Pesquise defeitos edições da autenticação TACACS

Índice

Introdução

Este documento descreve as etapas para pesquisar defeitos edições da autenticação do Terminal Access Controller Access Control System (TACACS) no Roteadores e no Switches de Cisco IOS/IOS-XE.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento básico destes assuntos:

- Configuração da autenticação, da autorização e da contabilidade (AAA) em dispositivos Cisco
- Configuração de TACACS

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Como o TACACS trabalha

O protocolo TACACS+ usa o Transmission Control Protocol (TCP) como o protocolo de transporte com número de porta de destino 49. Quando o roteador recebe uma solicitação de login, estabelece uma conexão de TCP com o servidor de TACACS, afixa que uma alerta de nome de usuário é indicada ao usuário. Quando o usuário incorpora o username, o roteador comunica-se outra vez com o servidor de TACACS para a solicitação da senha. Uma vez que o usuário incorpora a senha, o roteador envia esta informação ao servidor de TACACS outra vez. O

servidor de TACACS verifica as credenciais do usuário e envia uma resposta de volta ao roteador. O resultado de uma sessão de AAA pode ser qualquer um:

PASSAGEM: Quando você está autenticado o serviço começa somente se a autorização de AAA é configurada no roteador. A fase da autorização começa neste tempo.

FALHA: Quando você falhar a autenticação. Você pôde ser negado um acesso mais adicional ou ser alertado para experimentar de novo a sequência de login, segundo o demônio TACACS+. Nisto, você pode precisar de verificar as políticas configuradas para ver se há o usuário no servidor de TACACS, se você recebe uma FALHA do server

ERRO: Indica que um erro ocorreu durante a autenticação. Isto pode estar no demônio ou na conexão de rede entre o demônio e o roteador. Se uma resposta de erro é recebida, o roteador tenta tipicamente usar um método alternativo para autenticar o usuário.

Estes são a configuração básica do AAA e TACACS em um roteador Cisco

```
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
```

Pesquise defeitos edições TACACS

Etapa 1. Verifique a Conectividade ao servidor de TACACS com um **telnet na** porta 49 do roteador com interface de origem apropriada. Caso que o roteador não pode conectar ao servidor de TACACS na porta 49, pôde haver alguma Firewall ou lista de acessos que obstruem o tráfego.

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

Etapa 2. Verifique que o cliente de AAA está configurado corretamente no servidor de TACACS com o endereço IP de Um ou Mais Servidores Cisco ICM NT correto e a chave secreta compartilhada. Se o roteador tem interfaces enviadas múltiplas, está sugerido para configurar a interface de origem TACACS usando o comando seguinte. Você pode precisar de configurar a relação, de que o endereço IP de Um ou Mais Servidores Cisco ICM NT é configurado como o endereço IP cliente no servidor de TACACS, como a interface de origem TACACS no roteador

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

Etapa 3. Verifique se a interface de origem TACACS está em um roteamento virtual e em uma transmissão (VRF). Caso que a relação está em um VRF, você pode precisar de configurar a

informação VRF sob o Grupo de servidores AAA. Consulte o link para a configuração de VRF TACACS ciente.

Etapa 4. Execute o **teste aaa** e verifique que nós estamos recebendo a resposta correta do server

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

Etapa 5. Se o **teste aaa** falha, permita estes debuga junto para analisar as transações entre o roteador e o servidor de TACACS para identificar a causa de raiz.

```
debug aaa authentication

debug aaa authorization

debug tacacs

debug ip tcp transaction
```

Este é um exemplo de debug em uma encenação de trabalho:

```
*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
```

Este é um exemplo de debug do roteador, quando o servidor de TACACS é configurado com pre uma chave compartilhada errada

```
*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).
```

Informações Relacionadas

- Configuração de TACACS no Cisco IOS
- **Suporte Técnico e Documentação - Cisco Systems**