

Solucionar problemas de autenticación de TACACS

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Cómo Funciona TACACS](#)

[Solucionar problemas de TACACS](#)

[Información Relacionada](#)

Introducción

Este documento describe los pasos para resolver problemas de autenticación TACACS en routers y switches Cisco IOS®/Cisco IOS® XE.

Prerequisites

Requirements

Cisco recomienda tener conocimientos básicos sobre estos temas:

- Configuración de autenticación, autorización y contabilidad (AAA) en dispositivos Cisco
- configuración de TACACS

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Cómo Funciona TACACS

El protocolo TACACS+ utiliza el protocolo de control de transmisión (TCP) como protocolo de transporte con el número de puerto de destino 49. Cuando el router recibe una solicitud de inicio de sesión, establece una conexión TCP con el servidor TACACS y publica el mensaje de nombre

de usuario que se muestra al usuario. Cuando el usuario ingresa el nombre de usuario, el router nuevamente se comunica con el servidor TACACS para la solicitud de contraseña. Una vez que el usuario introduce la contraseña, el router envía esta información al servidor TACACS de nuevo. El servidor TACACS verifica las credenciales del usuario y envía una respuesta al router. El resultado de una sesión AAA puede ser cualquiera de los siguientes:

PASS: cuando se autentica, el servicio comienza solamente si la autorización AAA se configura en el router. La fase de autorización comienza en este momento.

FAIL (Fallo): Si no ha superado la autenticación, se le puede denegar el acceso adicional o se le puede solicitar que vuelva a intentar el registro en secuencia. Depende del daemon TACACS+. En este caso, puede verificar las políticas configuradas para el usuario en el servidor TACACS, si recibe un FAIL del servidor.

ERROR: indica que se ha producido un error durante la autenticación. Esto puede ser en el daemon o en la conexión de red entre el daemon y el router. Si se recibe una respuesta de ERROR, el router normalmente intenta utilizar un método alternativo para autenticar al usuario.

Estas son las configuraciones básicas de AAA y TACACS en un router Cisco.

```
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
```

Solucionar problemas de TACACS

Paso 1.

Verifique la conectividad con el servidor TACACS con un telnet en el puerto 49 desde el router con la interfaz de origen apropiada. En caso de que el router no pueda conectarse al servidor TACACS en el puerto 49, puede haber algún firewall o listas de acceso que bloqueen el tráfico.

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

Paso 2.

Verifique que el cliente AAA esté configurado correctamente en el servidor TACACS con la dirección IP correcta y la clave secreta compartida. Si el router tiene varias interfaces salientes, se sugiere configurar la interfaz de origen TACACS con el uso de este comando. Puede configurar la interfaz, cuya dirección IP se configura como dirección IP del cliente en el servidor TACACS, como la interfaz de origen TACACS en el router

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

Paso 3.

Verifique si la interfaz de origen TACACS está en un Virtual Routing and Forwarding (VRF). En caso de que la interfaz esté en un VRF, puede configurar la información VRF bajo el grupo de servidores AAA. Consulte la [Guía de Configuración de TACACS](#) para la configuración de TACACS que reconoce VRF.

Paso 4.

Realice la prueba aaa y compruebe que recibe la respuesta correcta del servidor.

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

Paso 5.

Si la prueba aaa falla, habilite estos debugs juntos para analizar las transacciones entre el router y el servidor TACACS para identificar la causa raíz.

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

Este es un ejemplo de resultado de depuración en un escenario de trabajo:

*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 NoneSkipping
*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
```

Este es un ejemplo de salida de depuración del router cuando el servidor TACACS está configurado con una clave previamente compartida incorrecta.

```
*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).
```

Información Relacionada

- [Configuración de TACACS en Cisco IOS](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).