Analyser le comportement d'administration des périphériques AAA pour ASA

Contenu

Introduction

Ce document décrit le comportement d'administration des périphériques lorsqu'un ASA est configuré pour l'authentification et l'autorisation à l'aide d'un serveur AAA. Ce document montre l'utilisation de Cisco Identity Service Engine (ISE) en tant que serveur AAA avec Active Directory en tant que magasin d'identités externe. TACACS+ est le protocole AAA utilisé.

Contribution de Dinesh Moudgil et Poonam Garg, ingénieurs HTTS Cisco

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base de l'interface de ligne de commande et de l'ASDM d'ASA
- Connectivité entre ASA et serveur AAA
- Configuration AAA sur Cisco ISE pour l'authentification et l'autorisation

Components Used

Les informations de ce document sont basées sur la version logicielle suivante :

- ASAv exécutant la version 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 votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

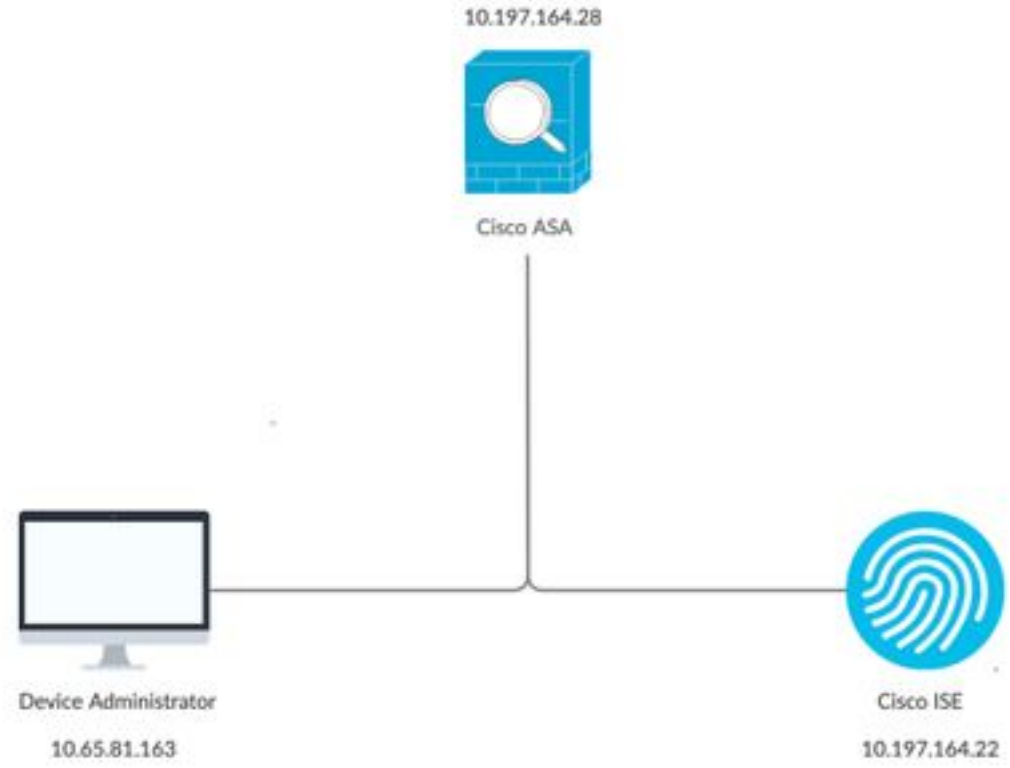
Cisco ASA prend en charge l'authentification des sessions administratives à l'aide d'une base de données d'utilisateurs locaux, d'un serveur RADIUS ou d'un serveur TACACS+. Un administrateur peut se connecter à Cisco ASA via :

- Telnet
- Secure Shell (SSH)
- Connexion de console série
- Cisco ASA Device Manager (ASDM)

Si vous vous connectez via Telnet ou SSH, l'utilisateur peut réessayer l'authentification trois fois en cas d'erreur de l'utilisateur. Après la troisième fois, la session d'authentification et la connexion à Cisco ASA sont fermées.

Avant de commencer la configuration, vous devez décider de la base de données utilisateur que vous utiliserez (serveur AAA local ou externe). Si vous utilisez un serveur AAA externe, tel que configuré dans ce document, configurez le groupe de serveurs et l'hôte AAA comme indiqué dans les sections suivantes. Vous pouvez utiliser les commandes d'authentification aaa et d'autorisation aaa pour exiger respectivement l'authentification et la vérification d'autorisation lors de l'accès à Cisco ASA pour administration.

Diagramme du réseau



Configuration

Il s'agit des informations utilisées pour tous les exemples de ce document.

a) Configuration ASA :

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

b) Configuration AAA :

L'authentification sur le serveur AAA est exécutée sur la séquence de magasin d'identités qui se compose d'AD et de la base de données locale

Cas 1 : Authentification ASA configurée via le serveur AAA

Sur ASA :

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

Sur le serveur AAA :

Résultats de l'autorisation :

a) Profil de la coque

Privilège par défaut : 1
Privilège maximal : 15

b) Jeu de commandes
Autoriser tout

Comportement de l'administrateur :

```
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
```

Journaux 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.
```

Observations :

1. L'authentification pour la session SSH est effectuée via le serveur AAA
2. L'autorisation est effectuée localement indépendamment du privilège configuré sur le serveur AAA dans le résultat de l'autorisation
3. Une fois l'utilisateur authentifié via le serveur AAA, lorsque l'utilisateur entre le mot clé « enable » (qui n'a pas de mot de passe défini par défaut) ou le mot de passe enable (s'il est configuré), le nom d'utilisateur correspondant utilisé est **enable_15**

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

4. Le privilège par défaut pour le mot de passe enable est 15, sauf si vous définissez le mot de passe enable avec un privilège spécifique. Exemple :

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

5. Si vous utilisez enable avec des privilèges différents, le nom d'utilisateur correspondant qui apparaît sur ASA est **enable_x** (où x est le privilège)

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

Cas 2 : Authentification ASA et autorisation exec configurées via le serveur AAA

Sur ASA :

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

Sur le serveur AAA :

Résultats de l'autorisation :

a) Profil de la coque

Privilège par défaut : 1
Privilège maximal : 15

b) Jeu de commandes
Autoriser tout

Comportement de l'administrateur :

```
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
```

Journaux 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.
```

Observations :

1. L'authentification et l'autorisation exec sont effectuées via le serveur AAA
2. L'autorisation Exec régit le privilège utilisateur pour toutes les demandes de connexions de console (ssh, telnet et enable) configurées pour l'authentification.

> **Note**: Ceci n'inclut pas la connexion série à l'ASA

3. Le serveur AAA est configuré de manière à fournir le privilège par défaut 1 et le privilège maximum de 15 en raison de l'autorisation
4. Lorsque l'utilisateur se connecte à ASA via les informations d'identification TACACS+ configurées sur le serveur AAA, le serveur AAA lui accorde initialement le privilège 1
5. Une fois que l'utilisateur entre le mot clé « enable », appuie de nouveau sur Entrée (si le mot de passe enable n'est pas configuré) ou sur Mot de passe enable (s'il est configuré), il passe en mode privilégié où le privilège passe à 15

Cas 3 : Authentification ASA, autorisation exec et autorisation des commandes configurées via le serveur AAA

Sur ASA :

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

Sur le serveur AAA :

Résultats de l'autorisation :

a) Profil de la coque

Privilège par défaut : 1
Privilège maximal : 15

b) Jeu de commandes
Autoriser tout

Comportement de l'administrateur :

```
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
```

Journaux 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
```

Observations :

1. L'authentification et l'autorisation exec sont effectuées via le serveur AAA
2. L'autorisation Exec régit le privilège utilisateur pour toutes les demandes de connexions de console (ssh, telnet et enable) configurées pour l'authentification.
3. L'autorisation de commande est exécutée par le serveur AAA à l'aide de la commande « aaa Authorization command ISE LOCAL »

Note: Ceci n'inclut pas la connexion série à l'ASA

4. Lorsque l'utilisateur se connecte à ASA via les informations d'identification TACACS+ configurées sur le serveur AAA, le serveur AAA lui accorde initialement le privilège 1
5. Une fois que l'utilisateur entre le mot clé « enable », appuie de nouveau sur Entrée (si le mot de passe enable n'est pas configuré) ou sur Mot de passe enable (s'il est configuré), il passe en mode privilégié où le privilège passe à 15
6. L'autorisation de commande échoue avec cette configuration, car le serveur AAA affiche la commande émise par le nom d'utilisateur « enable_15 » au lieu d'un utilisateur authentifié connecté.
7. Toute commande exécutée sur une session existante échouera également en raison d'un échec d'autorisation de commande
8. Pour résoudre ce problème, créez un utilisateur nommé « enable_15 » sur le serveur AAA ou sur AD et ASA (pour le secours local) avec un mot de passe aléatoire

Une fois l'utilisateur configuré sur le serveur AAA ou AD, le comportement suivant est observé :

i. Pour l'authentification initiale, le serveur AAA vérifie le nom d'utilisateur réel de l'utilisateur connecté
ii. Une fois le mot de passe enable entré, il est vérifié localement sur l'ASA, car l'authentification enable ne pointe pas vers le serveur AAA dans cette configuration
iii. Après activation du mot de passe, toutes les commandes sont exécutées avec le nom d'utilisateur « enable_15 » et AAA autorise ces commandes en vertu de l'existence de ce nom d'utilisateur sur le serveur AAA ou AD

Une fois que l'utilisateur « enable_15 » est configuré, l'administrateur est autorisé à passer du mode privilégié au mode de configuration sur l'ASA.

Comportement de l'administrateur :

```
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
```

Journaux 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'
```

Note: Si l'autorisation de commande via TACACS est configurée sur l'ASA, il est obligatoire d'avoir « local » comme secours lorsque le serveur AAA n'est pas accessible.
En effet, l'autorisation de commande s'applique à toutes les sessions ASA (console série, ssh, telnet) même lorsque l'authentification n'est pas configurée pour la console série. Si le serveur AAA n'est pas accessible et que l'utilisateur « enable_15 » n'est pas présent dans la base de données locale, l'administrateur obtient l'erreur suivante :

Autorisation de secours. Nom d'utilisateur 'enable_15' non présent dans la base de données LOCAL
Échec de l'autorisation de commande

Journaux 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
```

Note: Avec la configuration ci-dessus, l'autorisation de commande fonctionnera, mais la comptabilité de commande affichera toujours le nom d'utilisateur « enable_15 » au lieu du nom d'utilisateur réel de l'utilisateur connecté. Cela devient difficile pour les administrateurs de déterminer quel utilisateur a exécuté la commande particulière sur l'ASA.

Pour résoudre ce problème de comptabilité relatif à l'utilisateur « enable_15 » :

1. Utilisez le mot clé "**auto-enable**" dans la commande d'autorisation exec sur l'ASA
2. Définissez le privilège maximum et par défaut sur 15 dans le profil de shell TACACS attribué à l'utilisateur authentifié

Cas 4 : Authentification ASA, autorisation exec avec activation automatique et autorisation de commande configurées via le serveur AAA

Sur ASA :

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

Sur le serveur AAA :

Résultats de l'autorisation :

a) Profil de la coque

Privilège par défaut : 15
Privilège maximal : 15

b) Jeu de commandes
Autoriser tout

Comportement de l'administrateur :

```
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)#
```

Journaux 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'
```

Observations :

1. L'authentification et l'autorisation exec sont effectuées via le serveur AAA
2. L'autorisation Exec régit le privilège utilisateur pour toutes les demandes de connexions de console (ssh, telnet et enable) configurées pour l'authentification.

Note: Ceci n'inclut pas la connexion série à l'ASA

3. L'autorisation de commande est exécutée par le serveur AAA à l'aide de la commande « aaa Authorization command ISE LOCAL »
4. Lorsque l'utilisateur se connecte à ASA via les informations d'identification TACACS+ configurées sur le serveur AAA, l'utilisateur obtient le privilège 15 par le serveur AAA et se connecte donc en mode privilégié
5. Avec la configuration ci-dessus, l'utilisateur n'est pas tenu d'entrer le mot de passe enable, et l'utilisateur « enable_15 » n'est pas nécessaire d'être configuré sur le serveur ASA ou AAA.
6. Le serveur AAA va maintenant signaler la demande d'autorisation de commande provenant du nom d'utilisateur réel de l'utilisateur connecté

Informations connexes

Voici quelques documents de référence relatifs à l'administration de périphériques AAA pour 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