

排除TACACS身份验证问题

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[TACACS的工作原理](#)

[排除TACACS问题](#)

[相关信息](#)

简介

本文档介绍对Cisco IOS®/Cisco IOS-XE路由器和交换机上的TACACS身份验证问题进行故障排除的步骤。

先决条件

要求

Cisco 建议您具有以下主题的基础知识：

- 思科设备上的身份验证、授权和记帐(AAA)配置
- TACACS配置

使用的组件

本文档不限于特定的软件和硬件版本。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

TACACS的工作原理

TACACS+协议使用传输控制协议(TCP)作为传输协议，目标端口号为49。当路由器收到登录请求时，它会与TACACS服务器建立TCP连接，并在连接后向用户显示用户名提示。当用户输入用户名时，路由器会再次与TACACS服务器通信以获取密码提示。用户输入密码后，路由器会将此信息再次发送到TACACS服务器。TACACS服务器验证用户凭证，并向路由器发送响应。AAA会话的结果可以是以下任何一项：

PASS：只有路由器上配置了AAA授权后，服务才开始进行身份验证。此时开始授权阶段。

FAIL：当身份验证失败时，可能会拒绝您进一步访问或提示您按顺序重试日志。它取决于

TACACS+后台程序。在此示例中，如果从服务器收到FAIL，则可以检查为TACACS服务器中的用户配置的策略

错误：表示身份验证期间出错。这可以在后台守护程序中，也可以在后台守护程序与路由器之间的网络连接中。如果收到ERROR响应，路由器通常会尝试使用替代方法进行用户身份验证。

以下是思科路由器上AAA和TACACS的基本配置

```
aaa new-model
aaa authentication log in default group tacacs+ local
aaa authorization exec default group tacacs+ local
!
tacacs server prod
address ipv4 10.106.60.182
key cisco123
!
ip tacacs source-interface Gig 0/0
```

排除TACACS问题

步骤1:

在端口49上使用适当的源接口从路由器通过telnet检验与TACACS服务器的连接。如果路由器无法连接到端口49上的TACACS服务器，则可能存在阻止流量的防火墙或访问列表。

```
Router#telnet 10.106.60.182 49
Trying 10.106.60.182, 49 ... Open
```

第二步：

验证AAA客户端是否在TACACS服务器上正确配置了正确的IP地址和共享密钥。如果路由器有多个传出接口，建议使用此命令配置TACACS源接口。您可以将接口（其IP地址在TACACS服务器上配置为客户IP地址）配置为路由器上的TACACS源接口

```
Router(config)#ip tacacs source-interface Gig 0/0
```

第三步：

验证TACACS源接口是否位于虚拟路由和转发(VRF)上。如果接口位于VRF上，您可以在AAA服务器组下配置VRF信息。有关VRF感知TACACS的配置，请参阅[TACACS配置指南](#)。

第四步：

执行测试aaa并验证我们是否从服务器收到正确的响应

```
Router#test aaa group tacacs+ cisco cisco legacy
Sending password
User successfully authenticated
```

第五步：

如果测试aaa失败，请同时启用这些调试，以分析路由器和TACACS服务器之间的事务以确定根本原因。

```
debug aaa authentication
debug aaa authorization
debug tacacs
debug ip tcp transaction
```

以下是工作场景中的调试输出示例：

```
*Apr 6 13:32:50.462: AAA/BIND(00000054): Bind i/f
*Apr 6 13:32:50.462: AAA/AUTHEN/LOGIN (00000054): Pick method list 'default'
*Apr 6 13:32:50.462: TPLUS: Queuing AAA Authentication request 84 for processing
*Apr 6 13:32:50.462: TPLUS(00000054) log in timer started 1020 sec timeout
*Apr 6 13:32:50.462: TPLUS: processing authentication start request id 84
*Apr 6 13:32:50.462: TPLUS: Authentication start packet created for 84()
*Apr 6 13:32:50.462: TPLUS: Using server 10.106.60.182
*Apr 6 13:32:50.462: TPLUS(00000054)/0/NB_WAIT/2432818: Started 5 sec timeout
*Apr 6 13:32:50.466: TPLUS(00000054)/0/NB_WAIT: socket event 2
*Apr 6 13:32:50.466: TPLUS(00000054)/0/NB_WAIT: wrote entire 38 bytes request
*Apr 6 13:32:50.466: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:50.466: TPLUS(00000054)/0/READ: Would block while reading
*Apr 6 13:32:50.466: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:50.466: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 43 bytes data)
*Apr 6 13:32:50.466: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:50.466: TPLUS(00000054)/0/READ: read entire 55 bytes response
*Apr 6 13:32:50.466: TPLUS(00000054)/0/2432818: Processing the reply packet
*Apr 6 13:32:50.466: TPLUS: Received authen response status GET_USER (7)
*Apr 6 13:32:53.242: TPLUS: Queuing AAA Authentication request 84 for processing
*Apr 6 13:32:53.242: TPLUS(00000054) log in timer started 1020 sec timeout
*Apr 6 13:32:53.242: TPLUS: processing authentication continue request id 84
```

```

*Apr 6 13:32:53.242: TPLUS: Authentication continue packet generated for 84
*Apr 6 13:32:53.242: TPLUS(00000054)/0/WRITE/10882BBC: Started 5 sec timeout
*Apr 6 13:32:53.242: TPLUS(00000054)/0/WRITE: wrote entire 22 bytes request
*Apr 6 13:32:53.246: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:53.246: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 16 bytes data)
*Apr 6 13:32:53.246: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:53.246: TPLUS(00000054)/0/READ: read entire 28 bytes response
*Apr 6 13:32:53.246: TPLUS(00000054)/0/10882BBC: Processing the reply packet
*Apr 6 13:32:53.246: TPLUS: Received authen response status GET_PASSWORD (8)
*Apr 6 13:32:54.454: TPLUS: Queuing AAA Authentication request 84 for processing
*Apr 6 13:32:54.454: TPLUS(00000054) log in timer started 1020 sec timeout
*Apr 6 13:32:54.454: TPLUS: processing authentication continue request id 84
*Apr 6 13:32:54.454: TPLUS: Authentication continue packet generated for 84
*Apr 6 13:32:54.454: TPLUS(00000054)/0/WRITE/2432818: Started 5 sec timeout
*Apr 6 13:32:54.454: TPLUS(00000054)/0/WRITE: wrote entire 22 bytes request
*Apr 6 13:32:54.458: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:54.458: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*Apr 6 13:32:54.458: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:54.458: TPLUS(00000054)/0/READ: read entire 18 bytes response
*Apr 6 13:32:54.458: TPLUS(00000054)/0/2432818: Processing the reply packet
*Apr 6 13:32:54.458: TPLUS: Received authen response status PASS (2)
*Apr 6 13:32:54.462: AAA/AUTHOR (0x54): Pick method list 'default'
*Apr 6 13:32:54.462: TPLUS: Queuing AAA Authorization request 84 for processing
*Apr 6 13:32:54.462: TPLUS(00000054) log in timer started 1020 sec timeout
*Apr 6 13:32:54.462: TPLUS: processing authorization request id 84
*Apr 6 13:32:54.462: TPLUS: Protocol set to None .....Skipping
*Apr 6 13:32:54.462: TPLUS: Sending AV service=shell
*Apr 6 13:32:54.462: TPLUS: Sending AV cmd*
*Apr 6 13:32:54.462: TPLUS: Authorization request created for 84(cisco)
*Apr 6 13:32:54.462: TPLUS: using previously set server 10.106.60.182 from group tacacs+
*Apr 6 13:32:54.462: TPLUS(00000054)/0/NB_WAIT/2432818: Started 5 sec timeout
*Apr 6 13:32:54.462: TPLUS(00000054)/0/NB_WAIT: socket event 2
*Apr 6 13:32:54.462: TPLUS(00000054)/0/NB_WAIT: wrote entire 62 bytes request
*Apr 6 13:32:54.462: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:54.462: TPLUS(00000054)/0/READ: Would block while reading
*Apr 6 13:32:54.470: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:54.470: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 18 bytes data)
*Apr 6 13:32:54.470: TPLUS(00000054)/0/READ: socket event 1
*Apr 6 13:32:54.470: TPLUS(00000054)/0/READ: read entire 30 bytes response
*Apr 6 13:32:54.470: TPLUS(00000054)/0/2432818: Processing the reply packet
*Apr 6 13:32:54.470: TPLUS: Processed AV priv-lvl=15
*Apr 6 13:32:54.470: TPLUS: received authorization response for 84: PASS
*Apr 6 13:32:54.470: AAA/AUTHOR/EXEC(00000054): processing AV cmd=
*Apr 6 13:32:54.470: AAA/AUTHOR/EXEC(00000054): processing AV priv-lvl=15
*Apr 6 13:32:54.470: AAA/AUTHOR/EXEC(00000054): Authorization successful

```

这是当TACACS服务器配置了错误的预共享密钥时来自路由器的调试输出示例。

```

*Apr 6 13:35:07.826: AAA/BIND(00000055): Bind i/f
*Apr 6 13:35:07.826: AAA/AUTHEN/LOGIN (00000055): Pick method list 'default'
*Apr 6 13:35:07.826: TPLUS: Queuing AAA Authentication request 85 for processing
*Apr 6 13:35:07.826: TPLUS(00000055) log in timer started 1020 sec timeout
*Apr 6 13:35:07.826: TPLUS: processing authentication start request id 85
*Apr 6 13:35:07.826: TPLUS: Authentication start packet created for 85()
*Apr 6 13:35:07.826: TPLUS: Using server 10.106.60.182
*Apr 6 13:35:07.826: TPLUS(00000055)/0/NB_WAIT/225FE2DC: Started 5 sec timeout
*Apr 6 13:35:07.830: TPLUS(00000055)/0/NB_WAIT: socket event 2
*Apr 6 13:35:07.830: TPLUS(00000055)/0/NB_WAIT: wrote entire 38 bytes request

```

```
*Apr 6 13:35:07.830: TPLUS(00000055)/0/READ: socket event 1
*Apr 6 13:35:07.830: TPLUS(00000055)/0/READ: Would block while reading
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: socket event 1
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: socket event 1
*Apr 6 13:35:07.886: TPLUS(00000055)/0/READ: read entire 18 bytes response
*Apr 6 13:35:07.886: TPLUS(00000055)/0/225FE2DC: Processing the reply packet
*Apr 6 13:35:07.886: TPLUS: received bad AUTHEN packet: length = 6, expected 43974
*Apr 6 13:35:07.886: TPLUS: Invalid AUTHEN packet (check keys).
```

相关信息

- [Cisco IOS上的TACACS配置](#)
- [技术支持和文档 - Cisco Systems](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。