IOS HTTP 서버의 AAA 제어

목차

소개

이 문서에서는 AAA(Authentication, Authorization, and Accounting)를 사용하여 Cisco IOS® HTTP 서버에 대한 액세스를 제어하는 방법을 보여 줍니다. AAA를 사용하는 Cisco IOS HTTP 서버에 대한 액세스 제어는 Cisco IOS 소프트웨어 릴리스에 따라 달라집니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

어떤 HTTP 서버 버전을 보유하고 있는지 확인

어떤 HTTP 서버 버전을 **볼 수** 있도록 exec 명령 show subsys name http를 실행합니다.

```
router1#show subsys name http

                    Class         Version
http                Protocol    1.001.001
```

HTTP V1.1 서버가 있는 시스템입니다.Cisco IOS Software 릴리스 12.2(15)T 및 모든 Cisco IOS Software 12.3 릴리스에는 HTTP V1.1이 있습니다.

```
router2#show subsys name http

                    Class         Version
http                Protocol    1.000.001
```

HTTP V1 서버가 있는 시스템입니다.12.2(15)T 이전 버전의 Cisco IOS Software 릴리스(Cisco IOS Software 릴리스 12.2(15)JA 포함) 및 12.2(15)XR(12.2)에는 HTTP V1이 있습니다.

HTTP V1 서버가 포함된 Cisco IOS 소프트웨어

HTTP V1 서버를 포함하는 Cisco IOS Software 릴리스에서는 HTTP 세션에서 가상 터미널 라인(vtys)을 사용합니다. 따라서 HTTP 인증 및 권한 부여는 vtys에 대해 구성된 동일한 방법으로 제어됩니다.

```
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
```

HTTP V1.1 서버가 포함된 Cisco IOS 소프트웨어

HTTP V1.1 서버가 포함된 Cisco IOS Software 릴리스에서는 HTTP 세션에서 vtys를 사용하지 않습니다.소켓을 사용합니다.

HTTP V1.1 서버 - Cisco 버그 ID CSCeb82510 이전

Cisco IOS Software 릴리스 12.3(7.3) 및 12.3(7.3)T에서 Cisco 버그 ID CSCeb82510(등록된 고객만 해당)을 통합하기 전에 HTTP V1.1 서버는 콘솔에 대해 구성된 동일한 인증 및 권한 부여 방법을 사용해야 합니다.

```
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
```

HTTP V1.1 서버 - Cisco 버그 ID CSCeb82510 이후

Cisco IOS Software Releases 12.3(7.3) 및 12.3(7.3)T에서 Cisco 버그 ID CSCeb82510(등록된 고객만 해당)의 통합을 통해 HTTP 서버는 자체 인증 및 권한 부여 방법을 사용할 수 있으며 **ip authentication aaa** 명령에 새 키워드를 사용할 수 있습니다.새 키워드는 다음과 같습니다.

```
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
```

다음은 출력의 예입니다.

```
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
```

디버그

HTTP 인증/권한 부여 문제를 해결하려면 다음 debug 명령을 실행합니다.

```
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+.
```

이 출력은 몇 가지 디버깅 예를 보여 줍니다.

```
*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.*

관련 정보

- TACACS+(Terminal Access Controller Access Control System)
- 원격 인증 전화 접속 사용자 서비스(RADIUS)
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems