ASAのAAAデバイス管理動作の分析

内容

概要

このドキュメントでは、ASAがAAAサーバを使用して認証および許可するように設定されている場合のデバイス管理動作について説明します。このドキュメントでは、外部IDストアとしてActive Directoryを使用するAAAサーバとしてCisco Identity Service Engine(ISE)を使用する方法について説明します。TACACS+は、使用中のAAAプロトコルです。

著者：Cisco HTTSエンジニア、Dinesh MoudgilおよびPoonam Garg

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ASAのCLIおよびASDMに関する基礎知識
- ASAとAAAサーバ間の接続
- 認証と認可のためのCisco ISEでのAAA設定

使用するコンポーネント

- 9.9(2)が稼働するASAv

- Cisco Identity Service Engine 2.6

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

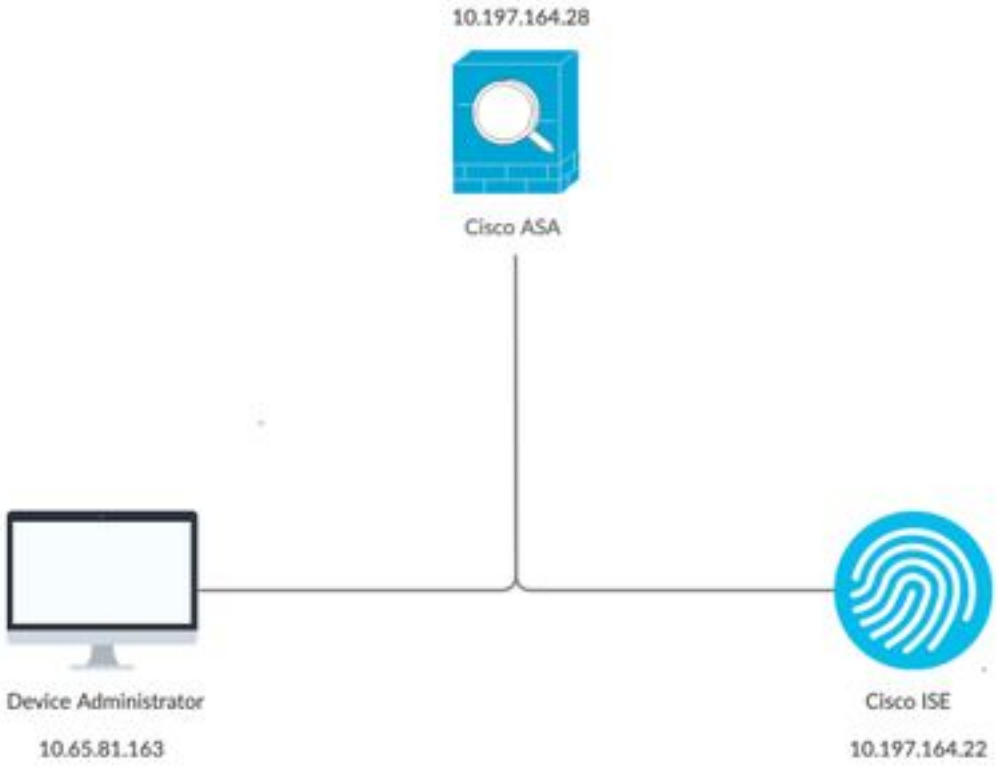
Cisco ASAは、ローカルユーザデータベース、RADIUSサーバ、またはTACACS+サーバを使用して、管理セッションの認証をサポートします。管理者は、次の方法でCisco ASAに接続できます。

- Telnet
- セキュア シェル（SSH）
- シリアルコンソール接続
- Cisco ASA Device Manager(ASDM)

TelnetまたはSSH経由で接続している場合、ユーザはユーザエラーの場合に3回認証を再試行できます。3回目の後、認証セッションとCisco ASAへの接続が閉じます。

設定を開始する前に、使用するユーザデータベース（ローカルまたは外部のAAAサーバ）を決定する必要があります。 このドキュメントで設定されている外部AAAサーバを使用している場合は、次の項で説明するようにAAAサーバグループとホストを設定します。aaa authenticationコマンドとaaa authorizationコマンドを使用すると、Cisco ASAにアクセスして管理する際に、それぞれ認証と認可の検証を要求できます。

ネットワーク図



設定

これは、このドキュメントのすべての例で使用される情報です。

a) ASAの設定：

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

b) AAA設定：

AAAサーバでの認証は、ADとローカルデータベースで構成されるIDストアシーケンスに対して実行されます

ケース 1：AAAサーバ経由で設定されたASA認証

ASA上：

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

AAAサーバ：

許可結果：

a)シェルプロファイル

デフォルト権限：1
最大特権：15

b)コマンドセット
すべて許可

管理者の動作：

```
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 ログ:

```
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.
```

観察:

1. SSHセッションの認証はAAAサーバを介して実行される
2.認可は、認可結果のAAAサーバに設定された特権に関係なく、ローカルで行われます
3.ユーザがAAAサーバ経由で認証された後、ユーザがキーワード「enable」（デフォルトではパスワードは設定されていません）を入力するか、イネーブルパスワードを入力すると（設定されている場合）、対応するユーザ名**はenable_15になります**

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

4.イネーブルパスワードのデフォルトの特権は、特定の特権でイネーブルパスワードを定義しない限り、15です。以下に、いくつかの例を示します。

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

5.異なる特権を持つenableを使用している場合、ASAで表示される対応するユーザ名は **enable_x**（xは特権）です

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

ケース 2：AAAサーバを介して設定されたASA認証およびexec許可

ASA上：

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

AAAサーバ：

許可結果：

a)シェルプロファイル

デフォルト権限：1
最大特権：15

b)コマンドセット
すべて許可

管理者の動作：

```
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 ログ:

```
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.
```

観察:

1.認証とexec許可はAAAサーバ経由で実行されます
2.認証が、認証用に設定されたコンソール接続（ssh、telnet、およびenable）に対するすべての要求に対するユーザ権限を制御します

注：これには、ASAへのシリアル接続は含まれません

3. AAAサーバは、認可の結果としてデフォルト特権1と最大特権15を提供するように設定されています
4.ユーザがAAAサーバに設定されたTACACS+クレデンシャルを使用してASAにログインすると、最初にユーザにAAAサーバから特権1が与えられます
5.ユーザがキーワード「enable」を入力し、Enterキーを再度押すか（enable passwordが設定されていない場合）、イネーブルパスワードを入力すると（設定されている場合）、特権が15に変更される特権モードに入ります

ケース 3：AAAサーバを介して設定されたASA認証、exec許可、およびコマンド許可

ASA上：

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

AAAサーバ：

許可結果：

a)シェルプロファイル

デフォルト権限：1
最大特権：15

b)コマンドセット
すべて許可

管理者の動作：

```
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 ログ:

```
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
```

観察:

1.認証とexec許可はAAAサーバ経由で実行されます
2.認証が、認証用に設定されたコンソール接続（ssh、telnet、およびenable）に対するすべての要求に対するユーザ権限を制御します
3.コマンド許可は、コマンド「aaa authorization command ISE LOCAL」を使用してAAAサーバによって実行されます

注：これには、ASAへのシリアル接続は含まれません

4.ユーザがAAAサーバに設定されたTACACS+クレデンシャルを使用してASAにログインすると、最初にユーザにAAAサーバから特権1が与えられます
5.ユーザがキーワード「enable」を入力し、再度enterキーを押すか（enable passwordが設定されていない場合）、イネーブルパスワードを入力すると（設定されている場合）、特権が15に変更される特権モードに入ります
6. AAAサーバは、実際にログインした認証ユーザではなく、ユーザ名「enable_15」によって発行されたコマンドを示すため、この設定ではコマンド許可が失敗します。
7.既存のセッションで実行されたコマンドも、コマンド許可の失敗により失敗します
8.これに対処するには、AAAサーバまたはADおよびASA（ローカルフォールバック用）で、ランダムなパスワードを使用して「enable_15」という名前のユーザを作成します

ユーザがAAAサーバまたはADに設定されると、次の動作が観察されます。

i.初期認証では、AAAサーバがログインユーザの実際のユーザ名を確認します
ii.イネーブルパスワードを入力すると、イネーブル認証はこの設定のAAAサーバを指さないため、ASAでローカルに確認されます
iii.パスワードを有効にすると、すべてのコマンドがユーザ名「enable_15」で実行され、AAAはAAAサーバまたはADにユーザ名が存在することによって、これらのコマンドを許可します

ユーザ「enable_15」が設定されると、管理者はASAの特権モードからコンフィギュレーションモードに移行できます。

管理者の動作：

```
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 ログ:

```
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'
```

注：TACACSを介したコマンド許可がASAで設定されている場合、AAAサーバに到達できない場合は、フォールバックとして「local」を設定する必要があります。
これは、認証がシリアルコンソール用に設定されていない場合でも、コマンド許可がすべてのASAセッション (シリアルコンソール、ssh、telnet) に適用されるためです。AAAサーバに到達できず、ユーザ「enable_15」がローカルデータベースにない場合、管理者は次のエラーを受け取ります。

フォールバック認証。ユーザ名「enable_15」がLOCALデータベースにない
command authorization failed

ASA ログ:

```
%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
```

> **注**：上記の設定では、コマンド許可は機能しますが、コマンドアカウンティングでは、ログインユーザの実際のユーザ名ではなく、ユーザ名「enable_15」が表示されます。これは、管理者がASAでどの特定のコマンドを実行したかを判断することが困難になります。
>
> 「enable_15」ユーザに関連するこのアカウンティング問題に対処するには、次の手順を実行します。
>
> 1. ASAのexec許可コマンドでキーワード「auto-enable」を使用する
> 2.認証されたユーザに割り当てられたTACACSシェルプロファイルで、デフォルトおよび最大特権を15に設定します

ケース 4：ASA認証、「auto-enable」を使用したexec許可、およびAAAサーバを介して設定されたコマンド許可

ASA上：

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

AAAサーバ：

許可結果：

a)シェルプロファイル

デフォルト権限：15
最大特権：15

b)コマンドセット
すべて許可

管理者の動作：

```
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 ログ:

```
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'
```

観察:

1.認証とexec許可はAAAサーバ経由で実行されます
2.認証が、認証用に設定されたコンソール接続（ssh、telnet、およびenable）に対するすべての

要求に対するユーザ権限を制御します

注：これには、ASAへのシリアル接続は含まれません

3.コマンド許可は、コマンド「aaa authorization command ISE LOCAL」を使用してAAAサーバによって実行されます
4.ユーザがAAAサーバに設定されたTACACS+クレデンシャルを使用してASAにログインすると、ユーザはAAAサーバから特権15を取得し、特権モードにログインします
5.上記の設定では、ユーザはイネーブルパスワードを入力する必要はなく、ユーザ「enable_15」はASAまたはAAAサーバで設定する必要はありません。
6. AAAサーバは、ログインユーザの実際のユーザ名から送信されたコマンド許可要求を報告します

関連情報

ASAのAAAデバイス管理に関連する参考資料を次に示します。

https://community.cisco.com/t5/security-documents/cisco-ise-device-administration-prescriptive-deployment-guide/ta-p/3738365#toc-hld--1046199281

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