ACS限制了与RADIUS的用户访问在连结配置示例

目录

简介

本文描述如何提供限制访问对于连结用户，以便他们能只输入有限的命令用思科安全访问控制服务器(ACS)作为RADIUS服务器。例如，您也许希望用户能登陆到特许或配置模式和只允许输入接口命令。为了达到此，您必须创建用户的一个自定义角色使用的RADIUS服务器的。

先决条件

要求

RADIUS服务器(在本例中的ACS)和连结一定能与联系和进行认证。

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
- 连结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

自定义角色的配置在连结的

为了创建为interface命令只提供读/写访问的角色，回车：

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

另外的permit访问规则定义与此语法：

```
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
```

配置认证和授权的连结

1. 为了创建交换机的一个本地用户有fallback的全双工权限，请输入**username命令**：
   `Switch(config)#username admin privilege 15 password 0 cisco123!`
2. 为了提供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
   ```
   注意：密钥必须匹配在此连结设备的RADIUS服务器配置的共享塞克雷。
3. 为了测试RADIUS服务器可用性，请参与**aaa命令的测验**：
   `switch# test aaa server Radius 10.10.1.1 user1 Ur2Gd2BH`因为没有配置，测验验证应该失效与从服务器的拒绝。然而，它确认服务器可及的。
4. 为了配置登录认证，回车：
   ```
   Switch(config)#aaa authentication login default group Radserver
   Switch(config)#aaa accounting default group Radserver
   Switch(config)#aaa authentication login error-enable
   ```
   如果RADIUS服务器不可用，您不必须担心本地fallback方法此处，因为连结退路到本地独自地。

ACS的配置

1. 导航对**策略元素>验证和权限>网络访问>授权配置文件**为了创建授权配置文件。
2. 输入一名称对于配置文件。
3. 在**自定义属性下请**选中，输入这些值：
   词典类型：RADIUS思科属性：cisco-av-pair需求：必须值：shell ：roles=Limited_Access
4. 提交更改为了创建连结交换机的一个基于属性的角色。
5. 创建一个新的授权规则或编辑在正确访问策略的一个当前规则。默认情况下RADIUS请求由网络访问策略处理。
6. 在**情况**地区中，请选择适当的条件。在成果区域中，请选择**Limited_Access配置文件**。
7. 单击 **Ok**。

验证

使用本部分可确认配置能否正常运行。

连结角色验证

输入**显示角色**on命令连结为了显示定义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
```

连结用户角色分配验证

登陆对与在ACS配置的用户名和密码的连结。在登录以后，请输入**show user-account**命令为了验证测试用户有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
```

一旦用户访问角色被确认，除interface命令之外，请交换到配置模式并且尝试输入命令。用户应该是拒绝访问。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

- **显示角色**-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且包括角色分配。

故障排除

此部分提供您能使用为了排除故障您的交换机配置的信息。

完成在交换机的这些步骤角色的分配：

1. 验证AAA组使用验证用**show running-config aaa**和**show aaa authentication**命令。
2. 对于RADIUS，请验证有AAA组的虚拟路由和转发(VRF)关联用**show aaa authentication**和**show running-config radius**命令。
3. 如果这些verify命令关联正确，输入**all命令的debug radius**为了启用跟踪记录。
4. 验证正确属性从ACS推送。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

> **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-**
- **显示AAA认证**
- **show running-config radius**
- **debug radius全部**