ASA에 대한 AAA 디바이스 관리 동작 분석

목차

소개

이 문서에서는 ASA가 AAA 서버를 사용하여 인증 및 권한 부여를 위해 구성된 경우 디바이스 관리 동작에 대해 설명합니다.이 문서에서는 Active Directory를 외부 ID 저장소로 사용하는 AAA 서버로 Cisco ISE(Identity Service Engine)를 사용하는 방법을 보여줍니다.TACACS+는 사용 중인 AAA 프로토콜입니다.

기고자: Dinesh Moudgil 및 Poonam Garg, Cisco HTTS 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA의 CLI 및 ASDM에 대한 기본 지식
- ASA와 AAA 서버 간 연결
- 인증 및 권한 부여를 위한 Cisco ISE의 AAA 구성

사용되는 구성 요소

.

- 9.9(2)를 실행하는 ASAv

- Cisco Identity Service Engine 2.6

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

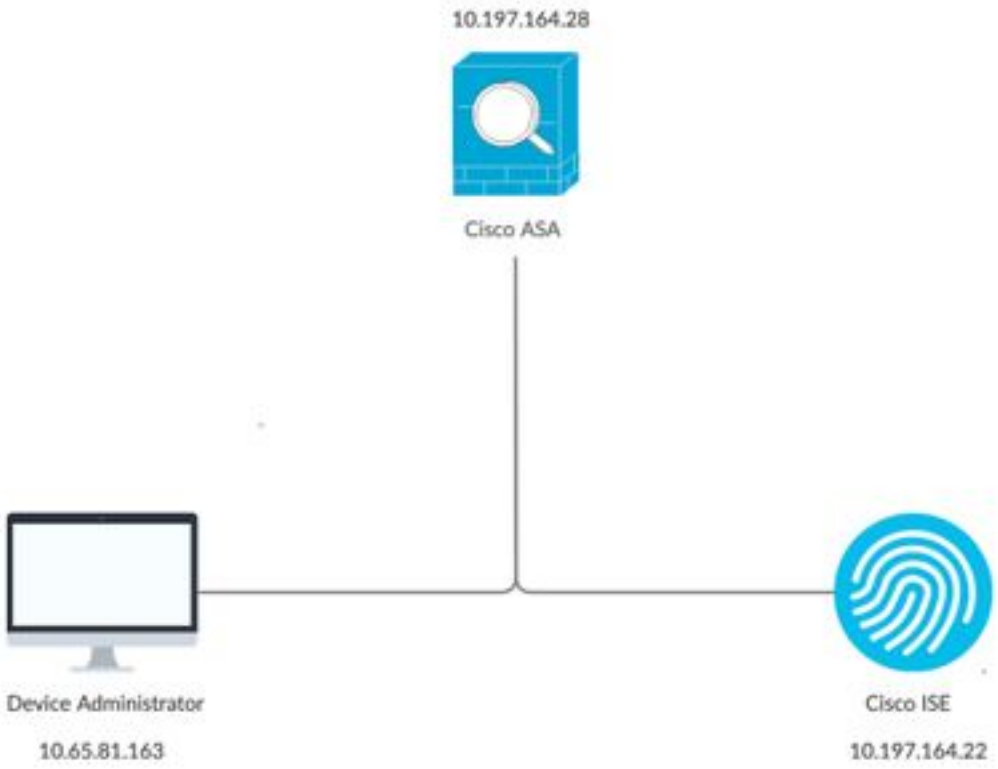
Cisco ASA는 로컬 사용자 데이터베이스, RADIUS 서버 또는 TACACS+ 서버를 사용하여 관리 세션 인증을 지원합니다.관리자는 다음을 통해 Cisco ASA에 연결할 수 있습니다.

- Telnet
- SSH(Secure Shell)
- 직렬 콘솔 연결
- Cisco ASA Device Manager(ASDM)

텔넷 또는 SSH를 통해 연결하는 경우 사용자 오류 발생 시 사용자는 3회 인증을 재시도할 수 있습니다.세 번째 시간이 지나면 Cisco ASA에 대한 인증 세션 및 연결이 닫힙니다.

컨피그레이션을 시작하기 전에 사용할 사용자 데이터베이스(로컬 또는 외부 AAA 서버)를 결정해야 합니다. 이 문서에 구성된 대로 외부 AAA 서버를 사용하는 경우 아래 섹션에서 설명한 대로 AAA 서버 그룹 및 호스트를 구성합니다.관리를 위해 Cisco ASA에 액세스할 때 각각 인증 및 권한 부여 확인을 요구하려면 aaa authentication 및 aaa authorization 명령을 사용할 수 있습니다.

네트워크 다이어그램



구성

이 문서의 모든 예제에 사용되는 정보입니다.

a) ASA 구성:

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

b) AAA 컨피그레이션:

AD 및 로컬 데이터베이스로 구성된 ID 저장소 시퀀스에 대해 AAA 서버에 대한 인증이 수행됩니다

사례 1:AAA 서버를 통해 구성된 ASA 인증

ASA의 경우:

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

AAA 서버:

인증 결과:

a) 셸 프로파일

기본 권한:1
최대 권한:15

b) 명령 집합
모두 허용

관리 동작:

```
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 로그:

```
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.
```

관찰:

1. SSH 세션에 대한 인증은 AAA 서버를 통해 수행됩니다.
2. 권한 부여는 권한 부여 결과에서 AAA 서버에 구성된 권한에 관계없이 로컬로 수행됩니다.
3. AAA 서버를 통해 사용자를 인증한 후 사용자가 "enable"(기본적으로 비밀번호가 설정되지 않음) 키워드를 입력하거나 enable 비밀번호(구성된 경우)를 입력하면 해당 사용자 이름이 **enable_15입니다**

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

4. 특정 권한을 가진 사용 가능 비밀번호를 정의하지 않는 한 사용 가능 비밀번호의 기본 권한은 15입니다.예:

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

5. 다른 권한으로 enable을 사용하는 경우 ASA에서 나타나는 해당 사용자 이름**은 enable_x입니다** (여기서 x는 권한).

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

사례 2:AAA 서버를 통해 구성된 ASA 인증 및 exec 권한 부여

ASA의 경우:

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

AAA 서버:

인증 결과:

a) 셸 프로파일

기본 권한:1
최대 권한:15

b) 명령 집합

모두 허용

관리 동작:

```
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 로그:

```
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.
```

관찰:

1. 인증 및 exec 권한 부여는 AAA 서버를 통해 수행됩니다.
2. exec 권한 부여는 인증을 위해 구성된 콘솔 연결(ssh, telnet 및 enable)에 대한 모든 요청에 대한 사용자 권한을 제어합니다.

참고:여기에는 ASA에 대한 직렬 연결이 포함되지 않습니다.

3. AAA 서버는 권한 부여 결과 기본 권한 1과 최대 권한 15를 제공하는 방식으로 구성됩니다.
4. 사용자가 AAA 서버에 구성된 TACACS+ 자격 증명을 통해 ASA에 로그인할 때 처음에 AAA 서버에 의해 사용자에게 권한 1이 주어집니다.
5. 사용자가 "enable" 키워드를 입력한 후 다시 입력(enable 비밀번호가 구성되지 않은 경우)하거나 enable 비밀번호(구성된 경우)를 입력하면 권한이 15로 변경되는 특권 모드로 들어갑니다.

사례 3:AAA 서버를 통해 구성된 ASA 인증, exec 권한 부여 및 명령 권한 부여

ASA의 경우:

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

AAA 서버:

인증 결과:

a) 셸 프로파일

기본 권한:1
최대 권한:15

b) 명령 집합
모두 허용

관리 동작:

```
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 로그:

```
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
```

관찰:

1. 인증 및 exec 권한 부여는 AAA 서버를 통해 수행됩니다.
2. exec 권한 부여는 인증을 위해 구성된 콘솔 연결(ssh, telnet 및 enable)에 대한 모든 요청에 대한 사용자 권한을 제어합니다.
3. 명령 권한 부여는 "aaa authorization command ISE LOCAL" 명령을 사용하여 AAA 서버에 의해 수행됩니다.

참고:여기에는 ASA에 대한 직렬 연결이 포함되지 않습니다.

4. 사용자가 AAA 서버에 구성된 TACACS+ 자격 증명을 통해 ASA에 로그인할 때 처음에 AAA 서버에 의해 사용자에게 권한 1이 주어집니다.
5. 사용자가 "enable" 키워드를 입력한 후 다시 입력(enable 비밀번호가 구성되지 않은 경우)하거나 enable 비밀번호(구성된 경우)를 입력하면 권한이 15로 변경되는 특권 모드로 들어갑니다.
6. AAA 서버가 실제 로그인한 인증된 사용자 대신 사용자 이름 "enable_15"에서 실행된 명령을 표시하므로 이 컨피그레이션에서는 명령 권한 부여가 실패합니다.
7. 명령 권한 부여 실패로 인해 기존 세션에서 실행되는 명령도 실패합니다.
8. 이 문제를 해결하려면 AAA 서버 또는 AD 및 ASA(로컬 폴백)에서 "enable_15"라는 이름의 사용자를 임의의 비밀번호로 생성합니다.

사용자가 AAA 서버 또는 AD에 구성되면 다음 동작이 관찰됩니다.

나.초기 인증을 위해 AAA 서버는 로그인한 사용자의 실제 사용자 이름을 확인합니다
2.enable 비밀번호를 입력하면 enable 인증이 이 컨피그레이션의 AAA 서버를 가리키지 않으므로 ASA에서 로컬로 확인됩니다

3.비밀번호를 활성화하면 모든 명령이 사용자 이름 "enable_15"로 실행되며 AAA는 AAA 서버 또는 AD에 해당 사용자 이름이 있기 때문에 이러한 명령을 허용합니다

사용자 "enable_15"가 구성되면 관리자가 권한 모드에서 ASA의 컨피그레이션 모드로 전환할 수 있습니다.

관리 동작:

```
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 로그:

```
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'
```

참고:TACACS를 통한 명령 권한 부여가 ASA에 구성된 경우 AAA 서버에 연결할 수 없을 때 폴백으로 "local"을 사용해야 합니다.
직렬 콘솔에 대한 인증이 구성되지 않은 경우에도 명령 권한 부여가 모든 ASA 세션(직렬 콘솔, ssh, 텔넷)에 적용되기 때문입니다.AAA 서버에 연결할 수 없고 사용자 "enable_15"가 로컬 데이터베이스에 없는 경우 관리자는 다음 오류를 가져옵니다.

대체 권한 부여.사용자 이름 'enable_15'가 로컬 데이터베이스에 없습니다.
명령 권한 부여 실패

ASA 로그:

```
%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
```

참고:위의 컨피그레이션을 사용하면 명령 권한 부여가 작동하지만 명령 어카운팅에는 로그인한 사용자의 실제 사용자 이름 대신 사용자 이름 "enable_15"가 계속 표시됩니다.따라서 관리자는 ASA에서 어떤 사용자가 어떤 명령을 실행했는지 확인하기 어렵습니다.

"enable_15" 사용자와 관련된 이 계정 문제를 해결하려면 다음을 수행합니다.

1. ASA의 exec authorization 명령에서 "auto-enable" 키워드를 사용합니다.
2. 인증된 사용자에게 할당된 TACACS 셸 프로파일에서 기본 및 최대 권한을 15로 설정합니다.

사례 4:ASA 인증, AAA 서버를 통해 구성된 "auto-enable"을 사용한 exec 권한 부여 및 명령 권한 부여

ASA의 경우:

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

AAA 서버:

인증 결과:

a) 셸 프로파일

기본 권한:15
최대 권한:15

b) 명령 집합
모두 허용

관리 동작:

```
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 로그:

```
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'
```

관찰:

1. 인증 및 exec 권한 부여는 AAA 서버를 통해 수행됩니다.
2. exec 권한 부여는 인증을 위해 구성된 콘솔 연결(ssh, telnet 및 enable)에 대한 모든 요청에 대한 사용자 권한을 제어합니다.

> **참고:**여기에는 ASA에 대한 직렬 연결이 포함되지 않습니다.

3. 명령 권한 부여는 "aaa authorization command ISE LOCAL" 명령을 사용하여 AAA 서버에 의해 수행됩니다.
4. 사용자가 AAA 서버에 구성된 TACACS+ 자격 증명을 통해 ASA에 로그인하면 사용자는 AAA 서버에서 권한 15를 획득하여 권한 모드에 로그인합니다.
5. 위의 컨피그레이션을 통해 사용자는 enable 비밀번호를 입력하지 않아도 되며, ASA 또는 AAA 서버에서 "enable_15" 사용자를 구성할 필요가 없습니다.
6. 이제 AAA 서버는 로그인한 사용자의 실제 사용자 이름에서 명령 권한 부여 요청을 보고합니다.

관련 정보

다음은 ASA용 AAA 디바이스 관리 관련 참조 문서입니다.

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