

如何配置Cisco VPN 3000集中器以支持管理帐户的TACACS+认证

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置TACACS+服务器](#)

[在TACACS+服务器中为VPN 3000集中器添加条目](#)

[在TACACS+服务器中添加用户帐户](#)

[编辑TACACS+服务器上的组](#)

[配置VPN 3000集中器](#)

[在VPN 3000集中器中为TACACS+服务器添加条目](#)

[修改VPN集中器上的管理员帐户以进行TACACS+身份验证](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档提供分步说明，以配置Cisco VPN 3000系列集中器，以支持管理帐户的TACACS+身份验证。

一旦在VPN 3000集中器上配置了TACACS+服务器，就不再使用本地配置的帐户名和密码，如admin、config、isp等。所有登录到VPN 3000集中器的登录都将发送到已配置的外部TACACS+服务器，以供用户和密码验证。

TACACS+服务器上每个用户的权限级别定义确定每个TACACS+用户名在VPN 3000集中器上的权限。然后，将其与VPN 3000集中器上本地配置的用户名下定义的AAA访问级别进行匹配。这是一个重要点，因为一旦定义了TACACS+服务器，VPN 3000集中器上本地配置的用户名就不再有效。但是，它们仍用于匹配从TACACS+服务器返回的权限级别，以及该本地用户下的AAA访问级别。然后，TACACS+用户名将分配给本地配置的VPN 3000集中器用户在其配置文件下定义的权限。

例如，配置部分中详细介绍了，TACACS+用户/组配置为返回TACACS+权限级别15。在VPN 3000集中器的Administrators部分下，管理员用户的AAA访问级别也设置为15。允许此用户修改所有部分下的配置，以及读取/写入文件。由于TACACS+权限级别和AAA访问级别匹配，因此TACACS+用户在VPN 3000集中器上获得了这些权限。

例如，如果您决定用户需要能够修改配置，但不能读/写文件，请在TACACS+服务器上为其分配12的权限级别。您可以选择介于1和15之间的任意数字。然后，在VPN 3000集中器上，选择其他本

地配置的管理员之一。接下来，将其AAA访问级别设置为12，并设置此用户的权限，以便能够修改配置，但不能读取/写入文件。由于权限/访问级别匹配，用户在登录时会获得这些权限。

不再使用VPN 3000集中器上本地配置的用户名。但是，使用每个用户下的访问权限和AAA访问级别来定义特定TACACS+用户在您登录时获得的权限。

[先决条件](#)

[要求](#)

尝试进行此配置之前，请确保满足以下要求：

- 确保从VPN 3000集中器到TACACS+服务器有IP连接。如果您的TACACS+服务器指向公共接口，请不要忘记在公共过滤器上打开TACACS+ (TCP端口49)。
- 确保通过控制台进行备份访问正常运行。首次设置时，很容易意外将所有用户锁定在配置之外。恢复访问的唯一方法是通过控制台，该控制台仍使用本地配置的用户名和密码。

[使用的组件](#)

本文档中的信息基于以下软件和硬件版本：

- Cisco VPN 3000集中器软件版本4.7.2.B (或者，3.0或更高版本的操作系统软件都可以运行。)
- 适用于Windows Servers版本4.0的思科安全访问控制服务器 (或者，2.4或更高版本的软件都可运行。)

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](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

[配置TACACS+服务器](#)

[在TACACS+服务器中为VPN 3000集中器添加条目](#)

要在TACACS+服务器中为VPN 3000集中器添加条目，请完成以下步骤。

1. 单击左面板中的**Network Configuration**。在 AAA Clients 下，单击 **Add Entry**。
2. 在下一个窗口中，填写表格，将VPN集中器添加为TACACS+客户端。本示例使用：AAA客户端主机名= VPN3000AAA客户端IP地址= 10.1.1.2密钥= csacs123使用= TACACS+(Cisco IOS)进行身份验证单击 **Submit+ Restart**。



Edit



Add AAA Client

AAA Client Hostname	<input type="text" value="VPN3000"/>
AAA Client IP Address	<input type="text" value="10.1.1.2"/>
Key	<input type="text" value="csacs123"/>
Authenticate Using	<input type="text" value="TACACS+ (Cisco IOS)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	

[在TACACS+服务器中添加用户帐户](#)

要在TACACS+服务器中添加用户帐户，请完成以下步骤。

1. 在TACACS+服务器中创建一个用户帐户，该帐户稍后可用于TACACS+身份验证。单击左面板中的“用户设置”，添加用户“johnsmith”，然后单击“添加/编辑”以执行此操作。
2. 为此用户添加密码，并将用户分配给包含其他VPN 3000集中器管理员的ACS组。注：本示例定义此特定用户ACS组配置文件下的权限级别。如果要逐个用户完成此操作，请选择Interface Configuration > TACACS+(Cisco IOS)，然后选中Shell(exec)服务的User框。只有这样，本文中描述的TACACS+选项才可在每个用户配置文件下使用。

[编辑TACACS+服务器上的组](#)

完成以下步骤以编辑TACACS+服务器上的组。

1. 单击左面板中的“组设置”。
2. 从下拉菜单中，在[Add a User Account in the TACACS+ Server](#)部分（本例中为Group 1）中选择用户添加到的组，然后单击Edit Settings。
3. 在下一个窗口中，确保在TACACS+ Settings (TACACS+设置)下选择了以下属性：外壳(exec)权限级别= 15完成后，单击“Submit + Restart(提交+重新启动)”。

配置VPN 3000集中器

在VPN 3000集中器中为TACACS+服务器添加条目

要在VPN 3000集中器中为TACACS+服务器添加条目，请完成以下步骤。

1. 在左侧面板的导航树中选择Administration > Access Rights > AAA Servers > Authentication，然后在右侧面板中单击Add。一旦单击Add以添加此服务器，VPN 3000集中器上本地配置的用户名/口令将不再使用。确保在锁定的情况下，通过控制台进行备份访问可正常工作。
2. 在下一个窗口中，填写如下所示的表格：身份验证服务器= 10.1.1.1 (TACACS+服务器的IP地址) 服务器端口= 0 (默认) 超时= 4重试次数= 2服务器密钥= csacs123验证=

csacs123

The screenshot shows a configuration page titled "Administration | Access Rights | AAA Servers | Authentication | Add". The page contains the following fields and instructions:

- Authentication Server:** 10.1.1.1 (Enter IP address or hostname.)
- Server Port:** 0 (Enter the server TCP port number (0 for default).)
- Timeout:** 4 (Enter the timeout for this server (seconds).)
- Retries:** 2 (Enter the number of retries for this server.)
- Server Secret:** [masked] (Enter the server secret.)
- Verify:** [masked] (Re-enter the server secret.)

Buttons: Add, Cancel

修改VPN集中器上的管理员帐户以进行TACACS+身份验证

完成以下步骤以修改VPN集中器上用于TACACS+身份验证的管理员帐户。

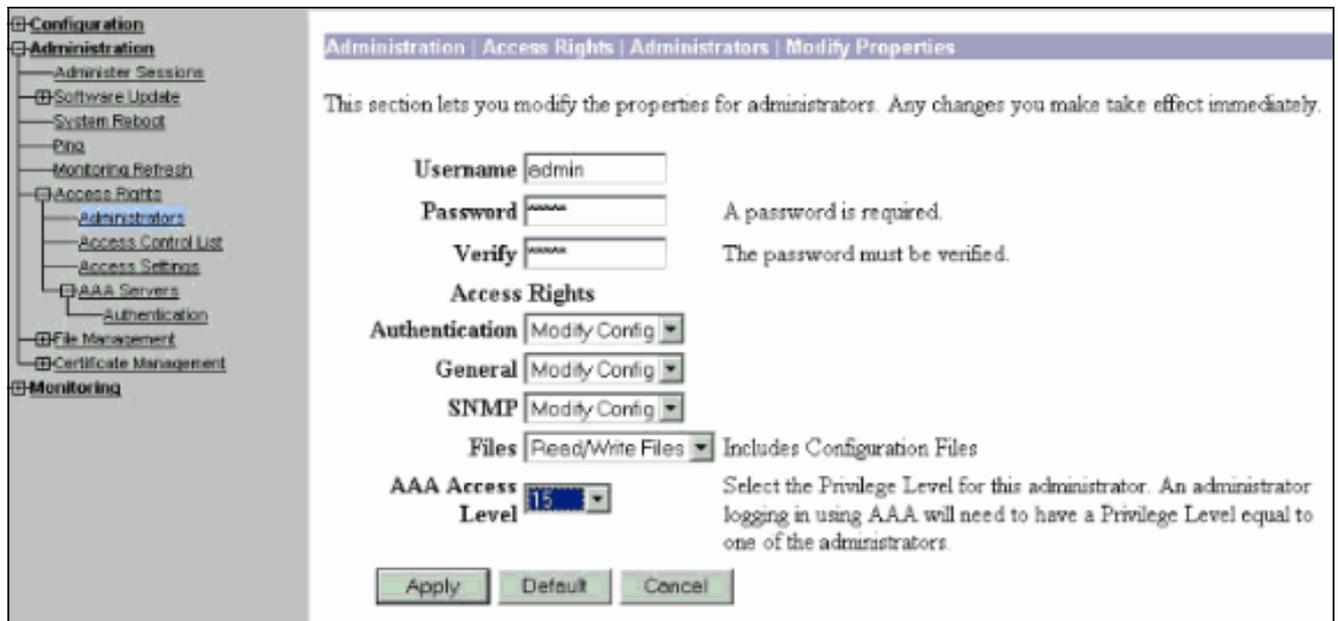
1. 单击**Modify**以修改用户admin的属性。

The screenshot shows a configuration page titled "Administration | Access Rights | Administrators". The page contains the following table:

Group Number	Username	Properties	Administrator Enabled
1	admin	Modify	<input checked="" type="checkbox"/>
2	config	Modify	<input type="checkbox"/>
3	isp	Modify	<input type="checkbox"/>
4	mis	Modify	<input type="checkbox"/>
5	user	Modify	<input type="checkbox"/>

Buttons: Apply, Cancel

2. 选择AAA Access Level (AAA访问级别) 为15。此值可以是介于1和15之间的任意数字。请注意，它必须与TACACS+服务器上用户/组配置文件下定义的TACACS+权限级别匹配。然后，TACACS+用户获取在此VPN 3000集中器用户下定义的权限，以修改配置、读取/写入文件等。



验证

当前没有可用于此配置的验证过程。

故障排除

完成这些说明中的步骤以排除配置故障。

1. 要测试身份验证：对于TACACS+服务器选择Administration > Access Rights > AAA Servers > Authentication。选择您的服务器，然后单击Test。



注意：在“管理”(Administration)选项卡上配置TACACS+服务器时，无法设置用户在VPN 3000本地数据库上进行身份验证。您只能使用其他外部数据库或TACACS服务器回退。输入TACACS+用户名和密码，然后单击OK。

Enter a username and password with which to test. Please wait for the operation to complete or timeout.

Username
 Password

OK

Cancel

系统将显示成功的身份验证。

Configuration

Administration

Administer Sessions

Software Update

System Reboot

Reboot Status

Ping

Traceroute

Monitoring Refresh

Access Rights

Administrators

Access Control List

Access Settings

AAA Servers

Authentication

File Management

Certificate Management

Monitoring

Success



Authentication Successful

Continue

- 如果发生故障，则会出现配置问题或IP连接问题。检查ACS服务器上的Failed Attempts Log（失败尝试日志），查找与故障相关的消息。如果此日志中未显示任何消息，则可能存在IP连接问题。TACACS+请求未到达TACACS+服务器。验证应用于适当VPN 3000集中器接口的过滤器是否允许TACACS+（TCP端口49）数据包进出。如果故障在日志中显示为服务被拒绝，则Shell(exec)服务未在TACACS+服务器的用户或组配置文件下正确启用。
- 如果测试身份验证成功，但VPN 3000集中器的登录仍然失败，请通过控制台端口检查可过滤事件日志。如果您看到类似消息：

```
65 02/09/2005 13:14:40.150 SEV=5 AUTH/32 RPT=2
```

```
User [ johnsmith ] Protocol [ HTTP ] attempted ADMIN logon.
```

```
Status: <REFUSED> authorization failure. NO Admin Rights
```

此消息表明在TACACS+服务器上分配的权限级别在任何VPN 3000集中器用户下都没有匹配的AAA访问级别。例如，用户johnsmith在TACACS+服务器上的TACACS+权限级别为7，但五个VPN 3000集中器管理员中没有一个AAA访问级别为7。

相关信息

- [Cisco VPN 3000 系列集中器支持页](#)
- [Cisco VPN 3000 系列客户端支持页](#)
- [IPsec 协商/IKE 协议支持页](#)

- [TACACS/TACACS+支持页面](#)
- [IOS 文档中的 TACACS+](#)
- [技术支持和文档 - Cisco Systems](#)