ACS 5.x AAA que põe em esconderijo no exemplo da configuração do IOS da Cisco

Índice

Introdução

Este documento descreve as etapas necessárias a fim configurar pôr em esconderijo de credenciais do usuário admin TACACS+ para o telnet e a linha acesso VTY. Pôr em esconderijo da autorização e da autenticação foi integrado na versão 15.0(1)M do ® do Cisco IOS. Esta característica permite um roteador de armazenar credenciais do Authentication, Authorization, and Accounting (AAA) em seu esconderijo depois que recebe uma resposta TACACS+ a um pedido AAA. O esconderijo está usado a fim impulsionar o desempenho e reduzir a quantidade de pedidos enviados ao servidor AAA, ou como um método de autenticação da reserva caso que o servidor AAA é inacessível.

Pré-requisitos

Requisitos

Cisco recomenda que você:

- Confirme a conectividade IP entre o roteador e a versão 5.x do Serviço de controle de acesso Cisco Secure (ACS).
- Defina o roteador no ACS como um cliente de AAA (dispositivos de rede) com o mesmo segredo compartilhado.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão de ACS 5
- Roteadores que executa a versão do Cisco IOS 15.1

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.

Configurar

Configuração em um roteador do Cisco IOS

1. Incorpore estes comandos a fim definir o servidor de TACACS e a chave pré-compartilhada:

```
Router(config)#tacacs-server host 192.168.159.41
Router(config)#tacacs-server timeout 4
Router(config)#tacacs-server key SECRET12345
```

2. Incorpore estes comandos a fim definir os grupos do perfil do esconderijo.
   Note: Cada nome de perfil deve combinar um username AAA.

```
Router(config)#aaa cache profile admin
Router(config-profile-map)# profile peteradmin
```

3. Incorpore estes comandos a fim atribuir a authentication e autorização que põe em esconderijo regras aos Grupos de servidores AAA:

```
Router(config-profile-map)# aaa group server tacacs+ admin-tac
Router(config-sg-tacacs+)# server 192.168.159.41
Router(config-sg-tacacs+)# cache authentication profile admin
Router(config-sg-tacacs+)# cache authorization profile admin
```

4. Defina as listas de método da authentication e autorização que contêm o método do esconderijo. Neste exemplo de configuração, o esconderijo é usado somente se os servidores AAA não respondem. Se a ordem é comutada **para pôr em esconderijo admin-TAC o grupo admin-TAC**, o esconderijo está olhado-acima primeiramente.
   Note: A senha da possibilidade do TACACS não é posta em esconderijo.

```
aaa authentication login mtac group admin-tac cache admin-tac local
aaa authorization exec default group admin-tac cache admin-tac local
aaa accounting exec default start-stop group admin-tac
```

5. Incorpore estes comandos a fim configurar o TACACS+ nas linhas VTY:

```
Router(config)#line vty 0 4
Router(config-line)#login authentication mtac
```

Configuração no ACS

1. Crie um usuário no ACS. Navegue aos **usuários e as lojas da identidade > criam o usuário**. Este exemplo usa o usuário de teste **Peteradmin**.

2. Os usuários admin TACACS+ precisam um perfil do shell que lhes permita um nível de privilégio de **15** de modo que possam incorporar o **modo enable**. A fim configurar o perfil do shell, navegue aos **elementos da política > à autorização e às permissões > à administração > ao shell do dispositivo perfis**.

3. Crie uma regra de seleção do serviço sob as **políticas de acesso > os serviços do acesso** para combinar o TACACS:

4. Navegue ao **dispositivo Admin priv15 > protocolos permitidos > Protocolos de autenticação seletos**, e configurar os **protocolos permitidos**. Este exemplo usa **PAP/ASCII**.

5. Navegue às **políticas de acesso > ao acesso presta serviços de manutenção > o dispositivo Admin priv15 > identidade**, e configuram a fonte da identidade para **usuários internos**.

6. Configurar a política da autorização sob **políticas de acesso > acesso presta serviços de manutenção > o dispositivo Admin priv15 > autorização**.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Teste o acesso do telnet

Estes debugam são usados a fim verificar a authentication e autorização que põe em esconderijo

para o TACACS+:

- **debugar eventos dos tacacs**
- **debugar o grupo do esconderijo aaa**

O telnet ao roteador com o usuário de TACACS e o TACACS permitem a senha:

```
username: peteradmin
password: peteradmin

R102>en
password: cpeter
R102#

R102#debug tacacs events
R102#debug aaa cache group
R102#
11:35:47.151: TPLUS: Queuing AAA Authentication request 16 for processing
11:35:47.159: TPLUS: processing authentication start request id 16
11:35:47.163: TPLUS: Authentication start packet created for 16()
11:35:47.167: TPLUS: Using server 192.168.159.41
11:35:47.187: TPLUS(00000010)/0/NB_WAIT/69540BEC: Started 4 sec timeout
11:35:47.223: TPLUS(00000010)/0/NB_WAIT: wrote entire 37 bytes request
11:35:47.227: TPLUS: Would block while reading pak header
11:35:47.251: TPLUS(00000010)/0/READ: read entire 12 header bytes (expect 16
bytes)
11:35:47.255: TPLUS(00000010)/0/READ: read entire 28 bytes response
11:35:47.255: TPLUS(00000010)/0/69540BEC: Processing the reply packet
11:35:47.259: TPLUS: Received authen response status GET_USER (7)
11:35:47.263: AAA/AUTHEN/CACHE: No username in response
11:35:56.703: TPLUS: Queuing AAA Authentication request 16 for processing
11:35:56.711: TPLUS: processing authentication continue request id 1611:35:56.715:
TPLUS: Authentication continue packet generated for 16
11:35:56.719: TPLUS(00000010)/0/WRITE/69540BEC: Started 4 sec timeout
11:35:56.727: TPLUS(00000010)/0/WRITE: wrote entire 27 bytes request
11:35:56.751: TPLUS(00000010)/0/READ: read entire 12 header bytes (expect 16
bytes)
11:35:56.751: TPLUS(00000010)/0/READ: read entire 28 bytes response
11:35:56.755: TPLUS(00000010)/0/69540BEC: Processing the reply packet
11:35:56.759: TPLUS: Received authen response status GET_PASSWORD (8)
11:35:56.763: AAA/AUTHEN/CACHE: Request status = 8, cannot add to cache
11:36:02.943: TPLUS: Queuing AAA Authentication request 16 for processing
11:36:02.955: TPLUS: processing authentication continue request id 16
11:36:02.959: TPLUS: Authentication continue packet generated for 16
11:36:02.963: TPLUS(00000010)/0/WRITE/69540BEC: Started 4 sec timeout
11:36:02.967: TPLUS(00000010)/0/WRITE: wrote entire 27 bytes request
11:36:03.971: TPLUS(00000010)/0/READ: read entire 12 header bytes (expect 6
bytes)
11:36:03.975: TPLUS(00000010)/0/READ: read entire 18 bytes response
11:36:03.975: TPLUS(00000010)/0/69540BEC: Processing the reply packet
11:36:03.979: TPLUS: Received authen response status PASS (2)
11:36:03.983: AAA/AUTHEN/CACHE: SG profile admin
11:36:03.987: AAA/AUTHEN/CACHE: SG block for admin found
11:36:03.987: AAA/AUTHEN/CACHE: matching profile found for peteradmin in admin
11:36:03.991: AAA/AUTHEN/CACHE: Dealing with authen_type = 1
11:36:03.995: TPLUS: Error occurs in reading packet header, shutdown the single
connection
11:36:04.047: TPLUS: Queuing AAA Authorization request 16 for processing
11:36:04.055: TPLUS: processing authorization request id 16
11:36:04.059: TPLUS: Protocol set to None .....Skipping
11:36:04.063: TPLUS: Sending AV service=shell
11:36:04.067: TPLUS: Sending AV cmd*
```

```
11:36:04.067: TPLUS: Authorization request created for 16(peteradmin)
11:36:04.071: TPLUS: using previously set server 192.168.159.41 from group
admin-tac
11:36:04.091: TPLUS(00000010)/0/NB_WAIT/689C0FDC: Started 4 sec timeout
11:36:04.127: TPLUS(00000010)/0/NB_WAIT: wrote entire 66 bytes request
11:36:04.131: TPLUS: Would block while reading pak header
11:36:05.319: TPLUS(00000010)/0/READ: read entire 12 header bytes (expect 6
bytes)
11:36:05.323: TPLUS(00000010)/0/READ: read entire 18 bytes response
11:36:05.327: TPLUS(00000010)/0/689C0FDC: Processing the reply packet
11:36:05.327: TPLUS: received authorization response for 16: PASS
11:36:05.335: AAA/AUTHEN/CACHE: SG profile admin
11:36:05.335: AAA/AUTHEN/CACHE: SG block for admin found
11:36:05.339: AAA/AUTHEN/CACHE: matching profile found for peteradmin in admin
11:36:05.339: AAA/AUTHOR/CACHE(00000010): Existing entry no set for authorization
11:36:05.347: TPLUS: Error occurs in reading packet header, shutdown the single
connection
11:36:05.419: TPLUS: Queuing AAA Accounting request 16 for processing
11:36:05.431: TPLUS: processing accounting request id 16
11:36:05.439: TPLUS: Sending AV task_id=6
11:36:05.439: TPLUS: Sending AV timezone=UTC
11:36:05.443: TPLUS: Sending AV service=shell
11:36:05.443: TPLUS: Accounting request created for 16(peteradmin)
11:36:05.447: TPLUS: using previously set server 192.168.159.41 from group
admin-tac
11:36:05.471: TPLUS(00000010)/0/NB_WAIT/689C0FDC: Started 4 sec timeout
11:36:05.523: TPLUS(00000010)/0/NB_WAIT: wrote entire 85 bytes request
11:36:05.523: TPLUS: Would block while reading pak header
11:36:05.587: TPLUS(00000010)/0/READ: read entire 12 header bytes (expect 5
bytes)
11:36:05.591: TPLUS(00000010)/0/READ: read entire 17 bytes response
11:36:05.591: TPLUS(00000010)/0/689C0FDC: Processing the reply packet
11:36:05.595: TPLUS: Received accounting response with status PASS
11:36:05.603: TPLUS: Error occurs in reading packet header, shutdown the single
connection
R102#
```

Verifique o esconderijo

Incorpore estes comandos a fim rever e cancelar a informação de cache:

- mostre o [cache group name] todo do grupo do esconderijo aaa
- cancele o [cache group name] todo do grupo do esconderijo aaa

```
R102#show aaa cache group admin-tac all
------------------------------------------------------------
Entries in Profile dB admin-tac for exact match
------------------------------------------------------------
Profile: peteradmin
Updated: 00:00:42
Parse User: N
Authen User: Y
Query Count: 2
6731AF7C 0 00000009 username(422) 10 peteradmin, service shell, protocol none
6731AF8C 0 0000000A cmd(73) 0 , service shell, protocol none
------------------------------------------------------------
Entries in Profile dB admin-tac for regexp match
------------------------------------------------------------
No entries found for regexp match
```

Simule uma falha ACS

Desligue o servidor ACS da rede a fim simular uma falha e invocar a verificação do esconderijo.

O telnet ao roteador com o usuário de TACACS e o local permitem a senha (permita a senha do TACACS não pode ser posto em esconderijo):

```
username: peteradmin
password: peteradmin

R102>en
password:
R102#
11:39:10.723: TPLUS: Queuing AAA Authentication request 17 for processing
11:39:10.735: TPLUS: processing authentication start request id 17
11:39:10.739: TPLUS: Authentication start packet created for 17()
11:39:10.743: TPLUS: Using server 192.168.159.41
11:39:10.759: TPLUS(00000011)/0/NB_WAIT/68A4A820: Started 4 sec timeout
11:39:14.759: TPLUS(00000011)/0/NB_WAIT/68A4A820: timed out
11:39:14.763: TPLUS(00000011)/0/NB_WAIT/68A4A820: timed out, clean up
11:39:14.767: TPLUS(00000011)/0/68A4A820: Processing the reply packet
11:39:14.771: AAA/AUTHEN/CACHE: Don't cache responses with errors
11:39:14.779: AAA/AUTHEN/CACHE(00000011): GET_USER for username NULL
11:39:23.315: AAA/AUTHEN/CACHE(00000011): GET_PASSWORD for username peteradmin
11:39:25.191: AAA/AUTHEN/CACHE(00000011): Found a match
11:39:25.195: AAA/AUTHEN/CACHE(00000011): PASS for username peteradmin
11:39:25.215: TPLUS: Queuing AAA Authorization request 17 for processing
11:39:25.223: TPLUS: processing authorization request id 17
11:39:25.227: TPLUS: Protocol set to None .....Skipping
11:39:25.231: TPLUS: Sending AV service=shell
11:39:25.235: TPLUS: Sending AV cmd*
11:39:25.239: TPLUS: Authorization request created for 17(peteradmin)
11:39:25.239: TPLUS: Using server 192.168.159.41
11:39:25.243: TPLUS(00000011)/0/IDLE/689C3A0C: got immediate connect on new 0
11:39:25.247: TPLUS(00000011)/0/WRITE/689C3A0C: Started 4 sec timeout
11:39:25.251: TPLUS(00000011)/0/WRITE: write to 192.168.159.41 failed with errno
257((ENOTCONN))
11:39:25.255: TPLUS: Protocol set to None .....Skipping
11:39:25.259: TPLUS: Sending AV service=shell
11:39:25.259: TPLUS: Sending AV cmd*
11:39:25.263: TPLUS: Authorization request created for 17(peteradmin)
11:39:25.263: TPLUS(00000011): Start write failed
11:39:29.247: TPLUS(00000011)/0/WRITE/689C3A0C: timed out
11:39:29.251: TPLUS: Protocol set to None .....Skipping
11:39:29.255: TPLUS: Sending AV service=shell
11:39:29.255: TPLUS: Sending AV cmd*
11:39:29.259: TPLUS: Authorization request created for 17(peteradmin)
11:39:29.263: TPLUS(00000011)/0/WRITE/689C3A0C: timed out, clean up
11:39:29.267: TPLUS: Error occured while writing, shutdown the single
connection
11:39:29.267: TPLUS(00000011)/0/689C3A0C: Processing the reply packet
11:39:29.271: AAA/AUTHEN/CACHE: Don't cache responses with errors
11:39:29.331: TPLUS: Queuing AAA Accounting request 17 for processing
11:39:29.343: TPLUS: processing accounting request id 17
11:39:29.351: TPLUS: Sending AV task_id=7
11:39:29.351: TPLUS: Sending AV timezone=UTC
11:39:29.355: TPLUS: Sending AV service=shell
11:39:29.359: TPLUS: Accounting request created for 17(peteradmin)
11:39:29.359: TPLUS: using previously set server 192.168.159.41 from group
admin-tac
11:39:29.379: TPLUS(00000011)/0/NB_WAIT/689C0FDC: Started 4 sec timeout
```

```
11:39:33.375: TPLUS(00000011)/0/NB_WAIT/689C0FDC: timed out
11:39:33.379: TPLUS: Choosing next server 192.168.159.41
11:39:33.383: TPLUS(00000011)/689C0FDC: releasing old socket 0
11:39:33.387: TPLUS(00000011)/0/NB_WAIT/689C0FDC: got immediate connect on
new 0
11:39:33.387: TPLUS(00000011)/0/WRITE/689C0FDC: Started 4 sec timeout
11:39:33.391: TPLUS(00000011)/0/WRITE: write to 192.168.159.41 failed with errno
257((ENOTCONN))
11:39:33.399: TPLUS: Sending AV task_id=7
11:39:33.399: TPLUS: Sending AV timezone=UTC
11:39:33.403: TPLUS: Sending AV service=shell
11:39:33.403: TPLUS: Accounting request created for 17(peteradmin)
11:39:33.407: TPLUS(00000011)/0/WRITE/689C0FDC: Write failed, this request
will be cleaned up after timeout
11:39:37.387: TPLUS(00000011)/0/WRITE/689C0FDC: timed out
11:39:37.395: TPLUS: Sending AV task_id=7
11:39:37.395: TPLUS: Sending AV timezone=UTC
11:39:37.399: TPLUS: Sending AV service=shell
11:39:37.403: TPLUS: Accounting request created for 17(peteradmin)
11:39:37.407: TPLUS: Choosing next server 192.168.159.41
11:39:37.407: TPLUS(00000011)/689C0FDC: releasing old socket 0
11:39:37.411: TPLUS(00000011)/0/WRITE/689C0FDC: got immediate connect on
new 0
11:39:37.415: TPLUS(00000011)/0/WRITE/689C0FDC: Started 4 sec timeout
11:39:37.415: TPLUS(00000011)/0/WRITE: write to 192.168.159.41 failed with errno
257((ENOTCONN))
11:39:37.423: TPLUS: Sending AV task_id=7
11:39:37.427: TPLUS: Sending AV timezone=UTC
11:39:37.427: TPLUS: Sending AV service=shell
11:39:37.431: TPLUS: Accounting request created for 17(peteradmin)
11:39:37.431: TPLUS(00000011)/0/WRITE/689C0FDC: Write failed, this request
will be cleaned up after timeout
11:39:41.411: TPLUS(00000011)/0/WRITE/689C0FDC: timed out
11:39:41.419: TPLUS: Sending AV task_id=7
11:39:41.423: TPLUS: Sending AV timezone=UTC
11:39:41.423: TPLUS: Sending AV service=shell
11:39:41.427: TPLUS: Accounting request created for 17(peteradmin)
11:39:41.431: TPLUS(00000011)/0/WRITE/689C0FDC: timed out, clean up
11:39:41.431: TPLUS: Error occured while writing, shutdown the single
connection
11:39:41.435: TPLUS(00000011)/0/689C0FDC: Processing the reply packet

Cached username and password works.

R102#clear aaa cache group admin-tac all
R102#show aaa cache group admin-tac all
------------------------------------------------------------
Entries in Profile dB admin-tac for exact match
------------------------------------------------------------
No entries found in Profile dB
```

Troubleshooting

A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.