Controle AAA do Server do HTTP IO

Índice

Introdução

Este documento mostra como controlar o acesso ao Server do HTTP de Cisco IOS® com Authentication, Authorization, and Accounting (AAA). O controle do acesso ao Server do HTTP do Cisco IOS com AAA varia baseado no Cisco IOS Software Release.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Determine que versão do Server do HTTP você tem

Emita o **HTTP do nome dos subsys do** exec command show a fim ver que versão do Server do HTTP você tem.

```
router1#show subsys name http Class Version http Protocol 1.001.001
```

Este é um sistema com o server HTTP V1.1. O Cisco IOS Software Release 12.2(15)T e todo o Cisco IOS Software 12.3 liberações têm HTTP V1.1.

```
router2#show subsys name http Class Version http Protocol 1.000.001
```

Este é um sistema com o server HTTP V1. Os Cisco IOS Software Release mais cedo do que 12.2(15)T (inclui Cisco IOS Software Releases 12.2(15)JA e 12.2(15)XR) têm HTTP V1.

Cisco IOS Software com o server HTTP V1

Nas liberações do Cisco IOS Software que contêm o server HTTP V1, linhas de terminal virtual do uso das sessões de HTTP (vtys). Consequentemente, a autenticação de HTTP e a autorização são controladas com os mesmos métodos que são configurados para os vtys.

```
ip http server
!
aaa new-model
aaa authentication login VTYSandHTTP radius local
aaa authorization exec VTYSandHTTP radius local
!
ip http authentication aaa
!
line vty 0 19
!--- The number of vtys you have. login authentication VTYSandHTTP authorization exec
VTYSandHTTP
```

Cisco IOS Software com o server HTTP V1.1

Nas liberações do Cisco IOS Software com o server HTTP V1.1, as sessões de HTTP não usam vtys. Usam os soquetes.

Server HTTP V1.1 - Antes do CSCeb82510 da identificação de bug Cisco

Antes da integração do CSCeb82510 da identificação de bug Cisco (clientes registrados somente) nos Cisco IOS Software Releases 12.3(7.3) e 12.3(7.3)T, o server HTTP V1.1 tem que usar o mesmo método de authentication e autorização que é configurado para o console.

```
ip http server
!
aaa new-model
aaa authentication login CONSOLEandHTTP radius local
aaa authorization exec CONSOLEandHTTP radius local
!
ip http authentication aaa
!
line con 0
 login authentication CONSOLEandHTTP
 authorization exec CONSOLEandHTTP
```

Server HTTP V1.1 - Após o CSCeb82510 da identificação de bug Cisco

Com a integração do CSCeb82510 da identificação de bug Cisco (clientes registrados somente) nos Cisco IOS Software Releases 12.3(7.3) e 12.3(7.3)T, o Server do HTTP pode usar métodos de authentication e autorização independentes do seus próprios, com palavras-chaves novas no

comando ip http authentication aaa. As palavras-chaves novas são:

```
router(config)#ip http authentication aaa command-authorization listname router(config)#ip http authentication aaa exec-authorization listname router(config)#ip http authentication aaa login-authentication listname
```

Esta é uma saída de exemplo:

```
ip http server
!
aaa new-model
aaa authentication login HTTPonly radius local
aaa authorization exec HTTPonly radius local
!
ip http authentication aaa
ip http authentication aaa exec-authorization HTTPonly
ip http authentication aaa login-authentication HTTPonly
```

Debug

Emita estes **comandos debug** a fim pesquisar defeitos problemas com autenticação de HTTP/autorização:

```
debug ip tcp transactions
debug modem
!--- If you use the HTTP 1.0 server. debug ip http authentication debug aaa authentication debug aaa authorization debug radius !--- If you use RADIUS. debug tacacs !--- If you use TACACS+.
```

Esta saída mostra que algum exemplo debuga:

```
*Apr 23 13:12:16.871: TCB626DD444 created
*Apr 23 13:12:16.871: TCP0: state was LISTEN -> SYNRCVD [80 -> 64.101.98.203(19662)]
*Apr 23 13:12:16.871: TCP0: Connection to 64.101.98.203:19662, received MSS 1460, MSS is 516
*Apr 23 13:12:16.875: TCP: sending SYN, seq 2078657456, ack 2459301798
*Apr 23 13:12:16.875: TCP0: Connection to 64.101.98.203:19662, advertising MSS 536
*Apr 23 13:12:16.899: TCP0: state was SYNRCVD -> ESTAB [80 -> 64.101.98.203(19662)]

 !--- The TCP connection from the browser on 64.101.98.203 to the !--- local HTTP server is established. *Apr 23 13:12:16.899: TCB62229100 accepting 626DD444 from 64.101.98.203.19662 *Apr 23 13:12:16.899: TCB626DD444 setting property TCP_PID (8) 626FEC84 *Apr 23 13:12:16.899: TCB626DD444 setting property TCP_NO_DELAY (1) 626FEC88 *Apr 23 13:12:16.899: TCB626DD444 setting property TCP_NONBLOCKING_WRITE (10) 626FED14 *Apr 23 13:12:16.899: TCB626DD444 setting property TCP_NONBLOCKING_READ (14) 626FED14 *Apr 23 13:12:16.899: TCB626DD444 setting property unknown (15) 626FED14 *Apr 23 13:12:16.919: HTTP AAA Login-Authentication List name: HTTPauthen *Apr 23 13:12:16.919: HTTP AAA Exec-Authorization List name: HTTPauthor *Apr 23 13:12:16.919: AAA/AUTHEN/LOGIN (00000000): Pick method list 'HTTPauthen' !--- Uses 'HTTPauthen' as the login authentication method. *Apr 23 13:12:16.919: RADIUS/ENCODE(00000000):Orig. component type = INVALID *Apr 23 13:12:16.919: RADIUS/ENCODE(00000000): dropping service type, "radius-server attribute 6 on-for-login-auth" is off *Apr 23 13:12:16.919: RADIUS(00000000): Config NAS IP: 0.0.0.0 *Apr 23 13:12:16.919: RADIUS(00000000): sending *Apr 23 13:12:16.919: RADIUS/ENCODE: Best Local IP-Address 172.16.175.103 for Radius-Server 10.1.2.3 *Apr 23 13:12:16.919: RADIUS(00000000): Send Access-Request to 10.1.2.3:1645 id 1645/2, len 51 *Apr 23 13:12:16.919: RADIUS: authenticator 5F 6E E6 C1 3E 40 5D E2 - FB AC E8 E8 E4 93 BA 98 *Apr 23 13:12:16.919: RADIUS: User-Name [1] 7 "cisco" *Apr 23 13:12:16.919: RADIUS: User-Password [2] 18 * *Apr 23 13:12:16.919: RADIUS: NAS-IP-Address [4] 6 172.16.175.103 !--- Sent an Access-Request to the RADIUS server !--- at 10.1.2.3 using the username of "cisco". *Apr 23 13:12:21.923: RADIUS: Retransmit to (10.1.2.3:1645,1646) for id 1645/2 *Apr 23 13:12:26.923: RADIUS: Retransmit to (10.1.2.3:1645,1646) for id 1645/2 *Apr 23 13:12:31.923: RADIUS: Retransmit to (10.1.2.3:1645,1646) for id 1645/2 *Apr 23 13:12:36.923: RADIUS: No response from (10.1.2.3:1645,1646) for id 1645/2 *Apr 23 13:12:36.923: RADIUS/DECODE: parse response no app start; FAIL *Apr 23 13:12:36.923: RADIUS/DECODE: parse response; FAIL *Apr 23 13:12:36.923: AAA/AUTHOR (0x0): Pick method list 'HTTPauthor' *Apr 23 13:12:36.923:
```

```
RADIUS/ENCODE(00000000):Orig. component type = INVALID *Apr 23 13:12:36.923: RADIUS(00000000):
Config NAS IP: 0.0.0.0 *Apr 23 13:12:36.923: RADIUS(00000000): sending *Apr 23 13:12:36.923:
RADIUS/ENCODE: Best Local IP-Address 172.16.175.103 for Radius-Server 10.1.2.3 *Apr 23
13:12:36.923: RADIUS(00000000): Send Access-Request to 10.1.2.3:1645 id 1645/3, len 57 *Apr 23
13:12:36.927: RADIUS: authenticator AA DB 63 E1 D4 BF 23 9E - 49 71 78 42 A5 A3 44 B8 *Apr 23
13:12:36.927: RADIUS: User-Name [1] 7 "cisco" *Apr 23 13:12:36.927: RADIUS: User-Password [2] 18
* *Apr 23 13:12:36.927: RADIUS: Service-Type [6] 6 Outbound [5] *Apr 23 13:12:36.927: RADIUS:
NAS-IP-Address [4] 6 172.16.175.103 *Apr 23 13:12:41.927: RADIUS: Retransmit to
(10.1.2.3:1645,1646) for id 1645/3 *Apr 23 13:12:46.927: RADIUS: Retransmit to
(10.1.2.3:1645,1646) for id 1645/3 *Apr 23 13:12:51.927: RADIUS: Retransmit to
(10.1.2.3:1645,1646) for id 1645/3 *Apr 23 13:12:56.927: RADIUS: No response from
(10.1.2.3:1645,1646) for id 1645/3 *Apr 23 13:12:56.927: RADIUS/DECODE: parse response no app
start; FAIL *Apr 23 13:12:56.927: RADIUS/DECODE: parse response; FAIL *Apr 23 13:12:56.927:
HTTP: Authentication failed for level 15 !--- Authentication has failed due to no response from
the RADIUS server. *Apr 23 13:12:56.927: TCB626DD444 shutdown writing *Apr 23 13:12:56.927:
TCP0: state was ESTAB -> FINWAIT1 [80 -> 64.101.98.203(19662)] *Apr 23 13:12:56.927: TCP0:
sending FIN *Apr 23 13:12:56.967: TCP0: state was FINWAIT1 -> FINWAIT2 [80 ->
64.101.98.203(19662)] *Apr 23 13:12:56.967: TCP0: FIN processed *Apr 23 13:12:56.971: TCP0:
state was FINWAIT2 -> TIMEWAIT [80 -> 64.101.98.203(19662)] *Apr 23 13:13:10.227: TCP0: state
was TIMEWAIT -> CLOSED [80 -> 64.101.98.203(16260)] *Apr 23 13:13:10.227: TCB 0x626DCFA0
destroyed !--- The TCP connection to the browser 64.101.93.203 is closed.
```

Informações Relacionadas

- Terminal Access Controller Access Control System (TACACS+)
- Remote Authentication Dial-In User Service (RADIUS)
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems