分析ASA的AAA裝置管理行為

目錄

簡介

本文檔介紹使用AAA伺服器配置ASA進行身份驗證和授權時的裝置管理行為。本文檔介紹使用思科身份服務引擎(ISE)作為AAA伺服器，Active Directory作為外部身份庫。TACACS+是正在使用的AAA通訊協定。

作者：Dinesh Moudgil和Poonam Garg，思科HTTS工程師

必要條件

需求

思科建議您瞭解以下主題：

- ASA CLI和ASDM的基本知識
- ASA和AAA伺服器之間的連線
- 思科ISE上的AAA配置用於身份驗證和授權

採用元件

- 運行9.9(2)的ASAv
- 思科身分識別服務引擎2.6

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

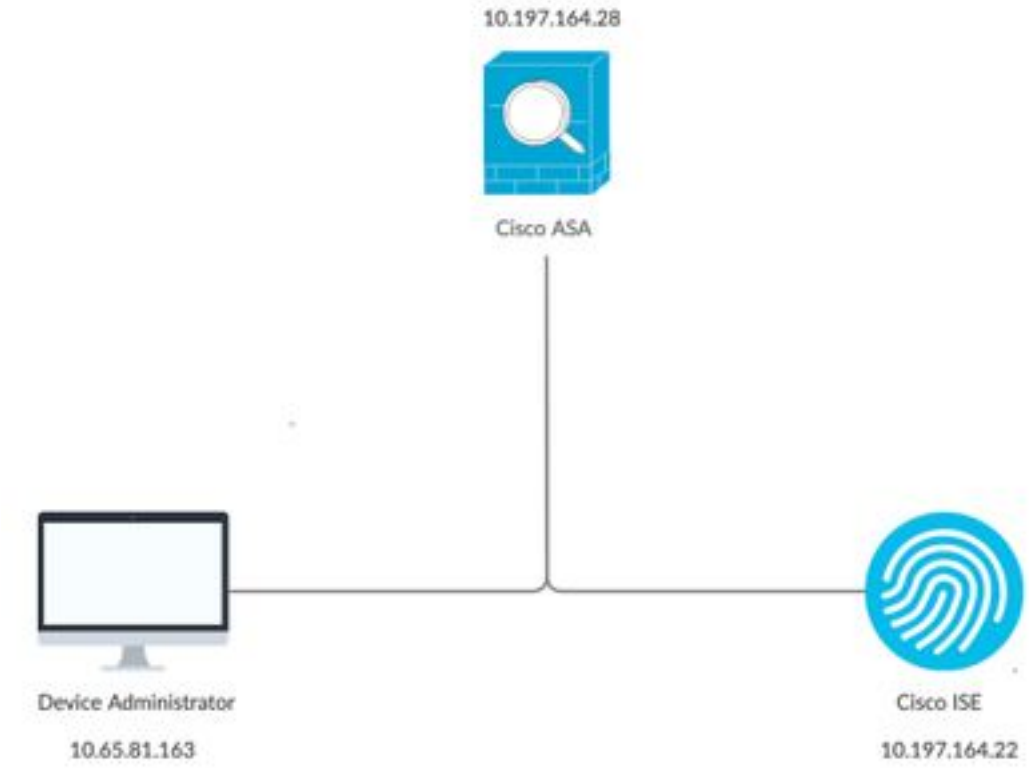
Cisco ASA通過使用本地使用者資料庫、RADIUS伺服器或TACACS+伺服器來支援管理會話的身份驗證。管理員可以通過以下方式連線到Cisco ASA:

- Telnet
- 安全殼層 (SSH)
- 串列控制檯連線
- Cisco ASA裝置管理員(ASDM)

如果通過Telnet或SSH連線，使用者可以在出現使用者錯誤的情況下重試身份驗證三次。第三次之後，將關閉身份驗證會話和與Cisco ASA的連線。

開始配置之前，必須決定要使用哪個使用者資料庫（本地或外部AAA伺服器）。 如果您使用外部AAA伺服器（如本文檔中所配置），請按照以下部分所述配置AAA伺服器組和主機。當訪問Cisco ASA進行管理時，您可以使用aaa authentication和aaa authorization命令分別要求身份驗證和授權驗證。

網路圖表



設定

這是用於本文檔中所有示例的資訊。

a)ASA配置：

```
aaa-server ISE protocol tacacs+
aaa-server ISE (internet) host 10.197.164.22
key *****
```

b)AAA配置：

在AAA伺服器上根據身份儲存序列執行身份驗證，該序列由AD和本地資料庫組成

案例1:通過AAA伺服器配置的ASA身份驗證

在ASA上：

```
aaa authentication ssh console ISE LOCAL
```

在AAA伺服器上：

授權結果：

a)殼配置檔案

預設許可權：1
最大許可權：15

b)命令集
全部允許

管理員行為：

```
Connection to 10.197.164.28 closed.
DMOUDGIL-M-N1D9:~ dmoudgil$
DMOUDGIL-M-N1D9:~ dmoudgil$
DMOUDGIL-M-N1D9:~ dmoudgil$ ssh ASA_priv1@10.197.164.28
ASA_priv1@10.197.164.28's password:
User ASA_priv1 logged in to ciscoasa
Logins over the last 9 days: 11. Last login: 12:59:51 IST May 7 2020 from 10.65.81.163
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
ciscoasa> enable
Password:
ciscoasa#
ciscoasa# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
```

ASA日誌：

```
May 07 2020 12:57:26: %ASA-6-113008: AAA transaction status ACCEPT : user = ASA_priv1
```

```
May 07 2020 12:57:26: %ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163,
Uname: ASA_priv1
May 07 2020 12:57:26: %ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163,
Uname: ASA_priv1
May 07 2020 12:57:26: %ASA-6-605005: Login permitted from 10.65.81.163/56048 to
internet:10.197.164.28/ssh for user "ASA_priv1"
May 07 2020 12:57:30: %ASA-7-111009: User 'enable_15' executed cmd: show logging
May 07 2020 12:57:40: %ASA-5-502103: User priv level changed: Uname: enable_15 From: 1 To: 15
May 07 2020 12:57:40: %ASA-5-111008: User 'ASA_priv1' executed the 'enable' command.
```

意見：

1.通過AAA伺服器執行SSH會話的身份驗證
2.無論授權結果中在AAA伺服器上配置的許可權如何，授權均在本地完成
3.使用者通過AAA伺服器進行身份驗證後，當使用者輸入關鍵字「enable」（預設情況下未設定密碼）或輸入啟用密碼（如果已配置）時，使用的相應使用者名稱是enable_15

```
May 07 2020 12:57:40: %ASA-5-502103: User priv level changed: Uname: enable_15 From: 1 To: 15
```

4.啟用口令的預設許可權為15，除非您使用特定許可權定義啟用口令。例如：

```
enable password C!sco123 level 9
```

5.如果使用具有不同許可權的enable，則ASA上出現的相應使用者名稱是enable_x（其中x是許可權）

```
May 07 2020 13:20:49: %ASA-5-502103: User priv level changed: Uname: enable_8 From: 1 To: 8
```

案例2:通過AAA伺服器配置的ASA身份驗證和exec授權

在ASA上：

```
aaa authentication ssh console ISE LOCAL
aaa authorization exec authentication-server
```

在AAA伺服器上：

授權結果：

a)殼配置檔案

預設許可權：1
最大許可權：15

b)命令集
全部允許

管理員行為：

```
DMOUDGIL-M-N1D9:~ dmoudgil$ ssh ASA_priv1@10.197.164.28
ASA_priv1@10.197.164.28's password:
User ASA_priv1 logged in to ciscoasa
Logins over the last 1 days: 8. Last login: 14:12:52 IST May 7 2020 from 10.65.81.163
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
ciscoasa> show curpriv
Username : ASA_priv1
Current privilege level : 1
Current Mode/s : P_UNPR
ciscoasa> enable
Password:
ciscoasa# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
```

ASA日誌：

```
May 07 2020 13:59:54: %ASA-6-113004: AAA user authentication Successful : server = 10.197.164.22
: user = ASA_priv1
May 07 2020 13:59:54: %ASA-6-302013: Built outbound TCP connection 75 for
internet:10.197.164.22/49 (10.197.164.22/49) to identity:10.197.164.28/49068
(10.197.164.28/49068)
May 07 2020 13:59:54: %ASA-6-113004: AAA user authorization Successful : server = 10.197.164.22
: user = ASA_priv1
May 07 2020 13:59:54: %ASA-6-113008: AAA transaction status ACCEPT : user = ASA_priv1
May 07 2020 13:59:54: %ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163,
Uname: ASA_priv1
May 07 2020 13:59:54: %ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163,
Uname: ASA_priv1
May 07 2020 13:59:54: %ASA-6-605005: Login permitted from 10.65.81.163/57671 to
internet:10.197.164.28/ssh for user "ASA_priv1"
May 07 2020 13:59:59: %ASA-5-502103: User priv level changed: Uname: enable_15 From: 1 To: 15
May 07 2020 13:59:59: %ASA-5-111008: User 'ASA_priv1' executed the 'enable' command.
```

意見：

1.身份驗證和exec授權通過AAA伺服器執行
2. Exec授權控制為身份驗證配置的所有控制檯連線（ssh、telnet和啟用）請求的使用者許可權

> **附註**：這不包括與ASA的串列連線

3. AAA伺服器的配置方式是提供預設許可權1，最大許可權15作為授權的結果
4.當使用者通過AAA伺服器上配置的TACACS+憑證登入到ASA時，AAA伺服器最初授予該使用者許可權1
5.使用者輸入關鍵字「enable」後，再次按enter（如果未配置啟用密碼）或輸入enable password（如果已配置），他們就會進入特權模式，此時許可權更改為15

案例3:通過AAA伺服器配置ASA身份驗證、exec授權和命令授權

在ASA上：

```
aaa authentication ssh console ISE LOCAL
aaa authorization exec authentication-server
aaa authorization command ISE LOCAL
```

在AAA伺服器上：

授權結果：

a)殼配置檔案

預設許可權：1
最大許可權：15

b)命令集
全部允許

管理員行為：

```
DMOUDGIL-M-N1D9:~ dmoudgil$ ssh ASA_priv1@10.197.164.28
ASA_priv1@10.197.164.28's password:
User ASA_priv1 logged in to ciscoasa
Logins over the last 1 days: 7. Last login: 17:12:23 IST May 9 2020 from 10.65.81.163
Failed logins since the last login: 0. Last failed login: 17:12:21 IST May 9 2020 from
10.65.81.163
Type help or '?' for a list of available commands.
ciscoasa> show curpriv
Username : ASA_priv1
Current privilege level : 1
Current Mode/s : P_UNPR
ciscoasa> enable
Password:
ciscoasa# show curpriv
Command authorization failed
```

ASA日誌：

```
May 09 2020 17:13:05: %ASA-6-113004: AAA user authentication Successful : server = 10.197.164.22
: user = ASA_priv1
May 09 2020 17:13:05: %ASA-6-302013: Built outbound TCP connection 170 for
internet:10.197.164.22/49 (10.197.164.22/49) to identity:10.197.164.28/21275
(10.197.164.28/21275)
May 09 2020 17:13:05: %ASA-6-302014: Teardown TCP connection 169 for internet:10.197.164.22/49
to identity:10.197.164.28/30256 duration 0:00:00 bytes 67 TCP Reset-I from internet
May 09 2020 17:13:05: %ASA-6-113004: AAA user authorization Successful : server = 10.197.164.22
: user = ASA_priv1
May 09 2020 17:13:05: %ASA-6-113008: AAA transaction status ACCEPT : user = ASA_priv1
May 09 2020 17:13:05: %ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163,
Uname: ASA_priv1
May 09 2020 17:13:05: %ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163,
Uname: ASA_priv1
May 09 2020 17:13:05: %ASA-6-605005: Login permitted from 10.65.81.163/49218 to
internet:10.197.164.28/ssh for user "ASA_priv1"
May 09 2020 17:13:05: %ASA-6-302014: Teardown TCP connection 170 for internet:10.197.164.22/49
to identity:10.197.164.28/21275 duration 0:00:00 bytes 61 TCP Reset-I from internet
May 09 2020 17:13:05: %ASA-7-609002: Teardown local-host internet:10.197.164.22 duration 0:00:00
May 09 2020 17:13:07: %ASA-7-609001: Built local-host internet:10.197.164.22
May 09 2020 17:13:07: %ASA-6-302013: Built outbound TCP connection 171 for
```

```
internet:10.197.164.22/49 (10.197.164.22/49) to identity:10.197.164.28/53081
(10.197.164.28/53081)
May 09 2020 17:13:07: %ASA-7-111009: User 'ASA_priv1' executed cmd: show curpriv
May 09 2020 17:13:08: %ASA-6-302014: Teardown TCP connection 171 for internet:10.197.164.22/49
to identity:10.197.164.28/53081 duration 0:00:00 bytes 82 TCP Reset-I from internet
May 09 2020 17:13:08: %ASA-7-609002: Teardown local-host internet:10.197.164.22 duration 0:00:00
May 09 2020 17:13:10: %ASA-5-502103: User priv level changed: Uname: enable_15 From: 1 To: 15
May 09 2020 17:13:10: %ASA-5-111008: User 'ASA_priv1' executed the 'enable' command.
May 09 2020 17:13:12: %ASA-7-609001: Built local-host internet:10.197.164.22
May 09 2020 17:13:12: %ASA-6-302013: Built outbound TCP connection 172 for
internet:10.197.164.22/49 (10.197.164.22/49) to identity:10.197.164.28/46803
(10.197.164.28/46803)
May 09 2020 17:13:12: %ASA-6-113016: AAA credentials rejected : reason = Unspecified : server =
10.197.164.22 : user = ***** : user IP = 10.65.81.163
May 09 2020 17:13:12: %ASA-6-302014: Teardown TCP connection 172 for internet:10.197.164.22/49
to identity:10.197.164.28/46803 duration 0:00:00 bytes 82 TCP Reset-I from internet
May 09 2020 17:13:12: %ASA-7-609002: Teardown local-host internet:10.197.164.22 duration 0:00:00
May 09 2020 17:13:20: %ASA-7-609001: Built local-host internet:10.197.164.22
May 09 2020 17:13:20: %ASA-6-302013: Built outbound TCP connection 173 for
internet:10.197.164.22/49 (10.197.164.22/49) to identity:10.197.164.28/6934 (10.197.164.28/6934)
May 09 2020 17:13:20: %ASA-6-113016: AAA credentials rejected : reason = Unspecified : server =
10.197.164.22 : user = ***** : user IP = 10.65.81.163
```

意見：

1.身份驗證和exec授權通過AAA伺服器執行
2. Exec授權控制為身份驗證配置的所有控制檯連線（ssh、telnet和啟用）請求的使用者許可權
3.命令授權由AAA伺服器使用命令「aaa authorization command ISE LOCAL」執行

附註：這不包括與ASA的串列連線

4.當使用者通過AAA伺服器上配置的TACACS+憑證登入到ASA時，AAA伺服器最初授予該使用者許可權1
5.使用者輸入關鍵字「enable」後，再次按enter鍵（如果未配置啟用密碼）或輸入啟用密碼（如果已配置），就會進入特權模式，此時許可權將更改為15
6.命令授權使用此配置失敗，因為AAA伺服器顯示由使用者名稱「enable_15」發出命令，而不是真正登入經過身份驗證的使用者。
7.在現有會話上執行的任何命令也會因命令授權失敗而失敗
8.要解決此問題，請使用隨機密碼在AAA伺服器上或AD和ASA（用於本地回退）上建立名為「enable_15」的使用者

在AAA伺服器或AD上配置使用者後，將觀察以下行為：

i.對於初始身份驗證，AAA伺服器驗證登入使用者的實際使用者名稱
二。一旦輸入啟用密碼，就會在ASA上進行本地驗證，因為啟用身份驗證不會指向此配置中的AAA伺服器
三。啟用密碼後，所有命令都使用使用者名稱「enable_15」執行，而AAA允許這些命令，因為在AAA伺服器或AD上存在該使用者名稱

配置使用者「enable_15」後，管理員即可從ASA上的許可權模式轉換到配置模式。

管理員行為：

```
DMOUDGIL-M-N1D9:~ dmoudgil$ ssh ASA_priv1@10.197.164.28
ASA_priv1@10.197.164.28's password:
User ASA_priv1 logged in to ciscoasa
Logins over the last 1 days: 2. Last login: 16:50:42 IST May 9 2020 from 10.65.81.163
Failed logins since the last login: 5. Last failed login: 16:53:55 IST May 9 2020 from
10.65.81.163
Type help or '?' for a list of available commands.
ciscoasa> show curpriv
Username : ASA_priv1
Current privilege level : 1
Current Mode/s : P_UNPR
ciscoasa> enable
Password:
ciscoasa# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
ciscoasa# configure terminal
```

ASA日誌：

```
May 09 2020 17:05:29: %ASA-6-113004: AAA user authentication Successful : server = 10.197.164.22
: user = ASA_priv1
May 09 2020 17:05:29: %ASA-6-302013: Built outbound TCP connection 113 for
internet:10.197.164.22/49 (10.197.164.22/49) to identity:10.197.164.28/31109
(10.197.164.28/31109)
May 09 2020 17:05:29: %ASA-6-113004: AAA user authorization Successful : server = 10.197.164.22
: user = ASA_priv1
May 09 2020 17:05:29: %ASA-6-113008: AAA transaction status ACCEPT : user = ASA_priv1
May 09 2020 17:05:29: %ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163,
Uname: ASA_priv1
May 09 2020 17:05:29: %ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163,
Uname: ASA_priv1
May 09 2020 17:05:29: %ASA-6-302014: Teardown TCP connection 112 for internet:10.197.164.22/49
to identity:10.197.164.28/7703 duration 0:00:00 bytes 67 TCP Reset-I from internet
May 09 2020 17:05:29: %ASA-6-605005: Login permitted from 10.65.81.163/65524 to
internet:10.197.164.28/ssh for user "ASA_priv1"
May 09 2020 17:05:29: %ASA-6-302014: Teardown TCP connection 113 for internet:10.197.164.22/49
to identity:10.197.164.28/31109 duration 0:00:00 bytes 61 TCP Reset-I from internet
May 09 2020 17:05:29: %ASA-7-609002: Teardown local-host internet:10.197.164.22 duration 0:00:00
May 09 2020 17:05:32: %ASA-7-609001: Built local-host internet:10.197.164.22
May 09 2020 17:05:32: %ASA-6-302013: Built outbound TCP connection 114 for
internet:10.197.164.22/49 (10.197.164.22/49) to identity:10.197.164.28/64339
(10.197.164.28/64339)
May 09 2020 17:05:32: %ASA-7-111009: User 'ASA_priv1' executed cmd: show curpriv
May 09 2020 17:05:32: %ASA-6-302014: Teardown TCP connection 114 for internet:10.197.164.22/49
to identity:10.197.164.28/64339 duration 0:00:00 bytes 82 TCP Reset-I from internet
May 09 2020 17:05:32: %ASA-7-609002: Teardown local-host internet:10.197.164.22 duration 0:00:00
May 09 2020 17:05:35: %ASA-5-502103: User priv level changed: Uname: enable_15 From: 1 To: 15
May 09 2020 17:05:35: %ASA-5-111008: User 'ASA_priv1' executed the 'enable' command.
May 09 2020 17:05:37: %ASA-7-609001: Built local-host internet:10.197.164.22
May 09 2020 17:05:37: %ASA-6-302013: Built outbound TCP connection 115 for
internet:10.197.164.22/49 (10.197.164.22/49) to identity:10.197.164.28/4236 (10.197.164.28/4236)
May 09 2020 17:05:37: %ASA-7-111009: User 'enable_15' executed cmd: show curpriv
May 09 2020 17:05:37: %ASA-6-302014: Teardown TCP connection 115 for internet:10.197.164.22/49
to identity:10.197.164.28/4236 duration 0:00:00 bytes 82 TCP Reset-I from internet
May 09 2020 17:05:37: %ASA-7-609002: Teardown local-host internet:10.197.164.22 duration 0:00:00
May 09 2020 17:05:44: %ASA-7-609001: Built local-host internet:10.197.164.22
May 09 2020 17:05:44: %ASA-6-302013: Built outbound TCP connection 116 for
internet:10.197.164.22/49 (10.197.164.22/49) to identity:10.197.164.28/27478
(10.197.164.28/27478)
May 09 2020 17:05:44: %ASA-5-111007: Begin configuration: 10.65.81.163 reading from terminal
```

```
May 09 2020 17:05:44: %ASA-5-111008: User 'enable_15' executed the 'configure terminal' command.
May 09 2020 17:05:44: %ASA-5-111010: User 'enable_15', running 'CLI' from IP 10.65.81.163,
executed 'configure terminal'
```

附註：如果在ASA上配置了通過TACACS的命令授權，則在AAA伺服器無法訪問時，必須將「本地」作為回退。
這是因為即使沒有為串列控制檯配置身份驗證，命令授權也會應用於所有ASA會話（串列控制檯、ssh、telnet）。如果AAA伺服器無法訪問，並且本地資料庫中不存在使用者「enable_15」，管理員會收到以下錯誤：

回退授權。使用者名稱「enable_15」不在LOCAL資料庫中
命令授權失敗

ASA日誌：

```
%ASA-4-409023: Attempting AAA Fallback method LOCAL for Authentication request for user cisco :
Auth-server group ISE unreachable
%ASA-6-113012: AAA user authentication Successful : local database : user = cisco
%ASA-4-409023: Attempting AAA Fallback method LOCAL for Authentication request for user cisco :
Auth-server group ISE unreachable
%ASA-6-113004: AAA user authorization Successful : server = LOCAL : user = cisco
%ASA-6-113008: AAA transaction status ACCEPT : user = cisco
%ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163, Uname: cisco
%ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163, Uname: cisco
%ASA-6-605005: Login permitted from 10.65.81.163/65416 to internet:10.197.164.28/ssh for user
"cisco"
%ASA-5-502103: User priv level changed: Uname: enable_15 From: 1 To: 15
%ASA-5-111008: User 'cisco' executed the 'enable' command.
%ASA-4-409023: Attempting AAA Fallback method LOCAL for Authorization request for user enable_15
: Auth-server group ISE unreachable
%ASA-5-111007: Begin configuration: 10.65.81.163 reading from terminal
%ASA-5-111008: User 'enable_15' executed the 'configure terminal' command.
%ASA-5-111010: User 'enable_15', running 'CLI' from IP 10.65.81.163, executed 'configure
terminal'
%ASA-4-409023: Attempting AAA Fallback method LOCAL for Authorization request for user enable_15
: Auth-server group ISE unreachable
```

附註：使用上述配置，命令授權將起作用，但命令記賬仍將顯示使用者名稱「enable_15」，而不是登入使用者的實際使用者名稱。管理員很難確定哪個使用者在ASA上執行了哪個特定命令。

要解決與「enable_15」使用者相關的記帳問題：

1.在ASA上的exec授權命令中使用**關鍵字**「auto-enable」
2.在分配給通過身份驗證的使用者的TACACS外殼配置檔案中將預設和最大許可權設定為15

案例4:ASA身份驗證、使用「auto-enable」的exec授權和通過AAA伺服器配置的命令授權

在ASA上：

```
aaa authentication ssh console ISE LOCAL
aaa authorization exec authentication-server auto-enable
aaa authorization command ISE LOCAL
```

在AAA伺服器上：

授權結果：

a)殼配置檔案

預設許可權：15
最大許可權：15

b)命令集
全部允許

管理員行為：

```
DMOUDGIL-M-N1D9:~ dmoudgil$ ssh ASA_priv1@10.197.164.28
ASA_priv1@10.197.164.28's password:
User ASA_priv1 logged in to ciscoasa
Logins over the last 1 days: 8. Last login: 17:13:05 IST May 9 2020 from 10.65.81.163
Failed logins since the last login: 0. Last failed login: 17:12:21 IST May 9 2020 from
10.65.81.163
Type help or '?' for a list of available commands.
ciscoasa# show curpriv
Username : ASA_priv1
Current privilege level : 15
Current Mode/s : P_PRIV
ciscoasa# configure terminal
ciscoasa(config)#
```

ASA日誌：

```
May 09 2020 17:40:04: %ASA-6-113004: AAA user authentication Successful : server = 10.197.164.22
: user = ASA_priv1
May 09 2020 17:40:04: %ASA-6-302013: Built outbound TCP connection 298 for
internet:10.197.164.22/49 (10.197.164.22/49) to identity:10.197.164.28/57617
(10.197.164.28/57617)
May 09 2020 17:40:04: %ASA-6-113004: AAA user authorization Successful : server = 10.197.164.22
: user = ASA_priv1
May 09 2020 17:40:04: %ASA-6-113008: AAA transaction status ACCEPT : user = ASA_priv1
May 09 2020 17:40:04: %ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163,
Uname: ASA_priv1
May 09 2020 17:40:04: %ASA-6-611101: User authentication succeeded: IP address: 10.65.81.163,
Uname: ASA_priv1
May 09 2020 17:40:04: %ASA-6-605005: Login permitted from 10.65.81.163/49598 to
internet:10.197.164.28/ssh for user "ASA_priv1"
May 09 2020 17:40:04: %ASA-6-302014: Teardown TCP connection 297 for internet:10.197.164.22/49
to identity:10.197.164.28/6083 duration 0:00:00 bytes 67 TCP Reset-I from internet
May 09 2020 17:40:04: %ASA-7-609001: Built local-host internet:139.59.219.101
May 09 2020 17:40:04: %ASA-6-302015: Built outbound UDP connection 299 for
internet:139.59.219.101/123 (139.59.219.101/123) to mgmt-gateway:192.168.100.4/123
(10.197.164.28/195)
May 09 2020 17:40:04: %ASA-6-302014: Teardown TCP connection 298 for internet:10.197.164.22/49
to identity:10.197.164.28/57617 duration 0:00:00 bytes 61 TCP Reset-I from internet
May 09 2020 17:40:04: %ASA-7-609002: Teardown local-host internet:10.197.164.22 duration 0:00:00
May 09 2020 17:40:09: %ASA-7-609001: Built local-host internet:10.197.164.22
May 09 2020 17:40:09: %ASA-6-302013: Built outbound TCP connection 300 for
internet:10.197.164.22/49 (10.197.164.22/49) to identity:10.197.164.28/4799 (10.197.164.28/4799)
```

```
May 09 2020 17:40:09: %ASA-7-111009: User 'ASA_priv1' executed cmd: show curpriv
May 09 2020 17:40:09: %ASA-6-302014: Teardown TCP connection 300 for internet:10.197.164.22/49
to identity:10.197.164.28/4799 duration 0:00:00 bytes 82 TCP Reset-I from internet
May 09 2020 17:40:09: %ASA-7-609002: Teardown local-host internet:10.197.164.22 duration 0:00:00
May 09 2020 17:40:14: %ASA-5-111007: Begin configuration: 10.65.81.163 reading from terminal
May 09 2020 17:40:14: %ASA-5-111008: User 'ASA_priv1' executed the 'configure terminal' command.
May 09 2020 17:40:14: %ASA-5-111010: User 'ASA_priv1', running 'CLI' from IP 10.65.81.163,
executed 'configure terminal'
```

意見：

1.身份驗證和exec授權通過AAA伺服器執行
2. Exec授權控制為身份驗證配置的所有控制檯連線（ssh、telnet和啟用）請求的使用者許可權

附註：這不包括與ASA的串列連線

3.命令授權由AAA伺服器使用命令「aaa authorization command ISE LOCAL」執行
4.當使用者通過AAA伺服器上配置的TACACS+憑據登入到ASA時，使用者將獲得AAA伺服器的許可權15，從而登入到許可權模式
5.使用上述配置時，不需要使用者輸入啟用密碼，也不需要在ASA或AAA伺服器上配置使用者「enable_15」。
6. AAA伺服器現在將報告來自登入使用者的實際使用者名稱的命令授權請求

相關資訊

以下是與AAA Device Administration for ASA相關的一些參考文檔：

https://community.cisco.com/t5/security-documents/cisco-ise-device-administration-prescriptive-deployment-guide/ta-p/3738365#toc-hId--1046199281

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200207-ISE-2-0-ASA-CLI-TACACS-Authentication.pdf