

Controle AAA do IOS HTTP Server

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Determine qual versão do servidor HTTP você tem](#)

[Software Cisco IOS com servidor HTTP V1](#)

[Software Cisco IOS com o servidor HTTP V1.1](#)

[Servidor HTTP V1.1 - Antes da ID de bug Cisco CSCeb82510](#)

[Servidor HTTP V1.1 - Após a ID de bug Cisco CSCeb82510](#)

[Debug](#)

[Informações Relacionadas](#)

[Introduction](#)

Este documento mostra como controlar o acesso ao servidor HTTP do Cisco IOS® com Autenticação, Autorização e Contabilidade (AAA). O controle de acesso ao servidor HTTP do Cisco IOS com AAA varia com base na versão do Cisco IOS Software.

[Prerequisites](#)

[Requirements](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

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

[Conventions](#)

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

[Determine qual versão do servidor HTTP você tem](#)

Emita o comando exec **show subsys name http** para ver qual versão do servidor HTTP você tem.

```
router1#show subsystem name http
```

```
Class          Version
http           Protocol  1.001.001
```

Este é um sistema com o servidor HTTP V1.1. O Cisco IOS Software Release 12.2(15)T e todas as versões do Cisco IOS Software 12.3 possuem HTTP V1.1.

```
router2#show subsystem name http
```

```
Class          Version
http           Protocol  1.000.001
```

Este é um sistema com o servidor HTTP V1. As versões do Cisco IOS Software anteriores a 12.2(15)T (inclui o Cisco IOS Software Release 12.2(15)JA e 12.2(15)XR) possuem HTTP V1.

Software Cisco IOS com servidor HTTP V1

Em versões do Cisco IOS Software que contêm o servidor HTTP V1, as sessões HTTP usam linhas de terminal virtual (vty). Portanto, a autenticação e a autorização HTTP são controladas com os mesmos métodos 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
```

Software Cisco IOS com o servidor HTTP V1.1

Em versões do Cisco IOS Software com o servidor HTTP V1.1, as sessões HTTP não usam vtys. Usam soquetes.

Servidor HTTP V1.1 - Antes da ID de bug Cisco CSCeb82510

Antes da integração da ID de bug da Cisco [CSCeb82510](#) (somente clientes [registrados](#)) no Cisco IOS Software Release 12.3(7.3) e 12.3(7.3)T, o servidor HTTP V1.1 precisa usar o mesmo método de autenticação e autorização 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
```

[Servidor HTTP V1.1 - Após a ID de bug Cisco CSCeb82510](#)

Com a integração do bug da Cisco ID [CSCeb82510](#) (somente clientes [registrados](#)) no Cisco IOS Software Release 12.3(7.3) e 12.3(7.3)T, o servidor HTTP pode usar métodos independentes de autenticação e autorização próprios, com novas palavras-chave no comando **ip http authentication aaa**. As novas palavras-chave 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](#)

Execute estes comandos **debug** para solucionar problemas com autenticação/autorização HTTP:

```
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 alguns exemplos de depuração:

```
*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 'HTTPhauthor' *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

- [Sistema de controle de acesso do controlador de acesso de terminal \(TACACS+\)](#)
- [Remote Authentication Dial-In User Service \(RADIUS\)](#)
- [Solicitações de Comentários \(RFCs\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)