

IOS HTTP مداخل AAA في مكحتل

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الاصطلاحات](#)

[تحديد إصدار خادم HTTP الذي لديك](#)

[برنامج Cisco IOS مع خادم HTTP v1](#)

[برنامج Cisco IOS مع خادم HTTP v1.1](#)

[خادم HTTP V1.1 - قبل Cisco CSCeb82510](#)

[خادم HTTP V1.1 - بعد Cisco CSCeb82510](#)

[تصحيح الأخطاء](#)

[معلومات ذات صلة](#)

المقدمة

يوضح هذا المستند كيفية التحكم في الوصول إلى خادم Cisco IOS® HTTP باستخدام المصادقة والتفويض والمحاسبة (AAA). يختلف التحكم في الوصول إلى خادم Cisco IOS HTTP مع AAA بناء على إصدار برنامج Cisco IOS Software.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

تحديد إصدار خادم HTTP الذي لديك

قم بإصدار أمر EXEC show subsys name http لترى أي إصدار من خادم HTTP لديك.

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

```
Class      Version
http      Protocol  1.001.001
```

هذا نظام مزود بخادم HTTP V1.1. برنامج IOS الإصدار T(15)12.2 من Cisco وجميع إصدارات برنامج Cisco IOS الإصدار 12.3 لها HTTP v1.1.

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

```
Class      Version
http      Protocol  1.000.001
```

هذا نظام مزود بخادم HTTP V1. تتضمن الإصدارات الأقدم من T(15)12.2 من Cisco IOS Software، الإصدار JA(15)12.2 و HTTP V1(15)12.2 XR.

[برنامج Cisco IOS مع خادم HTTP v1](#)

في إصدارات برنامج Cisco IOS التي تحتوي على خادم HTTP v1، تستخدم جلسات HTTP خطوط المحطة الطرفية الظاهرة (vty). لذلك، يتم التحكم في مصادقة HTTP والتفويض باستخدام نفس الطرق التي تم تكوينها لـ 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
  login authentication VTYSandHTTP authorization exec ---!
  VTYSandHTTP
```

[برنامج Cisco IOS مع خادم HTTP v1.1](#)

في إصدارات برنامج Cisco IOS مع خادم HTTP v1.1، لا تستخدم جلسات vty HTTP. إنهم يستخدمون المقابس.

[خادم HTTP V1.1 - قبل Cisco CSCeb82510](#)

قبل تكامل معرف تصحيح الأخطاء من Cisco CSCeb82510 (العملاء المسجلون فقط) في الإصدار 12.3(7.3) و T(7.3)12.3، يجب أن يستخدم خادم HTTP V1.1 نفس طريقة المصادقة والتفويض التي تم تكوينها لوحدة التحكم.

```
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
```

خادم V1.1 HTTP - بعد Cisco CSCeb82510

مع دمج معرف تصحيح الأخطاء من Cisco CSCeb82510 (العملاء المسجلون فقط) في الإصدار 12.3(7.3) و T(7.3)12.3 من برنامج Cisco IOS، يمكن لخادم HTTP استخدام طرق المصادقة والتفويض المستقلة الخاصة به، مع الكلمات الأساسية الجديدة في الأمر `ip http authentication aaa`. الكلمات الأساسية الجديدة هي:

```
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
```

هذا مثال للمخرجات:

```
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
```

تصحيح الأخطاء

قم بإصدار أوامر تصحيح الأخطاء هذه لاستكشاف أخطاء مصادقة/تفويض HTTP وإصلاحها:

```
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
يوضح هذا الإخراج بعض الأمثلة على تصحيح الأخطاء:
```

```
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*

معلومات ذات صلة

- نظام مراقبة الدخول إلى وحدة تحكم الوصول إلى المحطة الطرفية (+TACACS)
- خدمة مصادقة طلب اتصال المستخدم البعيد (RADIUS)
- طلبات التعليقات (RFCs)
- الدعم التقني والمستندات - Cisco Systems

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مه تلبل
Cisco يخلت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إأمئاد ةوچرلاب ي صؤت وتامچرتل هذه ةقد نع اهتيل وئسم Cisco
Systems (رفوتم طبارل) ي لصلأل يزي لچن إل دن تسمل