# Analisi del comportamento di amministrazione dei dispositivi AAA per ASA

## Sommario



## Introduzione

In questo documento viene descritto il comportamento dell'amministrazione del dispositivo quando un'ASA è configurata per l'autenticazione e l'autorizzazione tramite un server AAA. In questo documento viene mostrato come usare Cisco Identity Service Engine (ISE) come server AAA con Active Directory come archivio identità esterno. TACACS+ è il protocollo AAA in uso.


Contributo di Dinesh Moudgil e Poonam Garg, tecnici Cisco HTTS


## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di CLI e ASDM di ASA
- Connettività tra ASA e server AAA
- Configurazione AAA su Cisco ISE per l'autenticazione e l'autorizzazione

### Componenti usati

Le informazioni di questo documento si basano sulla seguente versione del software:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

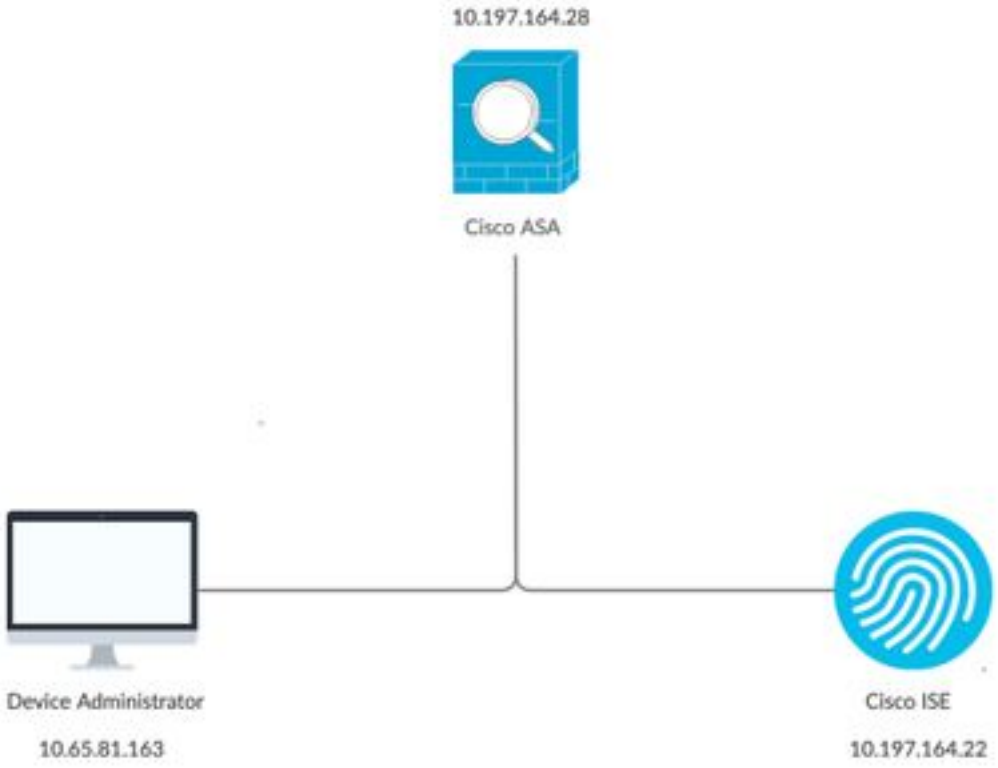
Cisco ASA supporta l'autenticazione delle sessioni amministrative tramite un database utenti locale, un server RADIUS o un server TACACS+. L'amministratore può connettersi all'appliance Cisco ASA tramite:

- Telnet
- SSH (Secure Shell)
- Connessione console seriale
- Cisco ASA Device Manager (ASDM)

Se la connessione è effettuata tramite Telnet o SSH, l'utente può riprovare a eseguire l'autenticazione tre volte in caso di errore. Dopo la terza volta, la sessione di autenticazione e la connessione all'appliance Cisco ASA vengono chiuse.

Prima di avviare la configurazione, è necessario decidere quale database utenti utilizzare (server AAA locale o esterno). Se si utilizza un server AAA esterno, come configurato in questo documento, configurare il gruppo di server AAA e l'host come descritto nelle sezioni seguenti. Per richiedere rispettivamente l'autenticazione e la verifica delle autorizzazioni quando si accede a Cisco ASA per l'amministrazione, è possibile usare i comandi di autenticazione aaa e autorizzazione aaa.

## Esempio di rete




# Configurazione

Queste sono le informazioni usate in tutti gli esempi riportati nel presente documento.

a) Configurazione ASA:

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

b) Configurazione AAA:

L'autenticazione sul server AAA viene eseguita sulla sequenza di archiviazione delle identità costituita da AD e dal database locale

## Caso 1: Autenticazione ASA configurata tramite server AAA

### Sull'appliance ASA:

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

### Sul server AAA:

Risultati autorizzazione:

a) Profilo del guscio

Privilegio predefinito: 1
Massimo privilegio: 15

b) Set di comandi
Consenti tutto

### Comportamento amministratore:

```
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
```

### Registri 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.
```

### Osservazioni:

1. L'autenticazione per la sessione SSH viene eseguita tramite il server AAA
2. L'autorizzazione viene eseguita localmente indipendentemente dal privilegio configurato sul server AAA nel risultato dell'autorizzazione
3. Dopo che l'utente è stato autenticato tramite il server AAA, quando immette la parola chiave "enable" (per impostazione predefinita non è impostata alcuna password) o la password di abilitazione (se configurata), il nome utente corrispondente utilizzato è **enable_15**

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

4. Il privilegio predefinito per la password enable è 15 a meno che non si definisca la password enable con un privilegio specifico. Ad esempio:

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

5. Se si utilizza enable con privilegi diversi, il nome utente corrispondente restituito sull'appliance ASA è **enable_x** (dove x è il privilegio)

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

## Caso 2: Autenticazione ASA e autorizzazione di esecuzione configurate tramite server AAA

### Sull'appliance ASA:

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

### Sul server AAA:

Risultati autorizzazione:

a) Profilo del guscio

Privilegio predefinito: 1
Massimo privilegio: 15

b) Set di comandi
Consenti tutto

### Comportamento amministratore:

```
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
```

### Registri 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.
```

### Osservazioni:

1. L'autenticazione e l'autorizzazione di esecuzione vengono eseguite tramite il server AAA
2. L'autorizzazione di esecuzione controlla i privilegi utente per tutte le richieste per le connessioni alla console (ssh, telnet e enable) configurate per l'autenticazione

> **Nota:** Ad eccezione della connessione seriale all'appliance ASA

3. Il server AAA è configurato in modo da fornire il privilegio predefinito 1 e il privilegio massimo di 15 come risultato dell'autorizzazione
4. Quando l'utente accede all'ASA con le credenziali TACACS+ configurate sul server AAA, inizialmente gli viene assegnato il privilegio 1 dal server AAA
5. Quando l'utente immette la parola chiave "enable", preme di nuovo "enter" (se la password di abilitazione non è configurata) o immette la password di abilitazione (se è configurata), entra nella modalità privilegiata in cui il privilegio diventa 15

## Caso 3: Autenticazione ASA, autorizzazione di esecuzione e autorizzazione dei comandi configurate tramite server AAA

### Sull'appliance ASA:

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

### Sul server AAA:

Risultati autorizzazione:

a) Profilo del guscio

Privilegio predefinito: 1
Massimo privilegio: 15

b) Set di comandi
Consenti tutto

### Comportamento amministratore:

```
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
```

## Registri 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
```

## Osservazioni:

1. L'autenticazione e l'autorizzazione di esecuzione vengono eseguite tramite il server AAA
2. L'autorizzazione di esecuzione controlla i privilegi utente per tutte le richieste per le connessioni alla console (ssh, telnet e enable) configurate per l'autenticazione
3. L'autorizzazione del comando viene eseguita dal server AAA con il comando "aaa authorization command ISE LOCAL"

**Nota:** Ad eccezione della connessione seriale all'appliance ASA

4. Quando l'utente accede all'ASA con le credenziali TACACS+ configurate sul server AAA, inizialmente gli viene assegnato il privilegio 1 dal server AAA
5. Dopo aver immesso la parola chiave "enable", aver premuto di nuovo "enter" (se la password di abilitazione non è configurata) o aver immesso la password di abilitazione (se configurata), l'utente passa alla modalità privilegiata in cui il privilegio diventa 15
6. L'autorizzazione del comando non riesce con questa configurazione perché il server AAA visualizza il comando emesso dal nome utente "enable_15" anziché dall'utente autenticato con accesso reale.
7. Qualsiasi comando eseguito su una sessione esistente avrà esito negativo anche a causa di un errore di autorizzazione del comando
8. Per risolvere questo problema, creare un utente denominato "enable_15" sul server AAA o su AD e ASA (per il fallback locale) con una password casuale

Dopo aver configurato l'utente sul server AAA o su AD, viene osservato il seguente comportamento:

i. Per l'autenticazione iniziale, il server AAA verifica il nome utente reale dell'utente connesso
ii. Dopo aver immesso la password, la verifica viene effettuata localmente sull'appliance ASA, in quanto l'autenticazione enable non punta al server AAA in questa configurazione
iii. Dopo aver abilitato la password, tutti i comandi vengono eseguiti con il nome utente "enable_15" e il server AAA consente l'esecuzione di questi comandi perché il nome utente esiste sul server AAA o su AD

Dopo aver configurato l'utente "enable_15", l'amministratore può passare dalla modalità privilegiata alla modalità di configurazione sull'appliance ASA.

## Comportamento amministratore:

```
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
```

## Registri 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:** Se l'autorizzazione del comando tramite TACACS è configurata sull'appliance ASA, è necessario usare "local" come fallback quando il server AAA non è raggiungibile.
Infatti, l'autorizzazione del comando viene applicata a tutte le sessioni ASA (console seriale, ssh, telnet) anche se l'autenticazione non è configurata per la console seriale. In questo caso, se il server AAA non è raggiungibile e l'utente "enable_15" non è presente nel database locale, l'amministratore riceve il seguente errore:

Autorizzazione di fallback. Nome utente 'enable_15' non presente nel database LOCALE
Autorizzazione del comando non riuscita

### Registri 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 configurazione precedente, l'autorizzazione dei comandi funzionerà ma l'accounting dei comandi visualizzerà comunque il nome utente "enable_15" anziché il nome utente reale dell'utente connesso. Ciò diventa difficile per gli amministratori determinare quale utente ha eseguito un determinato comando sull'appliance ASA.

Per risolvere questo problema di accounting relativo all'utente "enable_15":

1. Usare la parola chiave "**auto-enable**" nel comando di autorizzazione di esecuzione sull'appliance ASA
2. Impostare il privilegio predefinito e massimo su 15 nel profilo della shell TACACS assegnato all'utente autenticato

## Caso 4: Autenticazione ASA, autorizzazione di esecuzione con "abilitazione automatica" e autorizzazione del comando configurata tramite server AAA

### Sull'appliance ASA:

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

### Sul server AAA:

Risultati autorizzazione:

a) Profilo del guscio

Privilegio predefinito: 15
Massimo privilegio: 15

b) Set di comandi
Consenti tutto

## Comportamento amministratore:

```
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)#
```

## Registri 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'
```

## Osservazioni:

1. L'autenticazione e l'autorizzazione di esecuzione vengono eseguite tramite il server AAA
2. L'autorizzazione di esecuzione controlla i privilegi utente per tutte le richieste per le connessioni alla console (ssh, telnet e enable) configurate per l'autenticazione

**Nota:** Ad eccezione della connessione seriale all'appliance ASA

3. L'autorizzazione del comando viene eseguita dal server AAA con il comando "aaa authorization command ISE LOCAL"
4. Quando l'utente accede all'ASA con le credenziali TACACS+ configurate sul server AAA, ottiene il privilegio 15 dal server AAA e quindi accede alla modalità privilegiata
5. Con la configurazione precedente, non è necessario che l'utente immetta una password di abilitazione e non è necessario configurare l'utente "enable_15" sul server ASA o AAA.
6. Il server AAA segnalerà la richiesta di autorizzazione dei comandi proveniente dal nome utente reale dell'utente connesso

# Informazioni correlate

Di seguito sono riportati alcuni documenti di riferimento relativi all'amministrazione dei dispositivi AAA per l'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