供可用于对交换机配置进行故障排除的信息。

在交换机上完成以下角色分配步骤：

1. 使用**show running-config aaa**和**show aaa authentication**命令验证哪个AAA组用于身份验证。
2. 对于RADIUS，使用**show aaa authentication**和**show running-config radius**命令验证虚拟路由和转发(VRF)与AAA组的关联。
3. 如果这些命令验证关联正确，请输入**debug radius all**命令以启用跟踪日志记录。
4. 验证从ACS推送了正确的属性。

命令输出解释程序工具（仅限注册用户）支持某些 **show 命令。**使用输出解释器工具来查看 show 命令输出的分析。

> **注意**：使用debug命令之前，请参阅有关Debug命令**的重要**信息。

- **show running-config aaa**-
- **show aaa authentication**-
- **show running-config radius**
- **debug radius all**

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。