配置TACACS+、在Cisco Catalyst交换机的RADIUS和Kerberos

目录

简介

从 2.2 代码开始，Cisco Catalyst 系列交换机（运行 CatOS 的 Catalyst 4000、Catalyst 5000 和 Catalyst 6000）支持一些形式的身份验证（从 2.2 代码开始）。更高版本已增加了增强功能。用户设置的 TACACS+ TCP 端口 49（不是 XTACACS 用户数据协议端口 49），RADIUS 或者 Kerberos 服务器用于验证、授权和记帐 (AAA)，与路由器用户的设置相同。本文档介绍启用这些功能所必需的最低要求的命令。在所讨论版本的交换机文档中可以找到其他选项。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

因为更高版本的代码支持更多选项，您需要发出 **show version** 命令来确定交换机上的代码版本。一旦您确定在交换机上使用的代码版本，请使用下表来确定哪些选项可以在您的设备上使用，哪些选项是您希望配置的。

当您添加身份验证和授权时，请一直保留在交换机中。在另一个窗口中测试配置，以避免意外锁定。

方法（最低要求）	**Cat 版本 2.2 到 5.1**	**Cat 版本 5.1 到 5.4.1**	**Cat 版本 5.4.1 到 7.5.1**	**Cat 版本 7.5.1 及更高版本**
TACACS+ 身份验证 OR	步骤 A	步骤 A	步骤 A	步骤 A
RADIUS 身份验证 OR	不适用	步骤 B	步骤 B	步骤 B
Kerberos 身份验证 OR	不适用	不适用	步骤 K	步骤 K
本地用户名身份验证/授权	不适用	不适用	不适用	步骤 C
Plus（选项）				
TACACS+ 命令授权	不适用	不适用	步骤 D	步骤 D
TACACS+ Exec 授权	不适用	不适用	步骤 E	步骤 E
RADIUS Exec 授权	不适用	不适用	步骤 F	步骤 F
记帐 - TACACS+ 或 RADIUS	不适用	不适用	步骤 G	步骤 G
TACACS+ 启用授权	步骤 H	步骤 H	步骤 H	步骤 H
RADIUS 启用授权	不适用	步骤 I	步骤 I	步骤 I
TACACS+ 启用授权	不适用	不适用	步骤 J	步骤 J

配置步骤

步骤 A - TACACS+认证

使用更早的代码版本，其中的命令不如某些更高版本的命令复杂。您的交换机上可能提供了更高版本中的其他选项。

1. 如果服务器发生故障，请发出 **set authentication login local enable** 命令，以确保交换机中有后门。
2. 发出 **set authentication login tacacs enable** 命令，以启用 TACACS+ 身份验证。
3. 发出 **set tacacs server #.#.#.#** 命令来定义服务器。
4. 发出 **set tacacs key your_key** 命令来定义服务器密钥，这在使用 TACACS+ 时是可选的，因为它会造成从交换机到服务器的数据被加密。如果采用，它必须与服务器一致。**注意：** Cisco Catalyst OS 软件**不**接受问号 (**?**) 作为任何密钥或口令的一部分。问号在命令语法中明确表示需要帮助。

步骤 B - RADIUS 验证

使用更早的代码版本，其中的命令不如某些更高版本的命令复杂。您的交换机上可能提供了更高版本中的其他选项。

1. 如果服务器发生故障，请发出 **set authentication login local enable** 命令，以确保交换机中有后门。
2. 发出 **set authentication login radius enable** 命令来启用 RADIUS 身份验证。
3. 定义服务器。在其他所有 Cisco 设备上，默认的 RADIUS 端口为 1645/1646（身份验证/记帐）。Catalyst 上的默认端口为 1812/1813。如果您使用 Cisco Secure 或与其他 Cisco 设备通信的服务器，请使用 1645/1646 端口。发出 **set radius server #.#.#.# auth-port 1645 acct-port 1646 primary** 命令，以便在 Cisco IOS 中定义服务器，以及与 **radius-server source-ports 1645-1646** 等效的命令。
4. 定义服务器密钥。这是必须的，因为它会造成交换机到服务器的口令按照 RADIUS 身份验证/授权 RFC 2865 和 RADIUS 记帐 RFC 2866 所述被加密。 如果采用，它必须与服务器一致。发出 **set radius key your_key** 命令。

步骤 C - 本地用户名认证/授权

从 CatOS 版本 7.5.1 开始，支持本地用户身份验证。例如，您可以使用存储在 Catalyst 上的用户名和口令来完成身份验证/授权，而不是通过本地口令来进行身份验证。

只有两个针对本地用户身份验证的权限级别：0 或 15。级别 0 是无特权的 exec 级别。级别 15 是有特权的启用级别。

如果在本示例中添加以下命令，则用户 poweruser 可以在 Telnet 或交换机的控制台上实现启用模式，用户 nonenable 可以在 Telnet 或交换机的控制台上实现 exec 模式。

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

注意： 如果用户 nonenable 知道 **set enable password**，则该用户能够继续保持启用模式。

在配置之后，口令将被加密存储。

本地用户名认证可以与远程TACACS+ exec、命令记帐或远程RADIUS exec记帐一起使用。它还可

以与远程 TACACS+ exec 或命令授权一起使用，但这种使用方式毫无意义，因为用户名需要同时存储在 TACACS+ 服务器和本地交换机上。

步骤 D - TACACS+ 命令授权

在本示例中，交换机被告知要求通过 TACACS+ 仅对配置命令进行授权。在 TACACS+ 服务器发生故障的情况下，身份验证为无。这适用于控制台端口和 Telnet 会话。发出以下命令：

set authorization 命令 enable config tacacs none both

在本示例中，当您设置这些参数时，可以将 TACACS+ 服务器配置为允许：

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

set port enable 2/12 命令被发送到 TACACS+ 服务器以便验证。

注意： 在启用命令授权后，与不把 enable 视为命令的路由器不同的是，交换机在尝试启用时会向服务器发送 **enable** 命令。请确保服务器同样配置为允许 **enable** 命令。

步骤 E - TACACS+ Exec 授权

在本示例中，交换机被告知要求使用 TACACS+ 对 exec 会话进行授权。在 TACACS+ 服务器发生故障的情况下，授权为无。这适用于控制台端口和 Telnet 会话。发出 **set authorization exec enable tacacs+ none both** 命令

除认证请求外，它还从交换机上向TACACS+服务器发送单独的授权请求。如果为TACACS+服务器上的shell/exec配置了用户配置文件，则该用户可以访问交换机。

这可以防止未在服务器上配置 shell/exec 服务的用户（例如 PPP 用户）登录交换机。您收到 Exec mode authorization failed 消息。用户除了允许/拒绝 exec 模式以外，您还可以在进入服务器上分配的权限级别 15 时强制进入启用模式。它必须执行已修复 Cisco Bug ID CSCdr51314（仅限注册用户）的 runcode。

步骤 F - RADIUS Exec 授权

没有可以启用 RADIUS exec 授权的命令。另一种选择是在 RADIUS 服务器中将服务类型（RADIUS 属性 6）设置为管理（值为 6），以便将 RADIUS 服务器的用户以启用模式启动。如果服务设置为除“6-管理”以外的其他类型（例如“1-登录”、“7-shell”或“2-成帧”），用户会看到交换机 exec 提示符，而不是 enable 提示符。

将这些命令添加到交换机中，以便进行身份验证和授权：

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

步骤 G – 记帐 - TACACS+ 或 RADIUS

为了启用 TACACS+ 记帐：

1. 如果得到交换机提示符，请发出 **set accounting exec enable start-stop tacacs+** 命令。

2. Telnet 到交换机外的用户，发出 **set accounting connect enable start-stop tacacs+** 命令。
3. 如果重新启动交换机，请发出 **set accounting system enable start-stop tacacs+** 命令。
4. 执行命令的用户，发出 **set accounting commands enable all start-stop tacacs+** 命令。
5. 对服务器发出的提醒，例如，要每分钟更新一次记录，以显示用户仍处于登录状态，可发出 **set accounting update periodic 1** 命令。

为了启用 RADIUS 记帐：

1. 得到交换机提示符的用户，发出 **set accounting exec enable start-stop radius** 命令。
2. Telnet 到交换机外的用户，发出 **set accounting connect enable start-stop radius** 命令。
3. 如果重新启动交换机，请发出 **set accounting system enable start-stop radius** 命令。
4. 对服务器发出的提醒，例如，要每分钟更新一次记录，以显示用户仍处于登录状态，可发出 **set accounting update periodic 1** 命令。

TACACS+ 免费软件记录

此输出是关于记录如何在服务器上显示的示例：

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

UNIX 记录输出上的 RADIUS

此输出是关于记录如何在服务器上显示的示例：

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

步骤 H - TACACS+ 启用认证

完成这些步骤：

1. 发出 **set authentication enable local enable** 命令，以便确保在服务器发生故障时有后门。
2. 发出 **set authentication enable tacacs enable** 命令，以便通知交换机向服务器发送启用请求。

步骤 I - RADIUS 启用认证

添加这些命令是为了让交换机将用户名 $enab15$ 发送到 RADIUS 服务器。不是所有的 RADIUS 服务器都支持这种用户名。请参阅步骤 E，了解另一替代方案，例如，如果将服务类型设置为 “[RADIUS attribute 6 - to Administrative]”，从而以启用模式启动个人用户。

1. 发出 **set authentication enable local enable** 命令，以便确保在服务器发生故障时有后门。
2. 如果您的 RADIUS 服务器支持 $enab15$ 用户名，请发出 **set authentication enable radius enable** 命令，以便通知交换机向服务器发送启用请求。

步骤 J - TACACS+ 启用授权

当用户尝试启用时，此命令的新增内容会导致交换机将启用发送到服务器。服务器需要有 **enable** 命令权限。在本示例中，当服务器发生故障时将故障转移到无：

set author enable enable tacacs+ none both

步骤 K - Kerberos 认证

有关如何对交换机设置 Kerberos 的详细信息，请参阅使用身份验证、授权和记帐来控制并监控对交换机的访问。

密码 恢复

有关口令恢复过程的详细信息，请参阅口令恢复过程。

本页是 Cisco 产品的口令恢复过程的索引。

用于附加安全性的 ip permit 命令

对于附加安全性，可以通过 **ip permit** 命令配置 Catalyst，以控制 Telnet 的访问：

set ip permit enable telnet

set ip permit range mask|*主机*

这只允许指定的范围或主机 Telnet 到交换机。

调试 Catalyst

在 Catalyst 上启用调试之前，请查看服务器日志，以了解失败的原因。这样会更容易，并且可减少对交换机的中断。在早期的交换机版本中，**debug** 是以工程模式执行的。在更高的代码版本中，无需再为了执行 **debug** 命令而进入工程模式：

set trace tacacs|radius|kerberos 4

注意： set trace tacacs|radius|Kerberos 0 命令将 Catalyst 返回到 no-tracing 模式。

有关多层 LAN 交换机的详细信息，请参阅交换机产品支持页。

相关信息

- TACACS+ 和 RADIUS 的比较
- Cisco IOS 文档中的 RADIUS、TACACS+ 和 Kerberos
- RADIUS 支持页
- TACACS/TACACS+支持页面
- Kerberos 支持页
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems