AAA Control of the IOS HTTP Server

Contents

Introduction
Prerequisites
   Requirements
   Components Used
   Conventions
Determine Which HTTP Server Version You Have
Cisco IOS Software with the HTTP V1 Server
Cisco IOS Software with the HTTP V1.1 Server
   HTTP V1.1 Server – Before Cisco Bug ID CSCeb82510
   HTTP V1.1 Server – After Cisco Bug ID CSCeb82510
Debug
Related Information

Introduction

This document shows how to control access to the Cisco IOS® HTTP server with Authentication, Authorization, and Accounting (AAA). The control of access to the Cisco IOS HTTP server with AAA varies based on the Cisco IOS Software release.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Determine Which HTTP Server Version You Have

Issue the exec command show subsys name http in order to see what version of the HTTP server you have.

```
router1#show subsys name http
http                  Class     Version
                        Protocol   1.001.001
```

This is a system with the HTTP V1.1 server. Cisco IOS Software Release 12.2(15)T and all Cisco IOS Software 12.3 releases have HTTP V1.1.

```
router2#show subsys name http
```
<table>
<thead>
<tr>
<th>Class</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>http</td>
<td>1.000.001</td>
</tr>
</tbody>
</table>

This is a system with the HTTP V1 server. Cisco IOS Software releases earlier than 12.2(15)T (includes Cisco IOS Software Releases 12.2(15)JA and 12.2(15)XR) have HTTP V1.

## Cisco IOS Software with the HTTP V1 Server

In releases of Cisco IOS Software that contain the HTTP V1 server, HTTP sessions use virtual terminal lines (vtys). Therefore, HTTP authentication and authorization is controlled with the same methods that are configured for the 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
```

## Cisco IOS Software with the HTTP V1.1 Server

In releases of Cisco IOS Software with the HTTP V1.1 server, the HTTP sessions do not use vtys. They use sockets.

### HTTP V1.1 Server – Before Cisco Bug ID CSCeb82510

Before the integration of Cisco bug ID CSCeb82510 (registered customers only) in Cisco IOS Software Releases 12.3(7.3) and 12.3(7.3)T, the HTTP V1.1 server has to use the same authentication and authorization method that is configured for the 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
```

### HTTP V1.1 Server – After Cisco Bug ID CSCeb82510

With the integration of Cisco bug ID CSCeb82510 (registered customers only) in Cisco IOS Software Releases 12.3(7.3) and 12.3(7.3)T, the HTTP server can use independent authentication and authorization methods of its own, with new keywords in the `ip http authentication aaa` command. The new keywords are:

```
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

This is example output:

ip http server
!
new-model
authentication login HTTPonly radius local
authorization exec HTTPonly radius local
!
ip http authentication aaa
ip http authentication aaa exec-authorization HTTPonly
ip http authentication aaa login-authentication HTTPonly

**Debug**

Issue these **debug** commands in order to troubleshoot problems with HTTP authentication/authorization:

```
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+.
```

This output shows some example debugs:

```
*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: 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
```
Uses 'HTTPauthen' as the login authentication method.

Sent an Access-Request to the RADIUS server at 10.1.2.3 using the username of "cisco".

Authentication has failed due to no response from the RADIUS server.

The TCP connection to the browser 64.101.93.203 is closed.
Related Information

- Terminal Access Controller Access Control System (TACACS+)
- Remote Authentication Dial–In User Service (RADIUS)
- Requests for Comments (RFCs)
- Technical Support & Documentation – Cisco Systems