Nexus 4005I中的TACACS+配置示例

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[配置](#)
[逐步指导](#)
[TACACS+ CLI配置](#)
[验证](#)
[故障排除](#)
[相关信息](#)

简介

本文档介绍如何在Nexus 4000系列交换机中配置终端访问控制器访问控制系统(TACACS+)。Nexus 4000系列的TACACS+身份验证与Cisco Catalyst交换机相比略有不同。

先决条件

要求

Cisco 建议您了解以下主题：Cisco Nexus 7000系列NX-OS基础命令。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科Nexus 4005I交换机
- 思科安全访问控制服务器(ACS)5.x

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。

规则

关于文件规则的信息，请参见Cisco技术提示规则。

配置

本节中的配置示例介绍如何配置Nexus 4005I交换机和TACACS+服务器。

逐步指导

要配置Nexus交换机和TACACS+服务器，请完成以下步骤：

1. 启用TACACS+协议功能。必须使用预共享密钥配置ACS服务器的IP地址。如果有多个ACS服务器，则必须配置两台主机。
2. 启用AAA概念和AAA服务器组。在此配置示例中，AAA组名称为“ACS”。

TACACS+ CLI配置

ASA
!--- Enable TACACS+ on the device. feature tacacs+ tacacs-server host 10.0.0.1 key 7 Cisco tacacs-server host 10.0.0.2 key 7 Cisco tacacs-server directed-request *!--- Provide the name of your ACS server.* aaa group server tacacs+ **ACS** *!--- Mention the IP address of the tacacs-servers !--- referred to in the "tacacs-server host" command.* server 10.0.0.1 server 10.0.0.2 *!--- Telnet and ssh sessions.* aaa authentication login default group ACS local *!--- Console sessions.* aaa authentication login console group ACS local *!--- Accounting command.* aaa accounting default group ACS

注意：在ACS服务器中使用相同的预共享密钥“Cisco”进行Nexus 4000系列和ACS服务器之间的身份验证。

注意：如果TACACS+服务器关闭，则可以通过在交换机中配置用户名和密码来回退以进行本地身份验证。

Nexus操作系统不使用权限级别的*概念*，而是使用*角色*。默认情况下，您将被置于*网络操作员*角色。如果希望用户具有完全权限，则必须将其置于*network-admin*角色中，并且必须配置TACACS服务器以在用户登录时下推属性。对于TACACS+，您会返回TACACS自定义属性，其值 `roles="roleA"`。 对于完全访问用户，您使用：`cisco-av-pair*shell:roles="network-admin"`

`cisco-av-pair*shell:roles="network-admin"(The * makes it optional)`

`shell:roles="network-admin"`

验证

使用本节中的命令验证TACACS+服务器配置：

- **show tacacs-server** — 显示TACACS+服务器配置。
- **show aaa authentication [login {error-enable | mschap}]** — 显示已配置的身份验证信息。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 配置AAA
- 配置 TACACS+
- 技术支持和文档 - Cisco Systems