用于 AAA 的 TACACS+ 服务器

本章介绍如何配置 AAA 中使用的 TACACS+ 服务器。

关于用于 AAA 的 TACACS+ 服务器

ASA 支持使用以下协议进行 TACACS+ 服务器身份验证：ASCII、PAP、CHAP 和 MS-CHAPv1。

TACACS+ 属性

ASA 可支持 TACACS+ 属性。TACACS+ 属性可分隔身份验证、授权和记帐功能。该协议支持两种类型的属性：强制属性和可选属性。服务器和客户端都必须能够理解强制属性，而且必须将强制属性应用于用户。可选属性是否能被理解，或是否会被使用不作要求。

注释 要使用 TACACS+ 属性，请确保您已在 NAS 上启用 AAA 服务。

下表列出适用于直接转发代理连接的受支持的 TACACS+ 授权响应属性。

表 *1:* 支持的 *TACACS+* 授权响应属性

属性	说明
acl	确定要应用于连接的本地配置的 ACL。
idletime	指示经过身份验证的用户会话终止前可以处于非活动状态的时长（以分钟为单位）。

属性	说明
timeout	指示经过身份验证的用户会话终止前，身份验证凭据可以保持活动状态的时长（以分钟为单位）。

下表列出支持的 TACACS+ 记帐属性。

.

表 *2:* 支持的 *TACACS+* 记帐属性

属性	说明
bytes_in	指定此连接过程中传输的输入字节的数量（仅停止记录）
bytes_out	指定此连接过程中传输的输出字节的数量（仅停止记录）。
cmd	定义执行的命令（仅命令记帐）。
disc-cause	指定标识连接断开原因的数值代码（仅停止记录）。
elapsed_time	定义连接所消耗的秒数（仅停止记录）。
foreign_ip	指定隧道连接的客户端的 IP 地址。定义用于直接转发代理连接的最低安全性接口上的地址。
local_ip	指定对于隧道连接，客户端已连接到的 IP 地址。定义用于直接转发代理连接的最高安全性接口上的地址。
NAS port	包含连接的会话 ID。
packs_in	指定此连接过程中传输的输入数据包的数量。
packs_out	指定此连接过程中传输的输出数据包的数量。
priv-level	设置为命令记帐请求的用户权限级别，否则设置为 1。
rem_iddr	指示客户端的 IP 地址。
service	指定所使用的服务。对于仅进行命令记帐的情况，始终设置为“shell”。
task_id	指定记帐事务的唯一任务 ID。
username	指定用户的名称。

用于 AAA 的 TACACS+ 服务器准则

本节介绍您在配置用于 AAA 的 TACACS+ 服务器之前应检查的准则和限制。

IPv6

AAA 服务器可以使用 IPv4 或 IPv6 地址。

其他准则

- 在单模式下可以有最多 200 个服务器组，在多模式下每个情景可以有 4 个服务器组。
- 在单模式下每个组可以有最多 16 个服务器，在多模式下每个组可以有 8 个服务器。
- 对于在 ASA 设备模式下运行的 FPR1000、FPR2100 或 FPR3100 系列，必须遵守以下用户名约定：
  - 必须是 Linux 有效的用户名。
  - 必须仅使用小写字母。
  - 可以包含字母数字字符、句点 (.) 或连字符 (-)。
  - 必须不包含其他特殊字符，例如 at 符号 (@) 和斜线 (/)。

配置 TACACS+ 服务器

本节介绍如何配置 TACACS+ 服务器。

过程

步骤 1 配置 TACACS+ 服务器组，第 3 页。
步骤 2 向组中添加 TACACS+ 服务器，第 4 页。
步骤 3 （可选）添加身份验证提示，第 5 页。

配置 TACACS+ 服务器组

如果要将 TACACS+ 服务器用于身份验证、授权或记帐，则必须先创建至少一个 TACACS+ 服务器组，然后向每个服务器组添加一台或多台服务器。您可以按名称标识 TACACS+ 服务器组。

要添加 TACACS+ 服务器组，请执行以下步骤：

过程

步骤 1 依次选择 **Configuration** > **Device Management** > **Users/AAA** > **AAA Server Groups**。
步骤 2 在 **AAA Server Groups** 区域中，点击 **Add**。

系统将显示 **Add AAA Server Group** 对话框。

步骤 3 在 **Server Group** 字段中输入组的名称。

步骤 4 从 **Protocol** 下拉列表中选择 **TACACS**+ 服务器类型：

步骤 5 点击 **Accounting Mode** 字段中的 **Simultaneous** 或 **Single**。

在 Single 模式下，ASA 仅向一台服务器发送记账数据。

在 Simultaneous 模式下，ASA 将向组中的所有服务器发送记账数据。

步骤 6 点击 **Reactivation Mode** 字段中的 **Depletion** 或 **Timed**。

在 Depletion 模式下，只有在组中所有服务器都处于非活动状态后，故障服务器才重新激活。在 depletion 模式下，当停用服务器时，它将保持非活动状态，直到组中的所有其他服务器都处于非活动状态。如果发生这种情况，组内所有服务器都会被重新激活。这种方法可最大限度减少因出现故障的服务器而发生的连接延迟。

在 Timed 模式下，故障服务器会在 30 秒停机时间后被重新激活。

步骤 7 如果选择 Depletion 重新激活模式，请在 **Dead Time** 字段中输入时间间隔。

Dead Time 是从禁用组中的最后一个服务器到随后重新启用所有服务器所经过的时间，以分钟为单位。仅当配置回退到本地数据库时，失效时间时间才适用；身份验证将在本地尝试，直到失效时间结束。

步骤 8 添加允许失败的 AAA 事务的最大数量。

此选项设置在宣布无响应服务器为非活动状态之前允许的失败的 AAA 事务。

步骤 9 点击**确定 (OK)**。

系统将关闭 **Add AAA Server Group** 对话框，并将新服务器组添加到 **AAA Server Groups** 表。

步骤 10 点击 **Apply** 以将更改保存到运行配置。

向组中添加 TACACS+ 服务器

要将 TACACS+ 服务器添加到服务器组，请执行以下操作：

过程

步骤 1 依次选择 **Configuration** > **Device Management** > **Users/AAA** > **AAA Server Groups**。

步骤 2 点击要向其添加服务器的服务器组。

步骤 3 在 **Servers in the Selected Group** 区域点击 **Add**。

系统将为该服务器组显示 **Add AAA Server Group** 对话框。

步骤 4 选择身份验证服务器所在接口的名称。

步骤 5 为正添加到组中的服务器添加名称或 IP 地址。

步骤 6 指定与服务器的连接尝试超时值。

指定服务器的超时间隔（1-300 秒）；默认值为 10 秒。对于每个 AAA 事务，ASA 将重试连接尝试（基于重试间隔），直到达到超时。如果连续失败事务的数量达到 AAA 服务器组中指定的 maximum-failed-attempts 上限，则将会停用 AAA 服务器，并且 ASA 开始向另一台 AAA 服务器（如果已配置）发送请求。

步骤 7 指定服务器端口。服务器端口是端口号 139 或 ASA 与 TACACS+ 服务器进行通信所用的 TCP 端口号。

步骤 8 指定服务器密钥。向 ASA 进行 TACACS+ 服务器身份验证所用的共享密钥。您在此处配置的服务器密钥，应与在 TACACS+ 服务器上配置的密钥匹配。如果您不知道服务器密钥，请询问 TACACS+ 服务器管理员。最大字段长度为 64 个字符。

步骤 9 点击 **OK**。

系统将关闭 **Add AAA Server Group** 对话框，并会将 AAA 服务器添加到 AAA 服务器组。

步骤 10 点击 **Apply** 以将更改保存到运行配置。

添加身份验证提示

您可以指定在 AAA 身份验证质询过程中，将会向用户显示的文本。要求通过 TACACS+ 服务器进行用户身份验证时，您可以通过 ASA 为 HTTP、FTP 和 Telnet 访问指定 AAA 质询文本。此文本是主要用于修饰目的，并且显示在用户登录时看到的用户名和密码提示上方。

如果不指定身份验证提示，则用户在使用 RADIUS 服务器进行身份验证时会看到以下信息：

连接类型	默认提示
FTP	FTP 身份验证
HTTP	HTTP 身份验证
Telnet	无

要添加身份验证提示，请执行以下操作：

过程

步骤 1 依次选择**配置** > **设备管理** > **用户/AAA** > **身份验证提示**。

步骤 2 添加用户登录时在用户名和密码提示上方看到的文本。

下表显示身份验证提示的允许字符数限制：

应用	身份验证提示的字符数限制
Microsoft Internet Explorer	37
Telnet	235

应用	身份验证提示的字符数限制
FTP	235

步骤 3 在 **User accepted message** 和 **User rejected message** 字段中添加消息。

如果是通过 Telnet 进行用户身份验证，则可以使用 **User accepted message** 和 **User rejected message** 选项来显示不同的状态提示，以表明 AAA 服务器是接受，还是拒绝身份验证尝试。

如果 AAA 服务器对用户进行身份验证，则 ASA 会向用户显示 **User accepted message** 文本（如已指定）；否则， 会显示 **User rejected message** 文本（如已指定）。HTTP 和 FTP 会话的身份验证仅在提示时才会显示质询文本。系统不会显示 User accepted message 和 User rejected message 文本。

步骤 4 点击 **Apply** 以将更改保存到运行配置。

测试 TACACS+ 服务器身份验证和授权

要确认 ASA 是否能够联系 TACACS+ 服务器并对用户进行身份验证或授权，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备管理** > **用户/AAA** > **AAA 服务器组**。

步骤 2 点击服务器所在的服务器组。

步骤 3 点击要测试的服务器。

步骤 4 点击 **Test**。

系统将针对所选服务器显示 **Test AAA Server** 对话框。

步骤 5 点击要执行的测试的类型 - **Authentication** 或 **Authorization**。

步骤 6 输入用户名。

步骤 7 如果要测试身份验证，请输入该用户名的密码。

步骤 8 点击 **OK**。

ASA 将向服务器发送身份验证或授权测试消息。如果测试失败，系统会显示错误消息。

监控用于 AAA 的 TACACS+ 服务器

请参阅以下用于监控用于 AAA 的 TACACS+ 服务器的命令：

- **Monitoring > Properties > AAA Servers**

  此窗格显示已配置的 TACACS+ 服务器统计信息。

- **Tools > Command Line Interface**

  您可以在此窗格中发出各种非交互式命令并查看结果。

用于 AAA 的 TACACS+ 服务器的历史记录

表 *3:* 用于 *AAA* 的 *TACACS+* 服务器的历史记录

功能名称	平台版本	说明
TACACS+ 服务器	7.0(1)	介绍如何配置用于 AAA 的 TACACS+ 服务器。 引入了以下屏幕： Configuration > Device Management > Users/AAA > AAA Server Groups Configuration > Device Management > Users/AAA > Authentication Prompt。
包含 IPv6 地址、用于 AAA 的 TACACS+ 服务器	9.7(1)	现在可以将 IPv4 或 IPv6 地址用于 AAA 服务器。
每个组的 AAA 服务器组和服务器的数量上限都增加了。	9.13(1)	您可以配置更多 AAA 服务器组。在单情景模式下，您可以配置 200 AAA 服务器组（前一个限制为100）。在多情景模式下，您可以配置 8（前一个限制为4个）。 此外，在多情景模式下，您可以每组配置 8 个服务器（每个组的前一个限制为 4 个服务器）。单情景模式的每组限制 16，保持不变。 修改了 AAA 屏幕以接受这些新的限制。

用于 **AAA** 的 **TACACS+** 服务器的历史记录

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。