AAA-apparaatbeheergedrag voor ASA analyseren

Inhoud

Inleiding

Dit document beschrijft het gedrag van de apparaatbeheer wanneer een ASA is ingesteld voor verificatie en autorisatie met behulp van een AAA-server. Dit document toont het gebruik van Cisco Identity Services Engine (ISE) als een AAA-server met een actieve map als de Externe Identity Store. TACACS+ is het AAA-protocol dat in gebruik is.

Bijgedragen door Dinesh Moudgil en Poonam Garg, Cisco HTTS-engineers

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van ASA's CLI en ASDM
- Connectiviteit tussen ASA en AAA-server
- AAA-configuratie op Cisco ISE voor verificatie en autorisatie

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversie:

- ASAv-run 9.9(2)
- Cisco Identity Services Engine 2.6

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

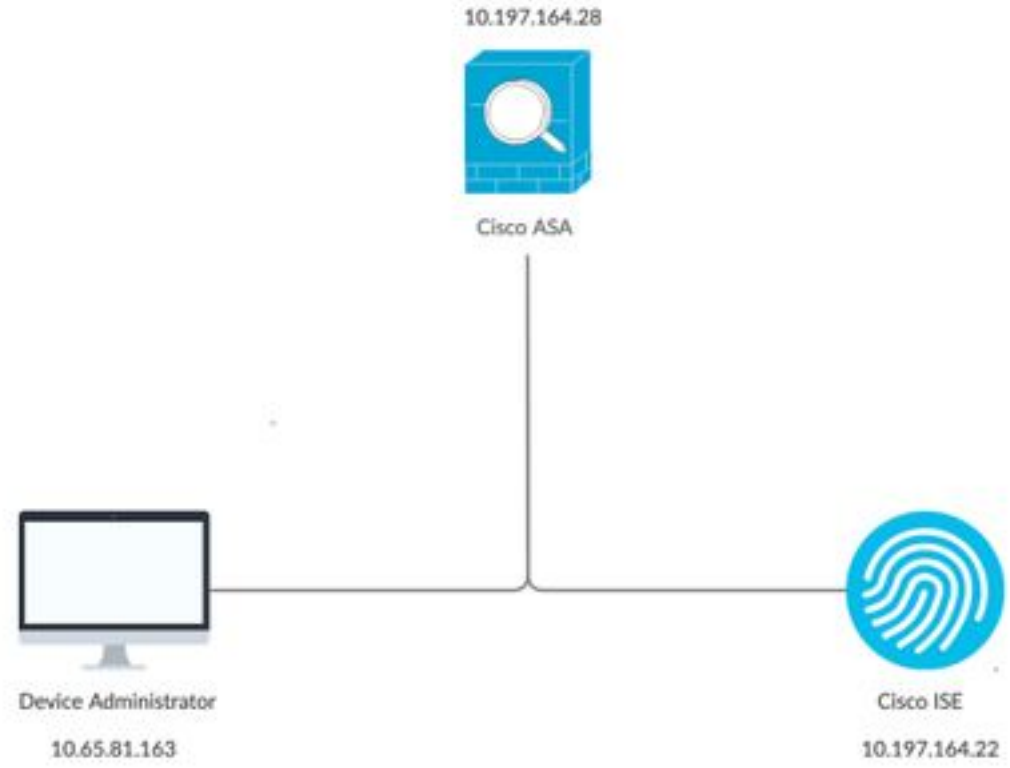
Cisco ASA ondersteunt de verificatie van beheersessies door gebruik te maken van een lokale gebruikersdatabase, een RADIUS-server of een TACACS+ server. Een beheerder kan met Cisco ASA verbinden via:

- Telnet
- Secure Shell (SSH)
- Seriële conservering
- Cisco ASA apparaatbeheer (ASDM)

Als u een verbinding maakt via telnet of SSH, kan de gebruiker de verificatie drie keer opnieuw proberen bij een gebruikersfout. Na de derde keer worden de verificatiesessie en de aansluiting op Cisco ASA gesloten.

Voordat u de configuratie start, moet u beslissen welke gebruikersdatabase u gebruikt (lokale of externe AAA-server). Als u een externe AAA-server gebruikt, zoals geconfigureerd in dit document, moet u de AAA-servergroep en -host configureren zoals in de onderstaande secties beschreven wordt. U kunt de AAA-verificatie en de AAA-autorisatie-opdrachten gebruiken om verificatie van verificatie en autorisatie respectievelijk te vereisen wanneer u Cisco ASA benadert voor beheer.

Netwerkdiagram



Configureren

Dit is de informatie die voor alle voorbeelden in dit document wordt gebruikt.

a) ASA-configuratie:

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

b) AAA-configuratie:

Verificatie op de AAA-server wordt uitgevoerd tegen Identity Store Sequence die uit AD en lokale database bestaat

Zaak 1: ASA-verificatie ingesteld via AAA-server

ASA:

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

Op AAA-server:

Resultaten van de vergunning:

a) Shell-profiel

Standaardvoorrecht: 1
Maximum aantal rechten: 15

b) Opdrachtset
Alles toestaan

Admin Gedrag:

```
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-bestanden:

```
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.
```

Opmerkingen:

1. Verificatie voor SSH-sessie wordt uitgevoerd via AAA-server
2. De vergunning wordt lokaal verleend, ongeacht het voorrecht dat in het vergunningsresultaat op de AAA-server is ingesteld
3. Nadat de gebruiker via AAA-server echt is bevonden, wanneer de gebruiker het trefwoord "Enable" (zonder wachtwoord ingesteld door standaard) invoert of het invoert wachtwoord in (indien ingesteld), wordt de gebruikte gebruikersnaam **Enable_15** gebruikt

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

4. Het defaultwachtwoord voor het inschakelen van het wachtwoord is 15, tenzij u definieert voor het inschakelen van het wachtwoord met een specifiek voorrecht. Bijvoorbeeld:

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

5. Als u gebruikt om bestand te maken tegen verschillende rechten, is de corresponderende gebruikersnaam die op ASA komt **Enable_x** (waarbij x het privilege is)

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

Zaak 2: ASA-verificatie en -machtiging via AAA-server

ASA:

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

Op AAA-server:

Resultaten van de vergunning:

a) Shell-profiel

Standaardvoorrecht: 1
Maximum aantal rechten: 15

b) Opdrachtset
Alles toestaan

Admin Gedrag:

```
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-bestanden:

```
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.
```

Opmerkingen:

1. Verificatie en externe autorisatie worden uitgevoerd via AAA-server
2. De EXec-vergunning regelt het gebruikersrecht voor alle verzoeken om de console-aansluitingen (ssh, telnet en Enable) die voor de verificatie zijn ingesteld

    Opmerking: Dit omvat geen seriële aansluiting op de ASA

3. AAA-server is zo geconfigureerd dat hij standaard voorrechten 1 en de maximale voorrechten van 15 biedt als gevolg van de vergunning
4. Wanneer de gebruiker zich via TACACS+ aanmeldingsgegevens op de AAA-server bij ASA inlogt, wordt de gebruiker aanvankelijk bevoorrecht 1 van de AAA-server gegeven
5. Zodra de gebruiker sleutelwoord "toelaten" invoert, druk nogmaals in (als om wachtwoord niet ingesteld wordt) of voer een wachtwoord in (indien ingesteld), dan worden ze in de geprivilegieerde modus waar de privilege in 15 verandert

Zaak 3: ASA-verificatie, externe autorisatie en opdracht, ingesteld via AAA-server

ASA:

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

Op AAA-server:

Resultaten van de vergunning:

a) Shell-profiel

  Standaardvoorrecht: 1
  Maximum aantal rechten: 15

b) Opdrachtset
  Alles toestaan

Admin Gedrag:

```
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-bestanden:

```
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
```

Opmerkingen:

1. Verificatie en externe autorisatie worden uitgevoerd via AAA-server
2. De EXec-vergunning regelt het gebruikersrecht voor alle verzoeken om de console-aansluitingen (ssh, telnet en Enable) die voor de verificatie zijn ingesteld
3. Opdrachtautorisatie wordt uitgevoerd door AAA-server met behulp van de opdracht "AAA autorisatie ISE LOCAL"

Opmerking: Dit omvat geen seriële aansluiting op de ASA

4. Wanneer de gebruiker zich via TACACS+ aanmeldingsgegevens op de AAA-server bij ASA inlogt, wordt de gebruiker aanvankelijk bevoorrecht 1 van de AAA-server gegeven
5. Zodra de gebruiker sleutelwoord "toelaten" invoert, druk nogmaals in (als om wachtwoord niet ingesteld te laten) of voer wachtwoord in (indien geconfigureerd), dan komen ze in de geprivilegieerde modus waar de privilege in 15 verandert
6. Opdrachtautorisatie faalt bij deze configuratie omdat de AAA-server laat zien dat de opdracht wordt gegeven door de gebruikersnaam "Enable_15" in plaats van door de gebruiker echt ingelogde gebruiker.
7. Een opdracht die op een bestaande sessie wordt uitgevoerd, zal ook mislukken als de opdracht niet is voltooid
8. Om dit aan te pakken, kunt u een gebruiker maken die "Enable_15" heet op AAA-server of op AD en ASA (voor plaatselijke back-up) met een willekeurig wachtwoord

Zodra de gebruiker op de AAA-server of AD is ingesteld wordt het volgende gedrag waargenomen:

i. Voor eerste authenticatie verifieert de AAA server de echte gebruikersnaam van de ingelogde gebruiker
ii. Nadat het wachtwoord is ingevoerd, wordt het lokaal op de ASA geverifieerd aangezien verificatie niet op de AAA-server in deze configuratie wijst
iii. Na het inschakelen van het wachtwoord worden alle opdrachten uitgevoerd met de gebruikersnaam "Enable_15" en AAA stelt deze opdrachten in op basis van het bestaan van de gebruikersnaam op AAA-server of op AD

Zodra de gebruiker "Enable_15" is ingesteld, mag de beheerder de voorkeurmodus overschakelen op de configuratiemodus in de ASA.

Admin Gedrag:

```
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-bestanden:

```
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'
```

> Opmerking: Als opdrachtautorisatie via TACACS op de ASA is ingesteld, is het verplicht om "lokaal" als reserve te hebben wanneer de AAA-server niet bereikbaar is.
> Dit komt doordat de opdrachtautorisatie van toepassing is op alle ASA sessies (seriële console, ssh, telnet) zelfs wanneer verificatie niet is ingesteld voor seriële console. In een dergelijk geval waarin AAA-server niet bereikbaar is en de gebruiker "Enable_15" niet aanwezig is in de lokale database, krijgt de beheerder de volgende fout:

Toestemming voor reddingssteun. Gebruikersnaam 'Enable_15' niet in LOCAL database
Opdrachtvergunning mislukt

ASA-bestanden:

```
%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
```

Opmerking: Met de bovenstaande configuratie zal de opdrachtautorisatie werken maar de opdrachtaccounting zal nog steeds de gebruikersnaam "Enable_15" in plaats van de echte gebruikersnaam voor de ingelogde gebruiker weergeven. Dit wordt moeilijk voor beheerders om te bepalen welke gebruiker welke specifieke opdracht op de ASA heeft uitgevoerd.

Om deze accounting kwestie met betrekking tot "Enable_15" gebruiker aan te pakken:

1. Gebruik het sleutelwoord "**autoenabled**" in de automatische autorisatie-opdracht van de ASA
2. Stel de standaard- en maximumvoorrechten in op 15 in het TACACS-shell-profiel dat is toegewezen aan de geauthentiseerde gebruiker

Zaak 4: ASA-verificatie, externe autorisatie met behulp van "autoconnect" en opdrachtautorisatie ingesteld via AAA-server

ASA:

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

Op AAA-server:

Resultaten van de vergunning:

a) Shell-profiel

Standaardvoorrecht: 15
Maximum aantal rechten: 15

b) Opdrachtset
Alles toestaan

Admin Gedrag:

```
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-bestanden:

```
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'
```

Opmerkingen:

1. Verificatie en externe autorisatie worden uitgevoerd via AAA-server
2. De EXec-vergunning regelt het gebruikersrecht voor alle verzoeken om de console-aansluitingen (ssh, telnet en Enable) die voor de verificatie zijn ingesteld

    Opmerking: Dit omvat geen seriële aansluiting op de ASA

3. Opdrachtautorisatie wordt uitgevoerd door AAA-server met behulp van de opdracht "AAA autorisatie ISE LOCAL"
4. Wanneer de gebruiker zich via TACACS+ aanmeldingsgegevens op de AAA-server bij ASA inlogt, krijgt de gebruiker bevoorrecht 15 op de AAA-server en logt hij dus in de bevoorrechtingsmodus
5. De gebruiker hoeft met de bovenstaande configuratie geen wachtwoord in te voeren om het wachtwoord in te schakelen. De gebruiker "Enable_15" hoeft niet op de ASA- of AAA-server te worden geconfigureerd.
6. AAA-server rapporteert nu het opdrachtautorisatieverzoek dat afkomstig is van de echte gebruikersnaam voor de inloggebruiker

Gerelateerde informatie

Hier zijn een aantal documenten ter referentie naar AAA-apparaatbeheer voor ASA:

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