

排除故障TACACS认证问题

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[TACACS如何工作](#)

[排除故障TACACS问题](#)

[相关信息](#)

简介

本文描述步骤排除故障终端访问控制器访问控制系统在思科IOS/IOS-XE路由器和交换机的验证(TACACS)问题。

先决条件

要求

Cisco 建议您具有以下主题的基础知识：

- 在Cisco设备的验证、授权和核算(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。

TACACS如何工作

TACACS+协议使用传输控制协议(TCP)作为传输协议用目的端口49。当路由器收到登录请求时，建立TCP连接用用户名提示显示给用户的TACACS服务器，张贴。当用户输入用户名时，路由器用密码提示的TACACS服务器再连通。一旦用户输入密码，路由器发送对再TACACS服务器的此信息。TACACS服务器验证用户凭证并且发送答复回到路由器。AAA会话的结果可以是其中每一个：

密码：当您验证时服务开始，只有当AAA授权在路由器配置。授权相位此时开始。

FAIL：当您失败验证。您也许拒绝进一步访问或是被提示的重试登录顺序，根据TACACS+守护程序。在这中，如果接收从服务器的FAIL您可能需要检查配置的策略TACACS服务器的用户

ERROR:它指示在验证时发生的一个错误。这可以在守护程序或在守护程序和路由器之间的网络连

接。如果错误反应接收，路由器典型地设法使用替代方法验证用户。

这些是AAA在Cisco路由器的基本配置和TACACS

```
aaa new-model

aaa authentication login 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
```

排除故障TACACS问题

步骤1.验证连接到有一telnet的TACACS服务器在从路由器的端口49有适当的源接口的。万一路由器不能连接到在波尔特49的TACACS服务器，也许有某防火墙或访问列表阻塞流量。

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

步骤2.验证AAA客户端在TACACS服务器适当地配置用正确IP地址和共享密钥。如果路由器有多流出接口，通过使用以下命令，被建议配置TACACS源接口。您可能需要配置接口，IP地址配置作为在TACACS服务器的客户端IP地址，作为在路由器的TACACS源接口

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

步骤3.请验证，如果TACACS源接口在虚拟路由和转发(VRF)。万一接口在VRF，您可能需要配置VRF信息在AAA服务器组下。VRF意识TACACS的配置的参考的[链路](#)。

步骤4.执行测验aaa并且验证我们接收从服务器的正确答复

```
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分析在路由器和TACACS服务器之间的处理识别根本原因。

```
debug aaa authentication

debug aaa authorization

debug tacacs

debug ip tcp transaction
```

这是在一个工作的方案的一debug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) login 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) login 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) login 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) login 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
```

当TACACS服务器配置与一错误的预共用的密钥时，这是从路由器的一debug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) login 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

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