Analyse des AAA-Geräteverwaltungsverhaltens für ASA

Inhalt

Einführung

Dieses Dokument beschreibt das Geräteverwaltungsverhalten, wenn eine ASA für die Authentifizierung und Autorisierung mithilfe eines AAA-Servers konfiguriert wird. In diesem Dokument wird die Verwendung der Cisco Identity Service Engine (ISE) als AAA-Server mit einem Active Directory als Externer Identitätsspeicher dargestellt. TACACS+ ist das verwendete AAA-Protokoll.

Unterstützt von Dinesh Moudgil und Poonam Garg, Cisco HTTS-Techniker

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundkenntnisse der CLI und ASDM von ASA
- Verbindungen zwischen ASA- und AAA-Server
- AAA-Konfiguration auf der Cisco ISE für Authentifizierung und Autorisierung

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der folgenden Softwareversion:

- ASAv mit 9.9(2)
- Cisco Identity Service Engine 2.6

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

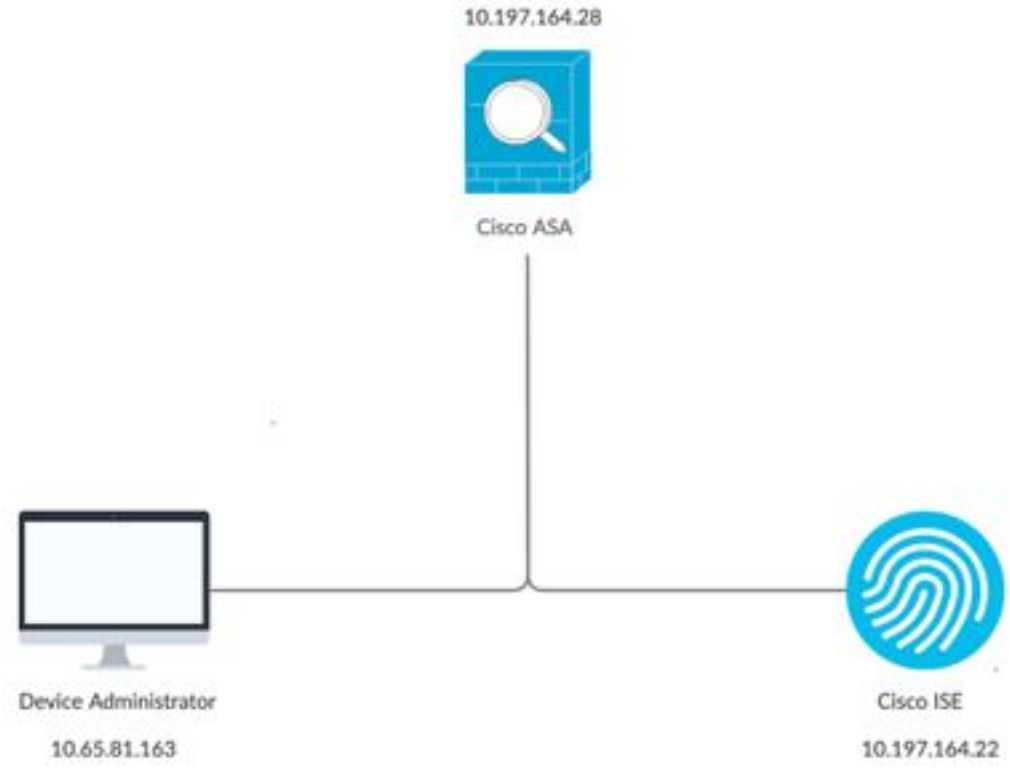
Die Cisco ASA unterstützt die Authentifizierung von Verwaltungssitzungen mithilfe einer lokalen Benutzerdatenbank, eines RADIUS-Servers oder eines TACACS+-Servers. Ein Administrator kann eine Verbindung zur Cisco ASA herstellen über:

- Telnet
- Secure Shell (SSH)
- Serielle Konsolenverbindung
- Cisco ASA Device Manager (ASDM)

Bei einer Verbindung über Telnet oder SSH kann der Benutzer die Authentifizierung dreimal wiederholen, falls ein Benutzerfehler auftritt. Nach dem dritten Mal werden die Authentifizierungssitzung und die Verbindung zur Cisco ASA geschlossen.

Bevor Sie die Konfiguration starten, müssen Sie entscheiden, welche Benutzerdatenbank Sie verwenden (lokaler oder externer AAA-Server). Wenn Sie einen externen AAA-Server verwenden, wie in diesem Dokument konfiguriert, konfigurieren Sie die AAA-Servergruppe und den Host wie in den folgenden Abschnitten beschrieben. Sie können die AAA-Authentifizierungs- und die AAA-Autorisierungsbefehle verwenden, um eine Authentifizierung bzw. Autorisierungsüberprüfung beim Zugriff auf die Cisco ASA für die Administration zu erfordern.

Netzwerkdiagramm



Konfigurieren

Dies sind die Informationen, die für alle Beispiele in diesem Dokument verwendet werden.

a) ASA-Konfiguration:

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

b) AAA-Konfiguration:

Die Authentifizierung auf dem AAA-Server erfolgt anhand der Identity Store Sequence, die aus AD und einer lokalen Datenbank besteht.

Fall 1: Konfiguration der ASA-Authentifizierung über AAA-Server

Auf ASA:

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

Auf AAA-Server:

Autorisierungsergebnisse:

a) Shell-Profil

Standardberechtigung: 1
Maximale Berechtigung: 15

b) Befehlssatz
Alle zulassen

Admin-Verhalten:

```
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-Protokolle:

```
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.
```

Beobachtungen:

1. Die Authentifizierung für die SSH-Sitzung erfolgt über den AAA-Server.
2. Die Autorisierung erfolgt lokal, unabhängig von der im Autorisierungsergebnis auf dem AAA-Server konfigurierten Berechtigung.
3. Nachdem der Benutzer über den AAA-Server authentifiziert wurde, gibt der Benutzer das Schlüsselwort "enable" ein (das standardmäßig kein Kennwort festgelegt hat) oder gibt das enable-Kennwort ein (sofern konfiguriert), und der entsprechende verwendete Benutzername lautet **enable_15.**

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

4. Die Standardberechtigung für das enable-Kennwort lautet 15, es sei denn, Sie definieren enable password mit einer bestimmten Berechtigung. Beispiel:

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

5. Wenn Sie enable mit unterschiedlichen Berechtigungen verwenden, lautet der entsprechende Benutzername, der auf der ASA verfügbar ist, **enable_x** (wobei x die Berechtigung ist).

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

Fall 2: Konfiguration der ASA-Authentifizierung und Exec-Autorisierung über AAA-Server

Auf ASA:

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

Auf AAA-Server:

Autorisierungsergebnisse:

a) Shell-Profil

Standardberechtigung: 1
Maximale Berechtigung: 15

b) Befehlssatz
Alle zulassen

Admin-Verhalten:

```
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-Protokolle:

```
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.
```

Beobachtungen:

1. Authentifizierung und exec-Autorisierung erfolgen über AAA-Server
2. Die Exec-Autorisierung regelt die Benutzerberechtigung für alle Anforderungen für die für die Authentifizierung konfigurierten Konsolenverbindungen (ssh, Telnet und enable).

> **Hinweis**: Dies schließt keine serielle Verbindung mit der ASA ein.

3. Der AAA-Server wird so konfiguriert, dass die Standard-Berechtigung 1 und die maximale Berechtigung von 15 Benutzern aufgrund der Autorisierung bereitgestellt werden.
4. Wenn sich der Benutzer über auf dem AAA-Server konfigurierte TACACS+-Anmeldeinformationen bei ASA anmeldet, erhält der Benutzer anfänglich die Berechtigung 1 des AAA-Servers.
5. Sobald der Benutzer das Schlüsselwort "enable" eingegeben hat, drückt er erneut die Eingabetaste (wenn das Kennwort nicht konfiguriert ist) oder gibt enable password (falls konfiguriert) ein, wechselt er in den privilegierten Modus, in dem die Berechtigung zu 15 geändert wird

Fall 3: ASA-Authentifizierung, exec-Autorisierung und Befehlsautorisierung über AAA-Server konfiguriert

Auf ASA:

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

Auf AAA-Server:

Autorisierungsergebnisse:

a) Shell-Profil

Standardberechtigung: 1
Maximale Berechtigung: 15

b) Befehlssatz
Alle zulassen

Admin-Verhalten:

```
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-Protokolle:

```
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
```

Beobachtungen:

1. Authentifizierung und exec-Autorisierung erfolgen über AAA-Server
2. Die Exec-Autorisierung regelt die Benutzerberechtigung für alle Anforderungen für die für die Authentifizierung konfigurierten Konsolenverbindungen (ssh, Telnet und enable).
3. Die Befehlsautorisierung wird vom AAA-Server mithilfe des Befehls "aaa authorized command ISE LOCAL" (AAA-Autorisierungsbefehl ISE LOCAL) durchgeführt.

> **Hinweis**: Dies schließt keine serielle Verbindung mit der ASA ein.

4. Wenn sich der Benutzer über auf dem AAA-Server konfigurierte TACACS+-Anmeldeinformationen bei ASA anmeldet, erhält der Benutzer anfänglich die Berechtigung 1 des AAA-Servers.
5. Sobald der Benutzer das Schlüsselwort "enable" eingegeben hat, drückt er erneut die Eingabetaste (wenn enable password nicht konfiguriert ist) oder gibt enable password (falls konfiguriert) ein, wechselt er in den privilegierten Modus, in dem die Berechtigung zu 15 geändert wird
6. Die Befehlsautorisierung schlägt mit dieser Konfiguration fehl, da der AAA-Server den Befehl anzeigt, der vom Benutzernamen "enable_15" statt vom authentifizierten Benutzer angemeldet ausgeführt wird.
7. Jeder Befehl, der auf einer vorhandenen Sitzung ausgeführt wird, schlägt ebenfalls aufgrund eines Befehlsermächtigungsfehlers fehl.
8. Erstellen Sie dazu einen Benutzer mit dem Namen "enable_15" auf dem AAA-Server oder auf AD und ASA (für lokales Fallback) mit einem zufälligen Kennwort.

Nachdem der Benutzer auf dem AAA-Server oder AD konfiguriert wurde, wird folgendes Verhalten beobachtet:

i. Für die erste Authentifizierung überprüft der AAA-Server den tatsächlichen Benutzernamen des angemeldeten Benutzers.
ii) Sobald das enable-Kennwort eingegeben wurde, wird es lokal auf der ASA überprüft, da die enable-Authentifizierung nicht auf den AAA-Server in dieser Konfiguration verweist.
iii) Nach Aktivierung des Kennworts werden alle Befehle mit dem Benutzernamen "enable_15" ausgeführt, und AAA lässt diese Befehle aufgrund des vorhandenen Benutzernamens auf dem AAA-Server oder AD zu

Sobald der Benutzer "enable_15" konfiguriert ist, kann der Administrator auf der ASA vom privilegierten Modus in den Konfigurationsmodus wechseln.

Admin-Verhalten:

```
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-Protokolle:

```
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'
```

Hinweis: Wenn die Befehlsautorisierung über TACACS auf der ASA konfiguriert ist, muss

"local" als Fallback angegeben werden, wenn der AAA-Server nicht erreichbar ist.
Dies liegt daran, dass die Befehlsautorisierung für alle ASA-Sitzungen (serielle Konsole, SSH, Telnet) gilt, auch wenn die Authentifizierung nicht für serielle Konsolen konfiguriert ist.
Wenn der AAA-Server nicht erreichbar ist und der Benutzer "enable_15" nicht in der lokalen Datenbank vorhanden ist, erhält der Administrator den folgenden Fehler:

Fallback-Autorisierung. Benutzername 'enable_15' nicht in LOKALER Datenbank Befehlsautorisierung fehlgeschlagen

ASA-Protokolle:

```
%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
```

Hinweis: Mit der oben beschriebenen Konfiguration funktioniert die Befehlsautorisierung, aber die Befehlsabrechnung zeigt den Benutzernamen "enable_15" anstelle des echten Benutzernamens des angemeldeten Benutzers an. Administratoren können nur schwer feststellen, welcher Benutzer welchen Befehl auf der ASA ausgeführt hat.

So beheben Sie dieses Problem mit der Buchhaltung für "enable_15"-Benutzer:

1. Verwenden Sie das Schlüsselwort "**auto-enable**" im exec-Autorisierungsbefehl auf der ASA.
2. Legen Sie im TACACS-Shell-Profil für den authentifizierten Benutzer die Standard- und die maximale Berechtigung auf 15 fest.

Fall 4: ASA-Authentifizierung, exec-Autorisierung mit "auto-enable" und Befehlsautorisierung, konfiguriert über AAA-Server

Auf ASA:

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

Auf AAA-Server:

Autorisierungsergebnisse:

a) Shell-Profil

Standardberechtigung: 15
Maximale Berechtigung: 15

b) Befehlssatz
Alle zulassen

Admin-Verhalten:

```
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-Protokolle:

```
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'
```

Beobachtungen:

1. Authentifizierung und exec-Autorisierung erfolgen über AAA-Server
2. Die Exec-Autorisierung regelt die Benutzerberechtigung für alle Anforderungen für die für die Authentifizierung konfigurierten Konsolenverbindungen (ssh, Telnet und enable).

> **Hinweis**: Dies schließt keine serielle Verbindung mit der ASA ein.

3. Die Befehlsautorisierung wird vom AAA-Server mithilfe des Befehls "aaa authorized command ISE LOCAL" (AAA-Autorisierungsbefehl ISE LOCAL) durchgeführt.
4. Wenn sich der Benutzer über auf dem AAA-Server konfigurierte TACACS+-Anmeldeinformationen bei ASA anmeldet, erhält der Benutzer die Berechtigung 15 durch den AAA-Server und meldet sich so in den Berechtigungsmodus an
5. Bei der obigen Konfiguration muss der Benutzer das enable-Kennwort nicht eingeben, und der Benutzer "enable_15" muss auf dem ASA- oder AAA-Server nicht konfiguriert werden.
6. Der AAA-Server meldet jetzt die Anforderung für die Befehlsautorisierung, die vom tatsächlichen Benutzernamen des angemeldeten Benutzers stammt.

Zugehörige Informationen

Nachstehend finden Sie Referenzdokumente für die AAA-Geräteadministration für ASA:

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

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