Controllo AAA del server HTTP IOS

Sommario

Introduzione

In questo documento viene spiegato come controllare l'accesso al server HTTP Cisco IOS® con autenticazione, autorizzazione e accounting (AAA). Il controllo dell'accesso al server HTTP Cisco IOS con AAA varia in base alla versione software Cisco IOS.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Determinare la versione del server HTTP disponibile

Utilizzare il comando exec **show subsys name http** per verificare la versione del server HTTP in uso.

```
router1#show subsys name http

                    Class          Version
http                Protocol     1.001.001
```

Questo è un sistema con il server HTTP V1.1. Il software Cisco IOS versione 12.2(15)T e tutte le versioni 12.3 del software Cisco IOS dispongono di HTTP V1.1.

```
router2#show subsys name http

                    Class          Version
http                Protocol     1.000.001
```

Questo è un sistema con il server HTTP V1. Il software Cisco IOS versioni precedenti alla 12.2(15)T (include il software Cisco IOS versione 12.2(15)JA e 12.2(15)XR) ha protocollo HTTP V1.

Software Cisco IOS con server HTTP V1

Nelle versioni del software Cisco IOS che contengono il server HTTP V1, le sessioni HTTP utilizzano linee terminali virtuali (vty). Pertanto, l'autenticazione e l'autorizzazione HTTP sono controllate con gli stessi metodi configurati per i vty.

```
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 con server HTTP V1.1

Nelle versioni del software Cisco IOS con il server HTTP V1.1, le sessioni HTTP non utilizzano vty. Loro usano delle prese.

Server HTTP V1.1 - Prima dell'ID bug Cisco CSCeb82510

Prima di integrare l'ID bug Cisco CSCeb82510 (solo utenti registrati) nel software Cisco IOS versione 12.3(7.3) e 12.3(7.3)T, il server HTTP V1.1 deve utilizzare lo stesso metodo di autenticazione e autorizzazione configurato per 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
```

Server HTTP V1.1 - Dopo l'ID bug Cisco CSCeb82510

Con l'integrazione dell'ID bug Cisco CSCeb82510 (solo utenti registrati) nel software Cisco IOS versione 12.3(7.3) e 12.3(7.3)T, il server HTTP può utilizzare metodi di autenticazione e autorizzazione indipendenti, con nuove parole chiave nel comando **ip http authentication aaa**. Le nuove parole chiave sono:

```
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
```

Questo è l'output di esempio:

```
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

Per risolvere i problemi di autenticazione/autorizzazione HTTP, usare i seguenti comandi **debug**:

```
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+.
```

Questo output mostra alcuni esempi di debug:

```
*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.
```

Informazioni correlate

- TACACS+ (Terminal Access Controller Access Control System)
- RADIUS (Remote Authentication Dial-In User Service)
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems