Análisis del comportamiento de administración de dispositivos AAA para ASA

Contenido

Introducción

Este documento describe el comportamiento de administración del dispositivo cuando se configura un ASA para la autenticación y autorización usando un servidor AAA. Este documento muestra el uso de Cisco Identity Service Engine (ISE) como servidor AAA con Active Directory como almacén de identidad externo. TACACS+ es el protocolo AAA en uso.

Colaboración de Dinesh Moudgil y Poonam Garg, ingenieros de Cisco HTTS

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de ASA CLI y ASDM
- Conectividad entre ASA y el servidor AAA
- Configuración AAA en Cisco ISE para Autenticación y Autorización

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software:’

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

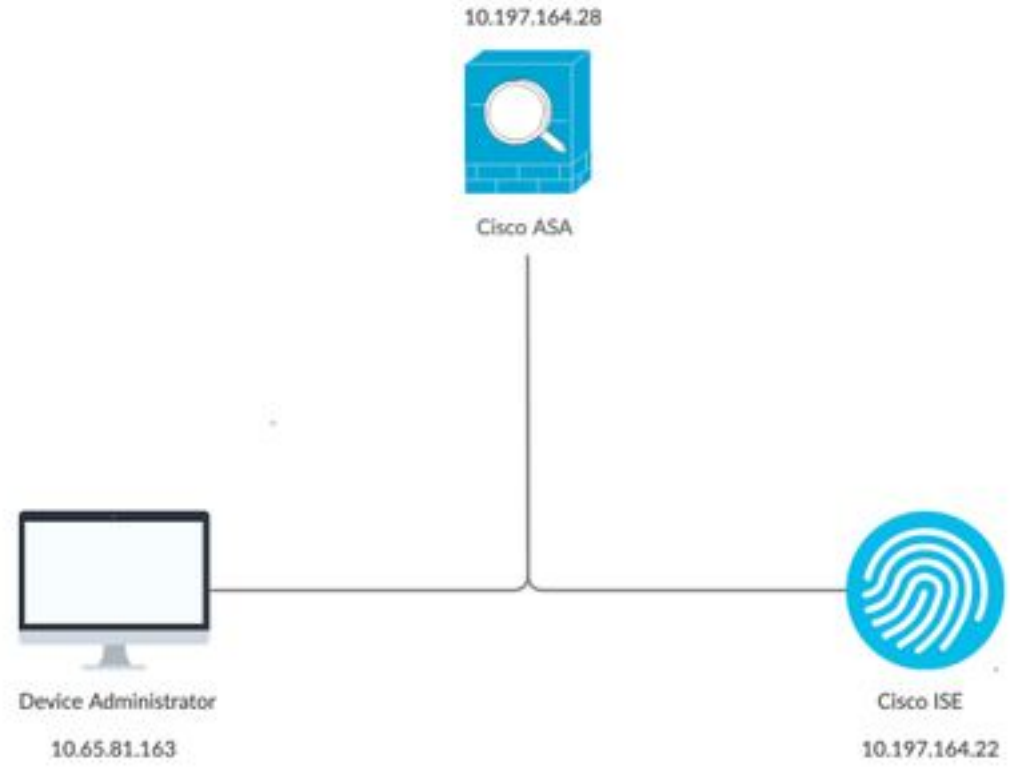
Cisco ASA admite la autenticación de sesiones administrativas mediante una base de datos de usuario local, un servidor RADIUS o un servidor TACACS+. Un administrador puede conectarse a Cisco ASA a través de:

- TELNET
- Secure Shell (SSH)
- Conexión de consola serie
- Administrador de dispositivos Cisco ASA (ASDM)

Si se conecta a través de Telnet o SSH, el usuario puede reintentar la autenticación tres veces en caso de error del usuario. Después de la tercera vez, se cierran la sesión de autenticación y la conexión a Cisco ASA.

Antes de iniciar la configuración, debe decidir qué base de datos de usuario utilizará (servidor AAA local o externo). Si está utilizando un servidor AAA externo, tal como se configura en este documento, configure el grupo de servidores y el host AAA como se describe en las secciones siguientes. Puede utilizar los comandos aaa authentication y aaa authorization para requerir autenticación y verificación de autorización respectivamente al acceder a Cisco ASA para administración.

Diagrama de la red



Configurar

Esta es la información utilizada para todos los ejemplos de este documento.

a) Configuración de ASA:

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

b) Configuración AAA:

La autenticación en el servidor AAA se realiza contra la Secuencia del almacén de identidad que consta de AD y base de datos local

Caso 1: Autenticación ASA configurada a través del servidor AAA

En ASA:

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

En el servidor AAA:

Resultados de la autorización:

a) Perfil de Shell

Privilegio predeterminado: 1
Privilegio máximo: 15

b) Conjunto de comandos
Permitir todo

Comportamiento del administrador:

```
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
```

Registros ASA:

```
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.
```

Observaciones:

1. La autenticación para la sesión SSH se realiza a través del servidor AAA
2. La autorización se realiza localmente independientemente del privilegio configurado en el servidor AAA en el resultado de la autorización
3. Después de que el usuario se autentica a través del servidor AAA, cuando el usuario ingresa la palabra clave "enable" (que no tiene ninguna contraseña establecida de forma predeterminada) o ingresa la contraseña de habilitación (si está configurada), el nombre de usuario correspondiente utilizado es **enable_15**

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

4. El privilegio predeterminado para habilitar la contraseña es 15 a menos que defina habilitar la contraseña con un privilegio específico. Por ejemplo:

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

5. Si utiliza enable con privilegios diferentes, el nombre de usuario correspondiente que aparece en ASA es **enable_x** (donde x es el privilegio)

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

Caso 2: Autenticación ASA y autorización exec configuradas a través del servidor AAA

En ASA:

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

En el servidor AAA:

Resultados de la autorización:

a) Perfil de Shell

Privilegio predeterminado: 1
Privilegio máximo: 15

b) Conjunto de comandos
Permitir todo

Comportamiento del administrador:

```
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
```

Registros ASA:

```
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.
```

Observaciones:

1. La autenticación y la autorización exec se realizan a través del servidor AAA
2. La autorización Exec rige el privilegio de usuario para todas las solicitudes de conexiones de consola (ssh, telnet y enable) configuradas para la autenticación

> **Nota:** Esto no incluye la conexión serial al ASA

3. El servidor AAA se configura de forma que proporcione el privilegio predeterminado 1 y el privilegio máximo de 15 como resultado de la autorización
4. Cuando el usuario inicia sesión en ASA a través de las credenciales TACACS+ configuradas en el servidor AAA, el usuario recibe inicialmente el privilegio 1 por el servidor AAA
5. Una vez que el usuario ingresa la palabra clave "enable", presiona enter again (si enable password no se configura) o ingresa enable password(if configured), entran en el modo privilegiado donde el privilegio cambia a 15

Caso 3: Autenticación ASA, autorización exec y autorización de comandos configurada a través del servidor AAA

En ASA:

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

En el servidor AAA:

Resultados de la autorización:

a) Perfil de Shell

Privilegio predeterminado: 1
Privilegio máximo: 15

b) Conjunto de comandos
Permitir todo

Comportamiento del administrador:

```
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
```

Registros ASA:

```
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
```

Observaciones:

1. La autenticación y la autorización exec se realizan a través del servidor AAA
2. La autorización Exec rige el privilegio de usuario para todas las solicitudes de conexiones de consola (ssh, telnet y enable) configuradas para la autenticación
3. La autorización de comandos la realiza el servidor AAA mediante el comando "aaa authorization command ISE LOCAL"

Nota: Esto no incluye la conexión serial al ASA

4. Cuando el usuario inicia sesión en ASA a través de las credenciales TACACS+ configuradas en el servidor AAA, el usuario recibe inicialmente el privilegio 1 por el servidor AAA
5. Una vez que el usuario ingresa la palabra clave "enable", presiona enter again (si enable password no se configura) o ingresa enable password (enable password) password (si se configura), entran en el modo privilegiado donde el privilegio cambia a 15
6. La autorización del comando falla con esta configuración porque el servidor AAA muestra el comando que ejecuta el nombre de usuario "enable_15" en lugar de un usuario autenticado con sesión real.
7. Cualquier comando ejecutado en una sesión existente también fallará debido a una falla de autorización de comandos
8. Para solucionar esto, cree un usuario denominado "enable_15" en el servidor AAA o en AD y ASA (para reserva local) con una contraseña aleatoria

Una vez que el usuario se configura en el servidor AAA o en AD, se observa el siguiente comportamiento:

i. Para la autenticación inicial, el servidor AAA verifica el nombre de usuario real del usuario conectado
ii. Una vez que se ingresa la contraseña de habilitación, se verifica localmente en el ASA ya que la autenticación de habilitación no apunta al servidor AAA en esta configuración
iii. Después de habilitar la contraseña, todos los comandos se ejecutan con el nombre de usuario "enable_15" y AAA permite esos comandos en virtud de la existencia de ese nombre de usuario en el servidor AAA o AD

Una vez configurado el usuario "enable_15", se permite al administrador pasar del modo de privilegio al modo de configuración en el ASA.

Comportamiento del administrador:

```
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
```

Registros ASA:

```
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'
```

Nota: Si la autorización de comandos a través de TACACS se configura en el ASA, es obligatorio tener "local" como reserva cuando el servidor AAA no es alcanzable.
Esto se debe a que la autorización de comandos se aplica a todas las sesiones ASA (consola serial, ssh, telnet) incluso cuando la autenticación no está configurada para la consola serial. En tal caso, cuando el servidor AAA no es accesible y el usuario "enable_15" no está presente en la base de datos local, el administrador recibe el siguiente error:

Autorización de reserva. El nombre de usuario 'enable_15' no está en la base de datos LOCAL
Error en la autorización del comando

Registros ASA:

```
%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
```

Nota: Con la configuración anterior, la autorización de comandos funcionará pero la contabilización de comandos seguirá mostrando el nombre de usuario "enable_15" en lugar del nombre de usuario real del usuario conectado. Esto se torna difícil para los administradores determinar qué usuario ejecutó cada comando en particular en el ASA.

Para solucionar este problema de contabilidad relacionado con el usuario "enable_15":

1. Utilice la palabra clave "**auto-enable**" en el comando exec authorization en el ASA
2. Establezca el privilegio predeterminado y máximo en 15 en el perfil de shell TACACS asignado al usuario autenticado

Caso 4: Autenticación ASA, autorización exec mediante "auto-enable" y autorización de comandos configurada a través del servidor AAA

En ASA:

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

En el servidor AAA:

Resultados de la autorización:

a) Perfil de Shell

Privilegio predeterminado: 15
Privilegio máximo: 15

b) Conjunto de comandos
Permitir todo

Comportamiento del administrador:

```
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)#
```

Registros ASA:

```
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'
```

Observaciones:

1. La autenticación y la autorización exec se realizan a través del servidor AAA
2. La autorización Exec rige el privilegio de usuario para todas las solicitudes de las conexiones de consola (ssh, telnet y enable) configuradas para la autenticación

> **Nota:** Esto no incluye la conexión serial al ASA

3. La autorización de comandos la realiza el servidor AAA mediante el comando "aaa authorization command ISE LOCAL"
4. Cuando el usuario inicia sesión en ASA a través de las credenciales TACACS+ configuradas en el servidor AAA, el usuario obtiene el privilegio 15 por el servidor AAA y, por lo tanto, inicia sesión en modo de privilegio
5. Con la configuración anterior, no se requiere que el usuario introduzca la contraseña de activación y el usuario "enable_15" no se debe configurar en el servidor ASA o AAA.
6. El servidor AAA ahora notificará la solicitud de autorización de comando proveniente del nombre de usuario real del usuario conectado

Información Relacionada

Estos son algunos documentos de referencia relacionados con la Administración de dispositivos AAA para 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