# 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 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** 确定服务器组名称和协议。

**aaa-server** *server_tag* **protocol tacacs+**

示例：

```
ciscoasa(config)# aaa-server servergroup1 protocol tacacs+
```

当您输入 **aaa-server protocol** 命令时，系统将会进入 aaa-server 组配置模式。

**步骤 2** 指定在尝试下一服务器前，会向组中带有 AAA 服务器的失败的 AAA 事务最大数量发送的请求的最大数量。

**max-failed-attempts** 编号

示例：

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

*number* 参数的范围可介于 1 到 5 之间。默认值为 3。

如果您使用本地数据库（仅用于管理访问）配置了回退方法，并且组中的所有服务器都无法响应，或者其响应无效，则会将该组视为无响应，并将尝试回退方法。该服务器组会在10分钟（默认值）内保持标记为无响应，以确保该时段内其他AAA请求不会尝试联系该服务器组，而是立即使用回退方法。要更改默认的无响应期间，请参阅下一步中的 **reactivation-mode** 命令。

如果没有回退方法，则 ASA 将继续重试该组中的服务器。

**步骤 3** 指定用于重新激活组中的故障服务器的方法（重新激活策略）。

**reactivation-mode** {**depletion** [ **deadtime** *minutes*] | **timed**}

示例：

```
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
```

**depletion** 关键字仅在组中的所有服务器都处于非活动状态后才会重新激活故障服务器。

**deadtime** *minutes* 关键字参数对用于指定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，范围介于 0 到 1440（以分钟为单位）之间。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。默认值为 10 分钟。

**timed** 关键字可在 30 秒停机时间后重新激活故障服务器。

**步骤 4** 将记帐消息发送到组中的所有服务器。

**accounting-mode simultaneous**

示例：

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

如要恢复仅向活动服务器发送消息的默认设置，请输入 **accounting-mode single** 命令。

### 示例

以下示例显示，如何添加拥有一台主用服务器和一台备用服务器的一个 TACACS+ 组。

```
ciscoasa(config)# aaa-server AuthInbound protocol tacacs+
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.1
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.2
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey2
ciscoasa(config-aaa-server-host)# exit
```

# 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** 确定 TACACS+ 服务器，以及该服务器所属的服务器组。

**aaa-server** *server_group* [**(***interface_name***)**] **host** *server_ip*

示例：

```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

如果不指定 **(***interface_name***)**，则 ASA 默认使用**内部**。

服务器可以使用 IPv4 或 IPv6 地址。

**步骤 2** 指定与服务器的连接尝试超时值。

**timeout** 秒

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 **retry-interval** 命令中定义的间隔），直到达到超时。如果连续失败事务数量达到 AAA 服务器组中 max-failed-attempts 命令上指定的上限，则将会停用 AAA 服务器，并且ASA 将开始向另一台 AAA 服务器（如果已配置）发送请求。

示例：

```
ciscoasa(config-aaa-server-host)# timeout 15
```

**步骤 3** 指定服务器端口作为端口号 49，或 ASA 与 TACACS+ 服务器进行通信所用的 TCP 端口号。

**server-port** *port_number*

示例：

```
ciscoasa(config-aaa-server-host)# server-port 49
```

**步骤 4** 指定服务器密钥值，该密钥值用于面向 TACACS+ 服务器对 NAS 进行身份验证。

**key**

示例：

```
ciscoasa(config-aaa-host)# key myexamplekey1
```

此密钥值是一个区分大小写的字母数字关键字，最大长度为 127 个字符，它的值与 TACACS+ 服务器上的密钥相同。超出127个字符后的所有字符都会被忽略。该密钥会在客户端和服务器之间使用，用于加密它们之间传输的数据，该密钥在客户端和服务器系统上必须相同。该密钥不能包含空格，但允许包含其他的特殊字符。

# 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：

- **show aaa-server**

  此命令可显示已配置的 TACACS+ 服务器统计信息。输入 **clear aaa-server statistics** 命令可清除 TACACS+ 服务器统计信息。

- **show running-config aaa-server**

  此命令可显示 TACACS+ 服务器运行配置。输入 **clear configure aaa-server** 命令可清除 TACACS+ 服务器配置。

# 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。<br>引入了以下命令：<br>**aaa-server protocol**、**max-failed-attempts**、**reactivation-mode**、**accounting-mode simultaneous**、**aaa-server host**、**aaa authorization exec authentication-server**、**server-port**、**key**、**clear aaa-server statistics**、**clear configure aaa-server**、**show aaa-server**、**show running-config aaa-server**、**username**、**service-type**、**timeout**。 |
| 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）。<br>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。<br>修改了以下命令以接受这些新限制：**aaa-server**、**aaa-server host**。 |

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。