

Contrôle AAA du serveur IOS HTTP

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Déterminez quelle version de serveur HTTP vous avez](#)

[Logiciel Cisco IOS avec serveur HTTP V1](#)

[Logiciel Cisco IOS avec serveur HTTP V1.1](#)

[Serveur HTTP V1.1 - Avant l'ID de bogue Cisco CSCeb82510](#)

[Serveur HTTP V1.1 - après l'ID de bogue Cisco CSCeb82510](#)

[Déboguer](#)

[Informations connexes](#)

[Introduction](#)

Ce document montre comment contrôler l'accès au serveur HTTP Cisco IOS® avec authentification, autorisation et comptabilité (AAA). Le contrôle d'accès au serveur HTTP Cisco IOS avec AAA varie selon la version du logiciel Cisco IOS.

[Conditions préalables](#)

[Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

[Components Used](#)

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

[Conventions](#)

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

[Déterminez quelle version de serveur HTTP vous avez](#)

Émettez la commande `exec show subsys name http` afin de voir quelle version du serveur HTTP vous avez.

```
router1#show subsys name http
```

```
Class          Version
http           Protocol  1.001.001
```

Il s'agit d'un système avec le serveur HTTP V1.1. Le logiciel Cisco IOS Version 12.2(15)T et toutes les versions du logiciel Cisco IOS Version 12.3 ont HTTP V1.1.

```
router2#show subsys name http
```

```
Class          Version
http           Protocol  1.000.001
```

Il s'agit d'un système avec le serveur HTTP V1. Les versions du logiciel Cisco IOS antérieures à 12.2(15)T (inclut les versions 12.2(15)JA et 12.2(15)XR du logiciel Cisco IOS) ont HTTP V1.

[Logiciel Cisco IOS avec serveur HTTP V1](#)

Dans les versions du logiciel Cisco IOS qui contiennent le serveur HTTP V1, les sessions HTTP utilisent des lignes de terminal virtuel (vtys). Par conséquent, l'authentification et l'autorisation HTTP sont contrôlées avec les mêmes méthodes que celles configurées pour les 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
```

[Logiciel Cisco IOS avec serveur HTTP V1.1](#)

Dans les versions du logiciel Cisco IOS avec le serveur HTTP V1.1, les sessions HTTP n'utilisent pas de vtys. Ils utilisent des prises.

[Serveur HTTP V1.1 - Avant l'ID de bogue Cisco CSCeb82510](#)

Avant l'intégration de l'ID de bogue Cisco [CSCeb82510](#) (clients [enregistrés](#) uniquement) dans les versions 12.3(7.3) et 12.3(7.3)T du logiciel Cisco IOS, le serveur HTTP V1.1 doit utiliser la même méthode d'authentification et d'autorisation que celle configurée pour la 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
```

Serveur HTTP V1.1 - après l'ID de bogue Cisco CSCeb82510

Avec l'intégration de l'ID de bogue Cisco [CSCeb82510](#) (clients [enregistrés](#) uniquement) dans les versions 12.3(7.3) et 12.3(7.3)T du logiciel Cisco IOS, le serveur HTTP peut utiliser des méthodes d'authentification et d'autorisation indépendantes, avec de nouveaux mots clés dans la commande **ip http authentication aaa**. Les nouveaux mots clés sont les suivants :

```
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
```

Voici un exemple de sortie :

```
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
```

Débuguer

Émettez ces commandes **debug** afin de résoudre les problèmes avec l'authentification/autorisation 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+.
```

Cette sortie montre quelques exemples de débogages :

```
*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 'HTTPaauthen' !--- Uses 'HTTPaauthen' 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 'HTTPaauthor' *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.
```

[Informations connexes](#)

- [Terminal Access Controller Access Control System](#)
- [RADIUS \(Remote Authentication Dial-In User Service\)](#)
- [Demandes de commentaires \(RFC\)](#)
- [Support et documentation techniques - Cisco Systems](#)