Risoluzione dei problemi di configurazione, autenticazione e altri problemi di ASDM

Sommario

Introduzione

In questo documento viene descritto il processo di risoluzione dei problemi per la configurazione, l'autenticazione e altri problemi di Adaptive Security Appliance Device Manager (ASDM).

Introduzione

Il documento fa parte della serie di risoluzione dei problemi ASDM insieme a questi documenti:

Collegamento1<>

Collegamento2<>

Collegamento 3<>

Risoluzione dei problemi di configurazione di ASDM

Problema 1. ASDM non visualizza alcun elenco di controllo di accesso (ACL) applicato a un'interfaccia

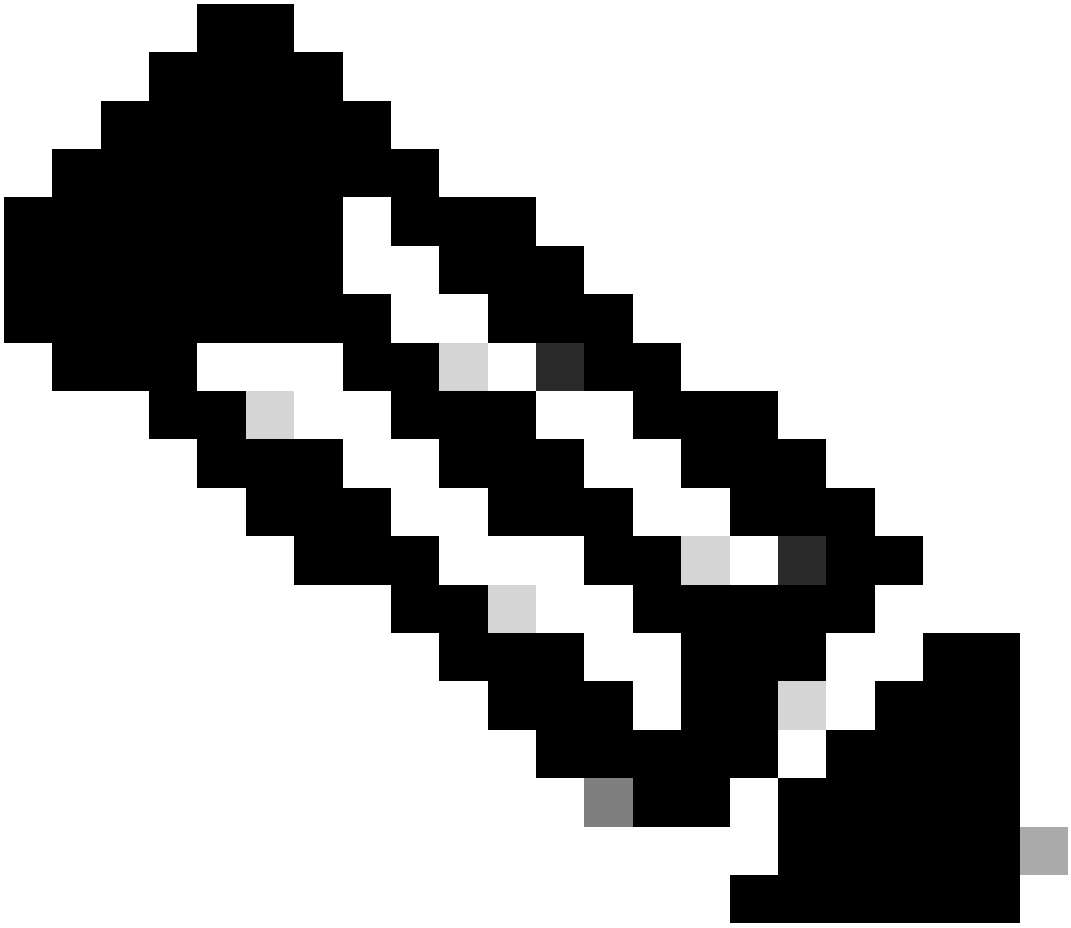
ASDM non visualizza gli elenchi di controllo di accesso (ACL) applicati a un'interfaccia, anche se all'interfaccia in questione è stato applicato un gruppo di accesso valido. Nel messaggio viene invece visualizzato "0 regole in ingresso". Questi sintomi vengono osservati negli ACL L3 e L2 entrambi configurati nella configurazione del gruppo di accesso per un'interfaccia:

<#root>

```
firewall(config)#
access-list 1 extended permit ip any

firewall(config)#
any access-list 2 extended permit udp any any

firewall(config)#
access-list 3 ethertype permit dsap bpdu


firewall(config)#
access-group 3 in interface inside

firewall(config)#
access-group 1 in interface inside

firewall(config)#
access-group 2 in interface outside
```

Risoluzione dei problemi - Azioni consigliate

Fare riferimento all'ID bug software Cisco CSCwj14147 "ASDM non riesce a caricare la configurazione del gruppo di accesso se gli ACL L2 e L3 sono misti".



Nota: Questo problema è stato risolto nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

Problema 2. Incoerenza nel numero di accessi tra la CLI di ASA e l'interfaccia utente di ASDM

Le voci di conteggio corrispondenze nell'ASDM non sono coerenti con il conteggio delle corrispondenze nell'elenco degli accessi segnalato dal comando show access-list sull'output del firewall.

Risoluzione dei problemi - Azioni consigliate

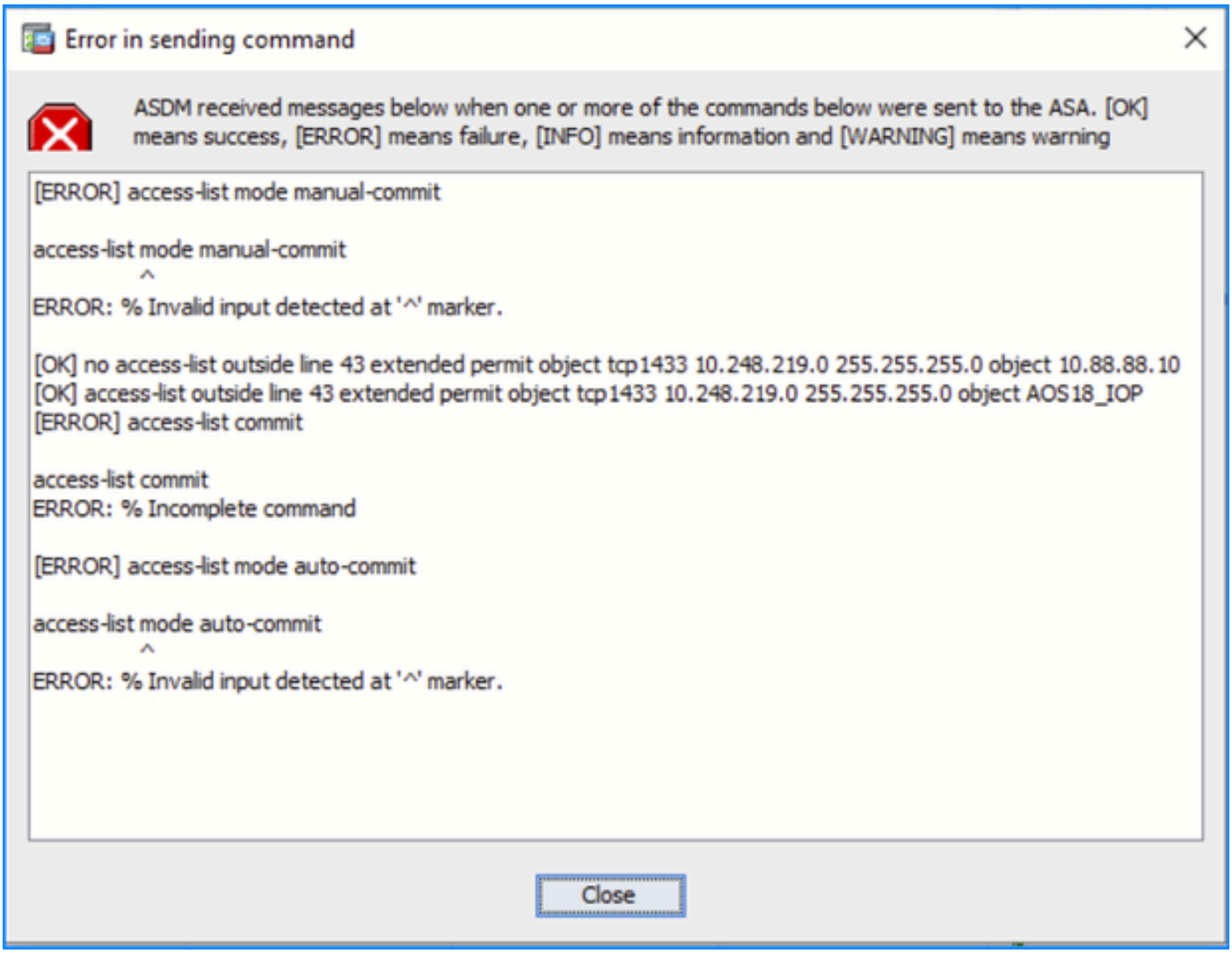
Fare riferimento all'ID bug Cisco CSCtq38377 del software "ENH: ASDM deve utilizzare il calcolo hash ACL sull'appliance ASA e non il calcolo automatico in locale" e l'ID bug Cisco CSCtq38405"ENH: L'ASA ha bisogno di un meccanismo per fornire le informazioni sull'hash

dell'ACL all'ASD"

Problema 3. "ERRORE: % Input non valido rilevato in corrispondenza del marcatore '^'." messaggio di errore durante la modifica di un ACL in ASDM

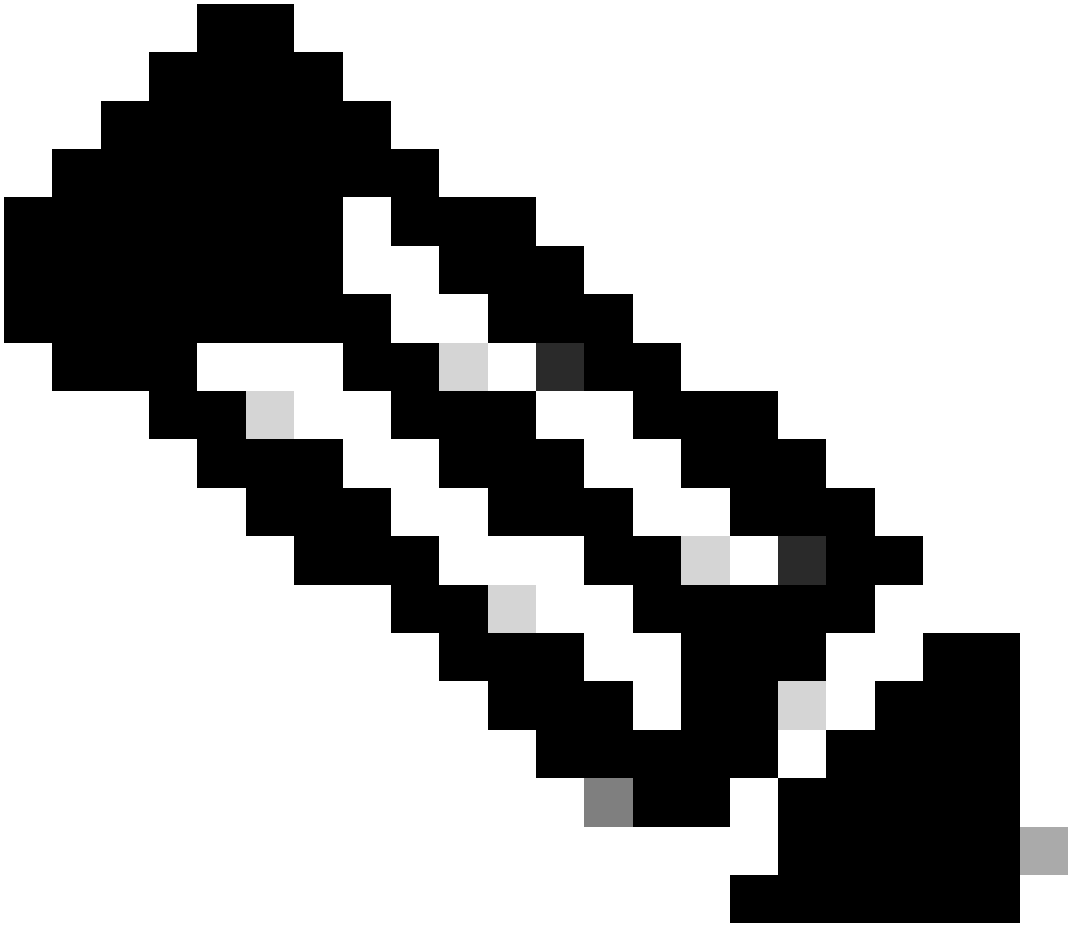
Viene visualizzato il messaggio di errore: % Input non valido rilevato in corrispondenza del marcatore '^'." Quando si modifica un ACL in ASDM, viene visualizzato il seguente messaggio di errore:

```
[ERROR] access-list mode manual-commit access-list mode manual-commit
                     ^
ERROR: % Invalid input detected at '^' marker.
[OK] no access-list ACL1 line 1 extended permit tcp object my-obj-1 object my-obj-2 eq 12345
[ERROR] access-list commit access-list commit
ERROR: % Incomplete command
[ERROR] access-list mode auto-commit access-list mode auto-commit
                     ^
ERROR: % Invalid input detected at '^' marker.
```



Risoluzione dei problemi - Azioni consigliate

Fare riferimento all'ID bug Cisco CSCvq05064 del software "Edit an entry (ACL) from ASDM fornisce un errore. Quando si usa ASDM con OpenJRE/Oracle - versione 7.12.2" e Cisco bug ID CSCvp88926 "Invio di comandi di aggiunta durante l'eliminazione dell'elenco degli accessi".



Nota: Questi problemi sono stati risolti nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

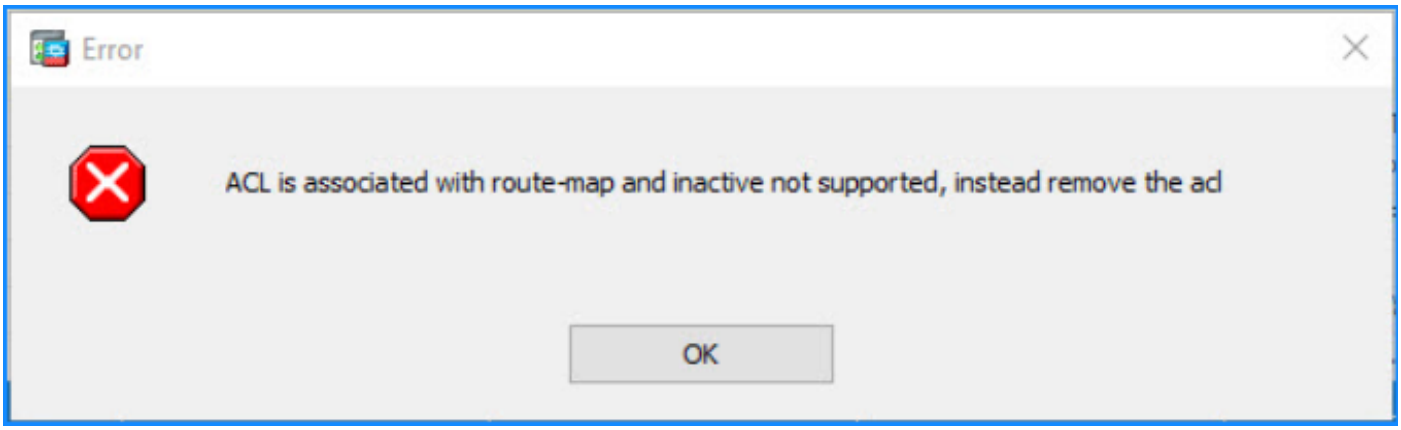
Problema 4. Viene visualizzato il messaggio di errore: ACL è associato a route-map e inattivo non supportato. Rimuovere il messaggio di errore "acl" in casi specifici

Viene visualizzato il messaggio di errore: ACL è associato a route-map e inattivo non supportato. Rimuovere il messaggio di errore "acl" viene visualizzato in uno dei seguenti casi:

1. Modificare un ACL in ASDM utilizzato in una configurazione di routing basata su criteri:

firewall (config)# access-list pbr linea 1 allow ip any host 192.0.2.1

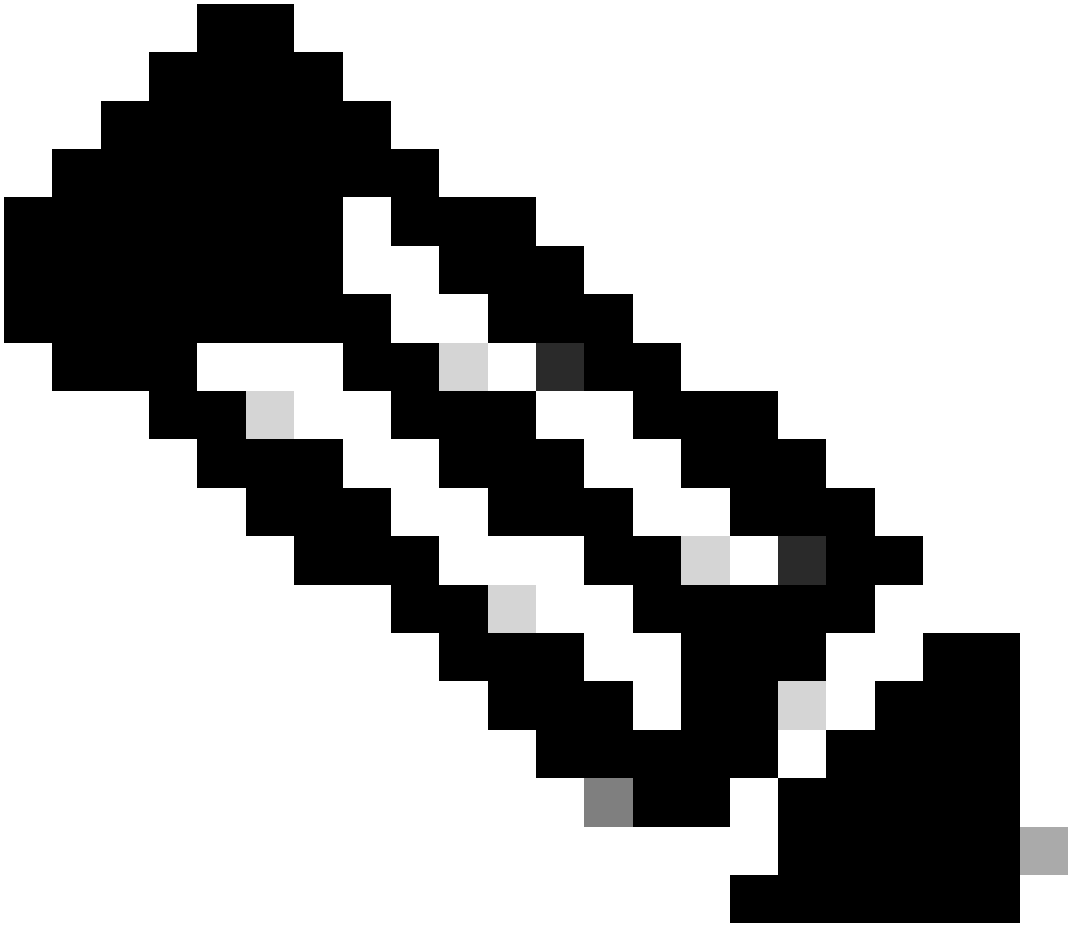
ERRORE: L'ACL è associato a route-map e non è supportato. Rimuovere l'ACL



2. Modificare un ACL ASDM > Configurazione -> VPN ad accesso remoto -> Accesso di rete (client) > Criteri di accesso dinamico

Risoluzione dei problemi - Azioni consigliate

1. Fare riferimento all'ID bug Cisco CSCwb57615 del software "Configuring pbr access-list with line number failed" (Configurazione dell'elenco degli accessi pbr con numero di riga non riuscita). Per risolvere il problema, è necessario escludere il parametro "line" dalla configurazione.
2. Fare riferimento all'ID bug Cisco CSCwe34665 del software "Unable to Edit the ACL objects if is already in use, get the exception" (Impossibile modificare gli oggetti ACL se è già in uso, recupero dell'eccezione).



Nota: Questi difetti sono stati risolti nelle recenti versioni del software ASA. Per ulteriori informazioni, controllare i dettagli del difetto.

Problema 5. Nessun log nel Visualizzatore log in tempo reale ASDM per connessioni negate in modo implicito

In ASDM Real-Time Log Viewer non vengono visualizzati i log per le connessioni negate in modo implicito.

Risoluzione dei problemi - Azioni consigliate

Il rifiuto implicito presente alla fine dell'elenco degli accessi non genera syslog. Se si desidera che tutto il traffico negato generi syslog, aggiungere la regola con la parola chiave log alla fine dell'ACL.

Problema 6. ASDM si blocca quando tenta di modificare un oggetto di rete o un object group

ASDM si blocca quando tenta di modificare un oggetto di rete o un object-group dalla scheda Indirizzi della pagina Configurazione > Firewall > Regole di accesso. Quando si verifica questo problema, l'utente non è in grado di modificare i parametri nella finestra dell'oggetto di rete.

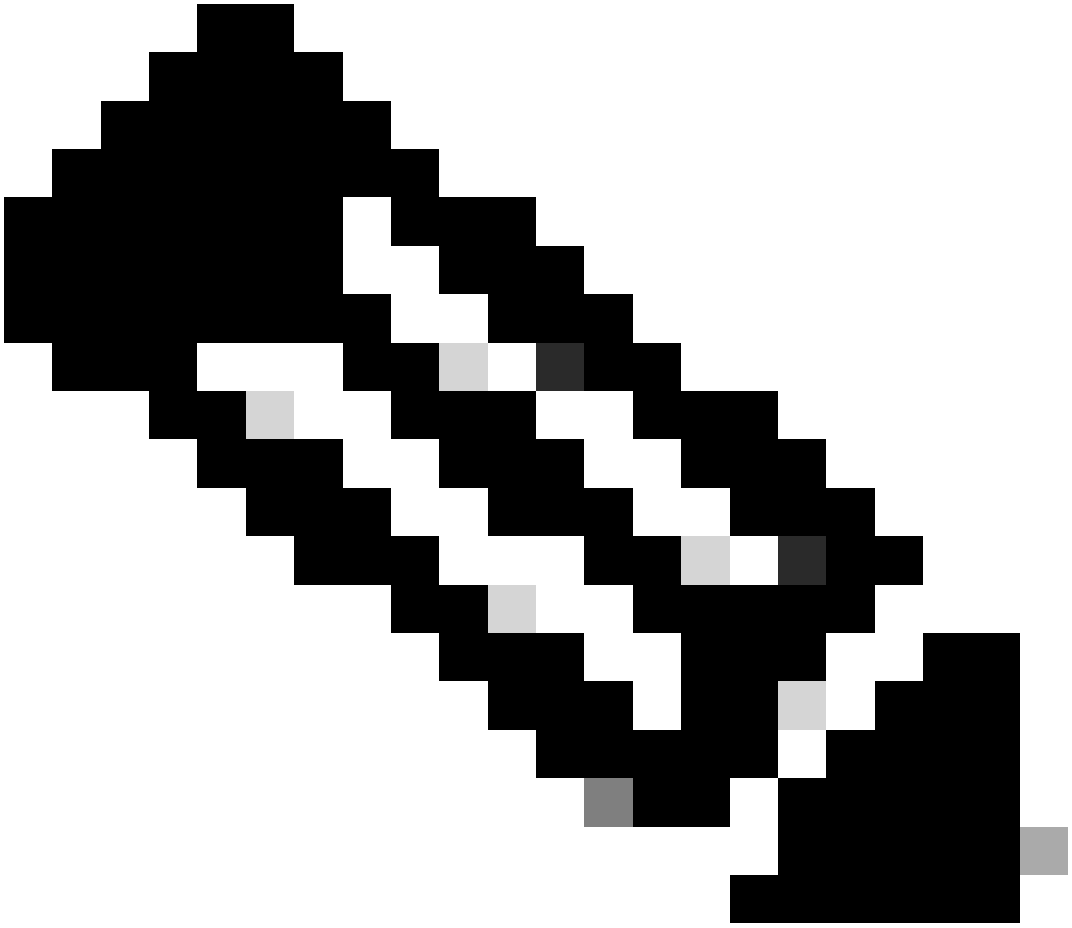
Risoluzione dei problemi - Azioni consigliate

Fare riferimento all'ID bug Cisco CSCwj12250 "ASDM si blocca quando si modificano oggetti o gruppi di oggetti di rete". Per risolvere il problema, disabilitare la raccolta di statistiche dell'host topN:

<#root>

```
ASA(config)#
```

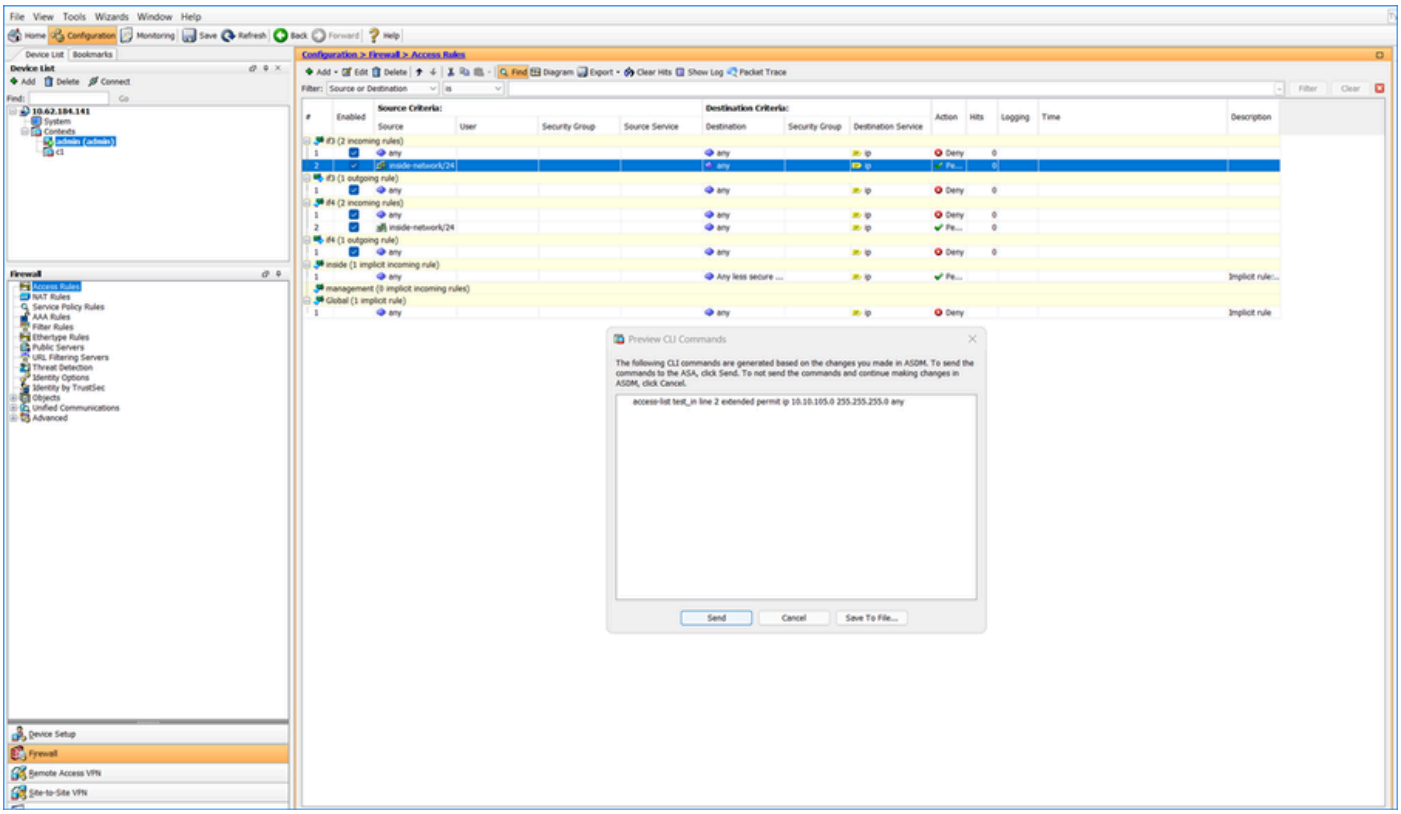
no hpm topN enable



Nota: Questo problema è stato risolto nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

Problema 7. ASDM può visualizzare regole aggiuntive della lista di controllo dell'accesso per interfacce diverse

Se si modifica un elenco di controllo di accesso a livello di interfaccia, ASDM può visualizzare regole aggiuntive per le diverse interfacce. Nell'esempio, una regola in entrata #2 è stata aggiunta all'ACL if3 dell'interfaccia. ASDM mostra anche il numero 2 per l'interfaccia if4, mentre questa regola non è stata configurata dall'utente. L'anteprima del comando mostra correttamente una singola modifica in sospeso. Problema di visualizzazione dell'interfaccia utente.



Risoluzione dei problemi - Azioni consigliate

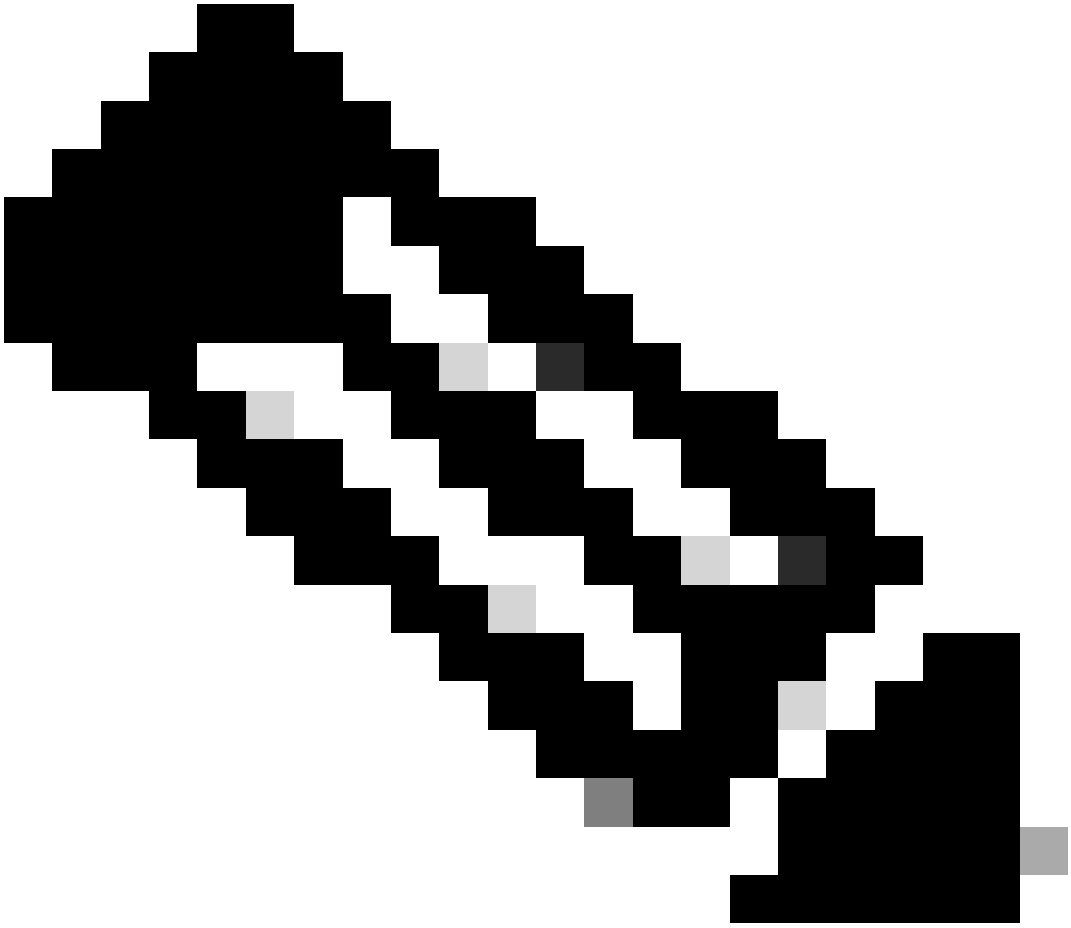
Fare riferimento all'ID bug Cisco CSCwm71434 del software "ASDM may display duplicate interface access-list entry" (ASDM può visualizzare voci duplicate dell'elenco degli accessi dell'interfaccia).

Problema 8. I log in tempo reale non sono disponibili nel Visualizzatore log in tempo reale

Nessun log visualizzato nel Visualizzatore log in tempo reale

Risoluzione dei problemi - Azioni consigliate

1. Verificare che la registrazione sia configurata. Fare riferimento al registro 1 di ASDM: Guida alla configurazione ASDM delle operazioni generali della serie Cisco ASA, 7.22, capitolo: Registrazione.
2. Fare riferimento all'ID bug Cisco CSCvf82966 "ASDM - Logging: Unable to View Real-Time logs" (Impossibile visualizzare i log in tempo reale).

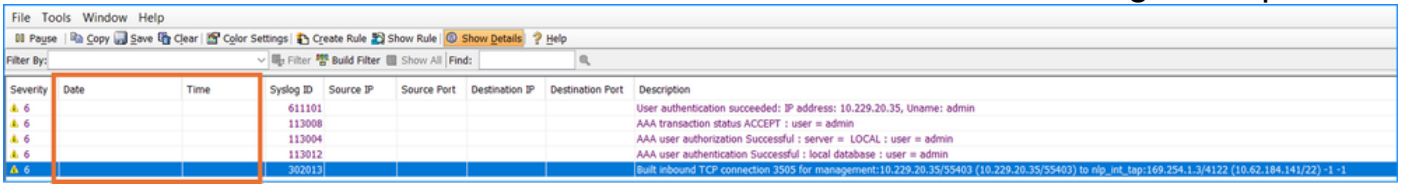


Nota: Questo problema è stato risolto nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

Riferimenti

- ASDM Book 1: Guida alla configurazione ASDM delle operazioni generali della serie Cisco ASA, 7.22, capitolo: Registrazione.

Problema 9. Le colonne Data e Ora sono vuote nel Visualizzatore log in tempo reale



Risoluzione dei problemi - Azioni consigliate

1. Verificare se viene utilizzato il formato timestamp di registrazione RFC5424:

```
<#root>

#

show run logging


logging enable

logging timestamp rfc5424
```

2. Se si usa il formato timestamp di registrazione RFC5424, fare riferimento all'ID bug software Cisco CSCvs52212 "ASDM ENH: per il visualizzatore del log degli eventi, di visualizzare i syslog ASA con il formato timestamp rfc5424". Per ovviare al problema, evitare di utilizzare il formato RFC5424:

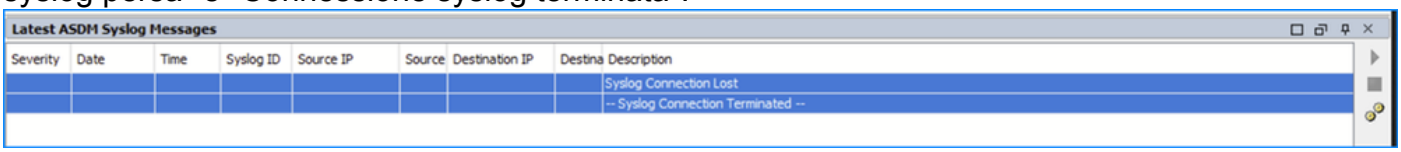
```
<#root>

firewall(config)#

no logging timestamp rfc5424


firewall(config)#

logging timestamp
```

3. Inoltre, fare riferimento all'ID bug Cisco CSCwh70323 "Voce di timestamp mancante per alcuni messaggi syslog inviati al server syslog".

Nota: Questo problema è stato risolto nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

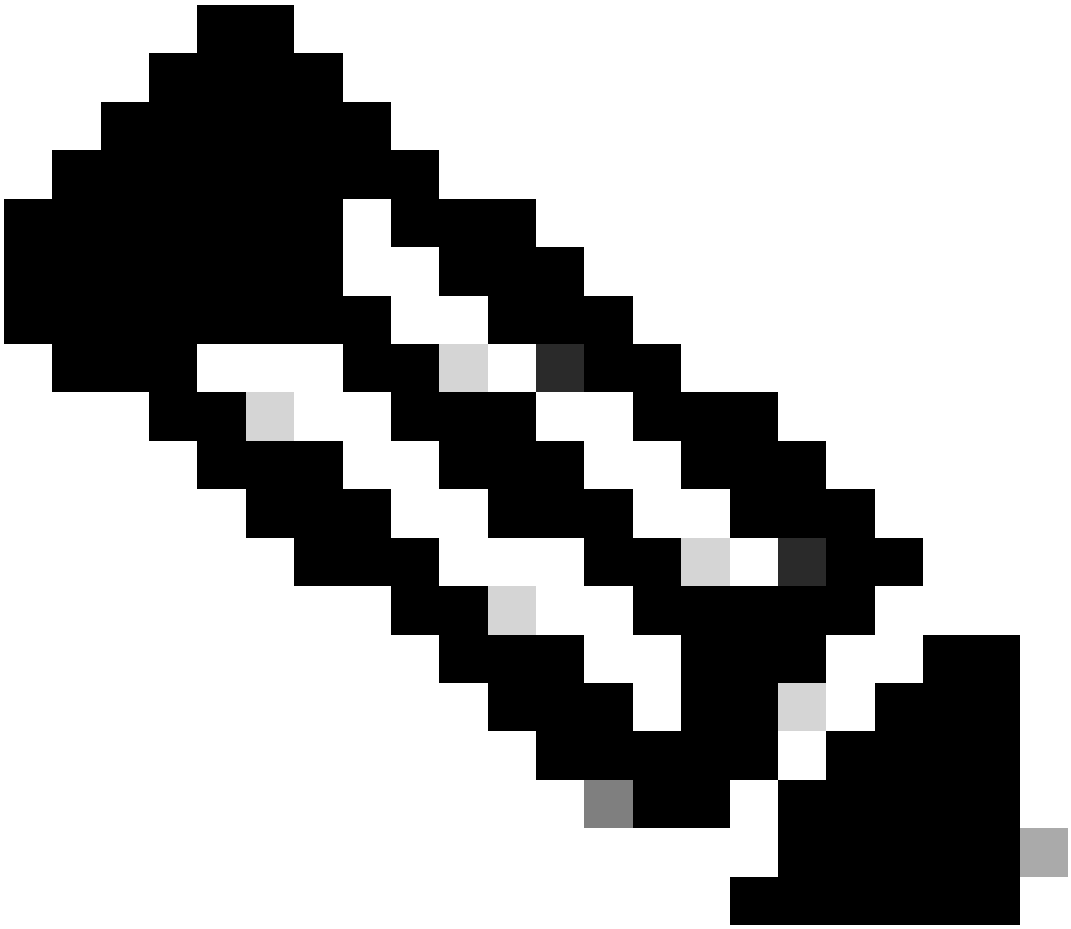
Problema 10. Il log su ASDM può avere esito negativo dopo il passaggio a un contesto diverso in un'appliance ASA multi-contesto

La scheda Ultimi messaggi di syslog ASDM nella home page visualizza i messaggi "Connessione syslog persa" e "Connessione syslog terminata":



Risoluzione dei problemi - Azioni consigliate

Verificare che la registrazione sia configurata. Fare riferimento all'ID bug Cisco CSCvz15404 "ASA: Modalità contesto multiplo: Quando si passa a un contesto diverso, il log ASDM si interrompe".



Nota: Questo problema è stato risolto nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

Problema 11. La sessione ASDM viene interrotta improvvisamente quando si passa da un contesto all'altro

La sessione ASDM viene interrotta improvvisamente quando si passa da un contesto all'altro e viene visualizzato il messaggio di errore "The maximum number of management session for protocol http or user already existing. Riprova più tardi". Nei messaggi syslog vengono visualizzati i seguenti log:

```
%ASA-3-768004: QUOTA: management session quota exceeded for http protocol: current 5, protocol limit 5

%ASA-3-768004: QUOTA: management session quota exceeded for http protocol: current 5, protocol limit 5
```

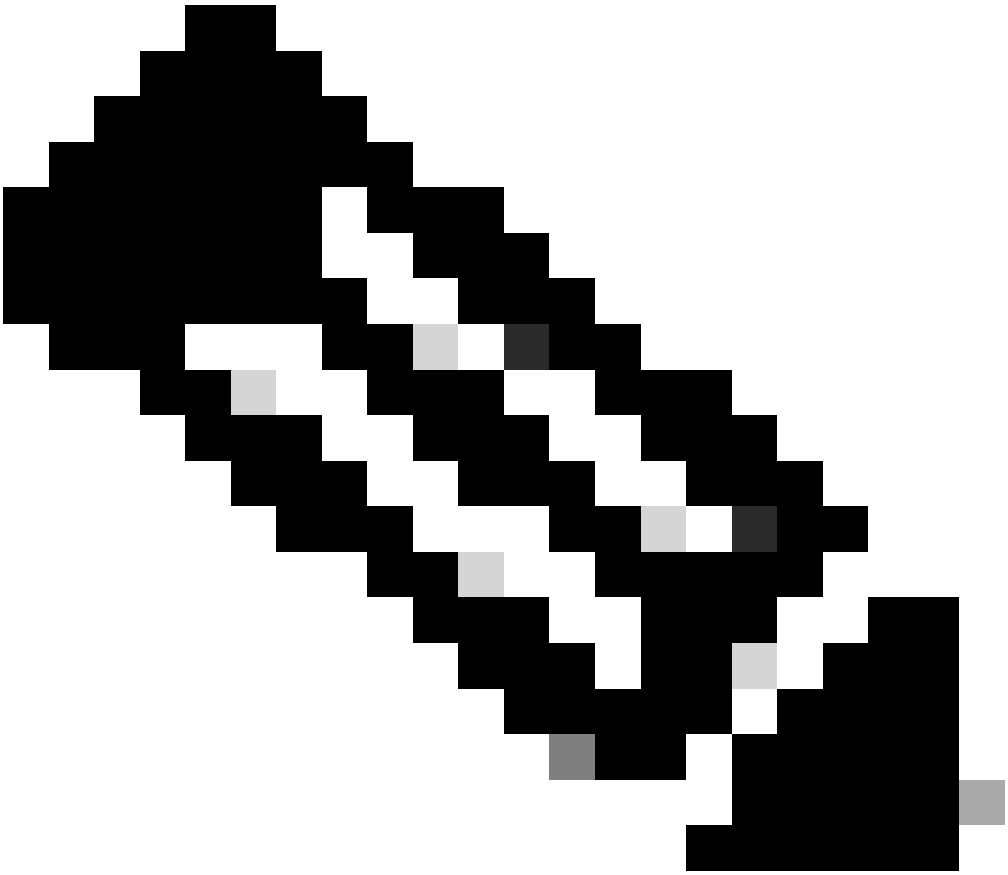
Risoluzione dei problemi - Azioni consigliate

1. Verificare se l'utilizzo corrente delle risorse ASDM ha raggiunto il limite. In questo caso, il contatore Rifiutato aumenta:

<#root>

```
firewall #

show resource usage resource ASDM


Resource                Current        Peak      Limit        Denied Context
ASDM

5

           5

5


10

 admin
```

2. Fare riferimento all'ID bug Cisco CSCvs72378 del software "ASDM session ying abrupently terminated when switching between difference contContext".



Nota: Questo problema è stato risolto nelle recenti versioni del software ASA. Per ulteriori informazioni, controllare i dettagli del difetto.

3. Se la versione software contiene la correzione per l'ID bug Cisco CSCvs72378 e la risorsa corrente ha raggiunto il limite, disconnettere alcune sessioni ASDM esistenti. È possibile chiudere ASDM o, in alternativa, cancellare le connessioni HTTPS per l'indirizzo IP dell'host che esegue ASDM. Nell'esempio si presume che il server HTTP su ASDM venga eseguito sulla porta HTTPS 443 predefinita:

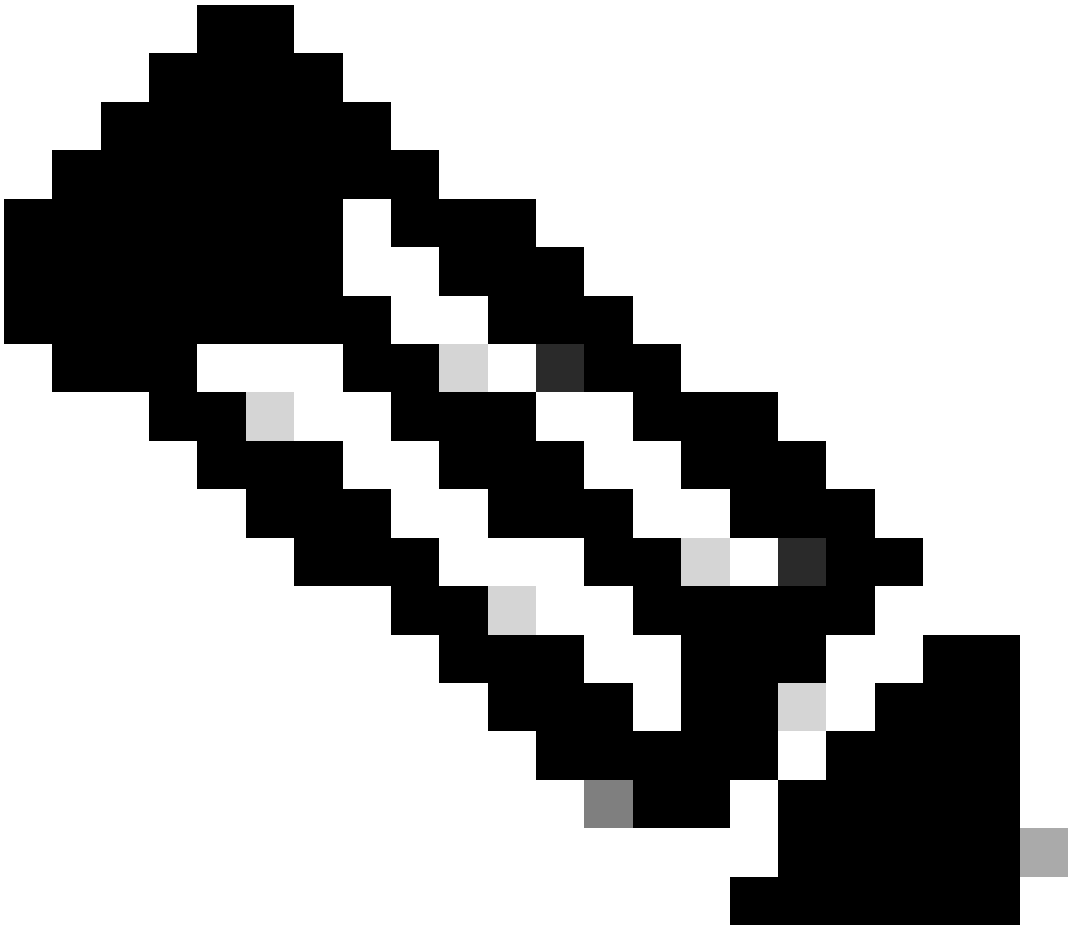
```
<#root>

#

show conn all protocol tcp port 443


TCP management  192.0.2.35:55281 NP Identity Ifc  192.0.2.1:443, idle 0:00:01, bytes 33634, flags UOB
TCP management  192.0.2.36:38844 NP Identity Ifc  192.0.2.1:443, idle 0:00:08, bytes 1629669, flags UOB
#

clear conn all protocol tcp port 443 address 192.0.2.35
```

Problema 12. ASDM esce/termina in modo casuale con il messaggio "ASDM ha ricevuto un messaggio dal dispositivo ASA da disconnettere. ASDM verrà chiuso."

Sull'appliance ASA multi-contesto, ASDM esce/termina in modo casuale con il messaggio "ASDM ha ricevuto un messaggio dal dispositivo ASA per la disconnessione. ASDM verrà chiuso.".

Risoluzione dei problemi - Azioni consigliate

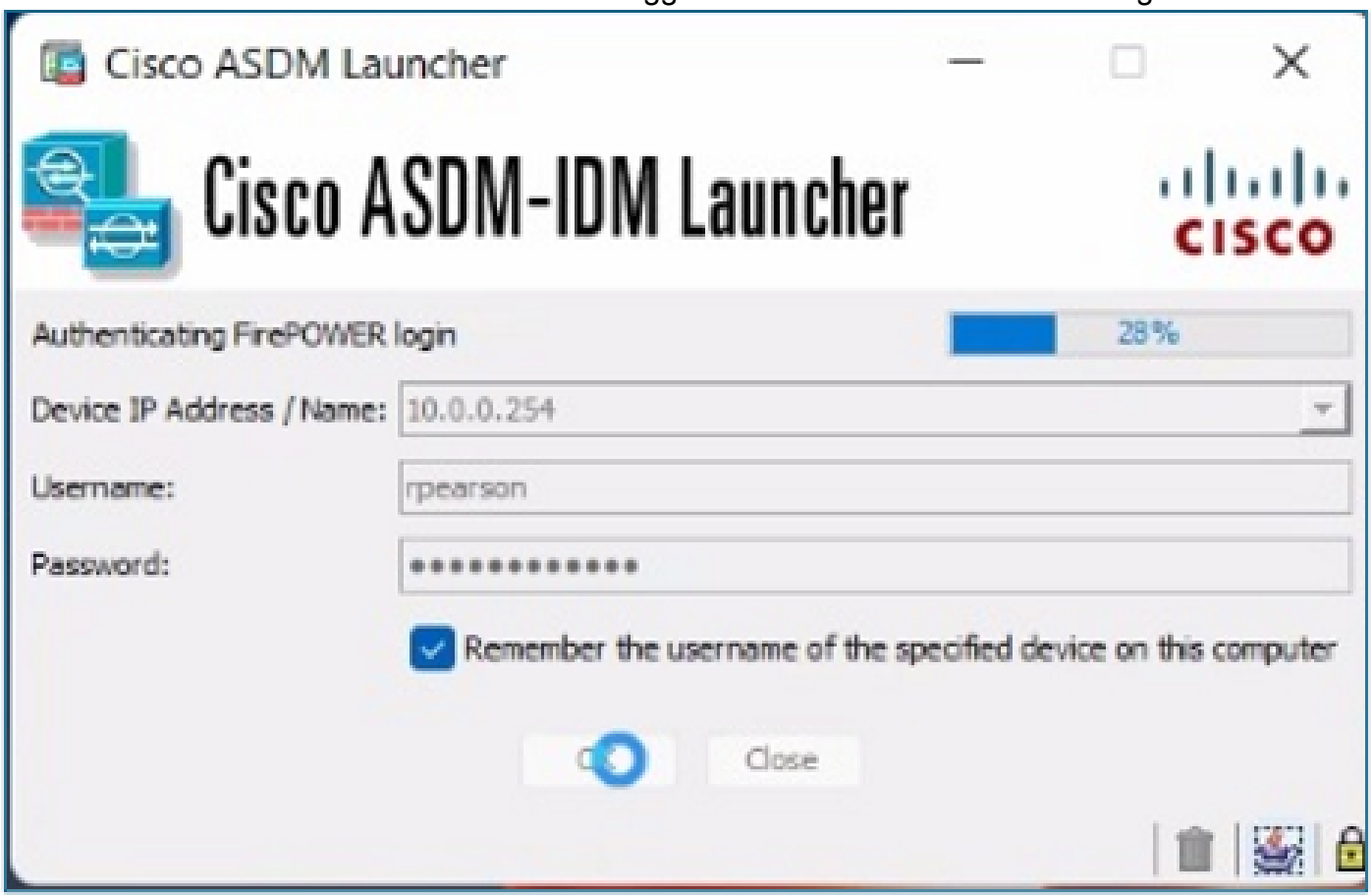
Fare riferimento all'ID bug Cisco CSCwh04395 "ASDM application random exits/terminates with an alert message on multi-context setup" (L'applicazione ASDM esce/termina in modo casuale con un messaggio di avviso sull'installazione in più contesti).



Nota: Questo problema è stato risolto nelle recenti versioni del software ASA. Per ulteriori informazioni, controllare i dettagli del difetto.

Problema 13. Il caricamento ASDM si blocca con il messaggio "Authentication FirePOWER login"

Il caricamento di ASDM si blocca con il messaggio "Authentication FirePOWER login":



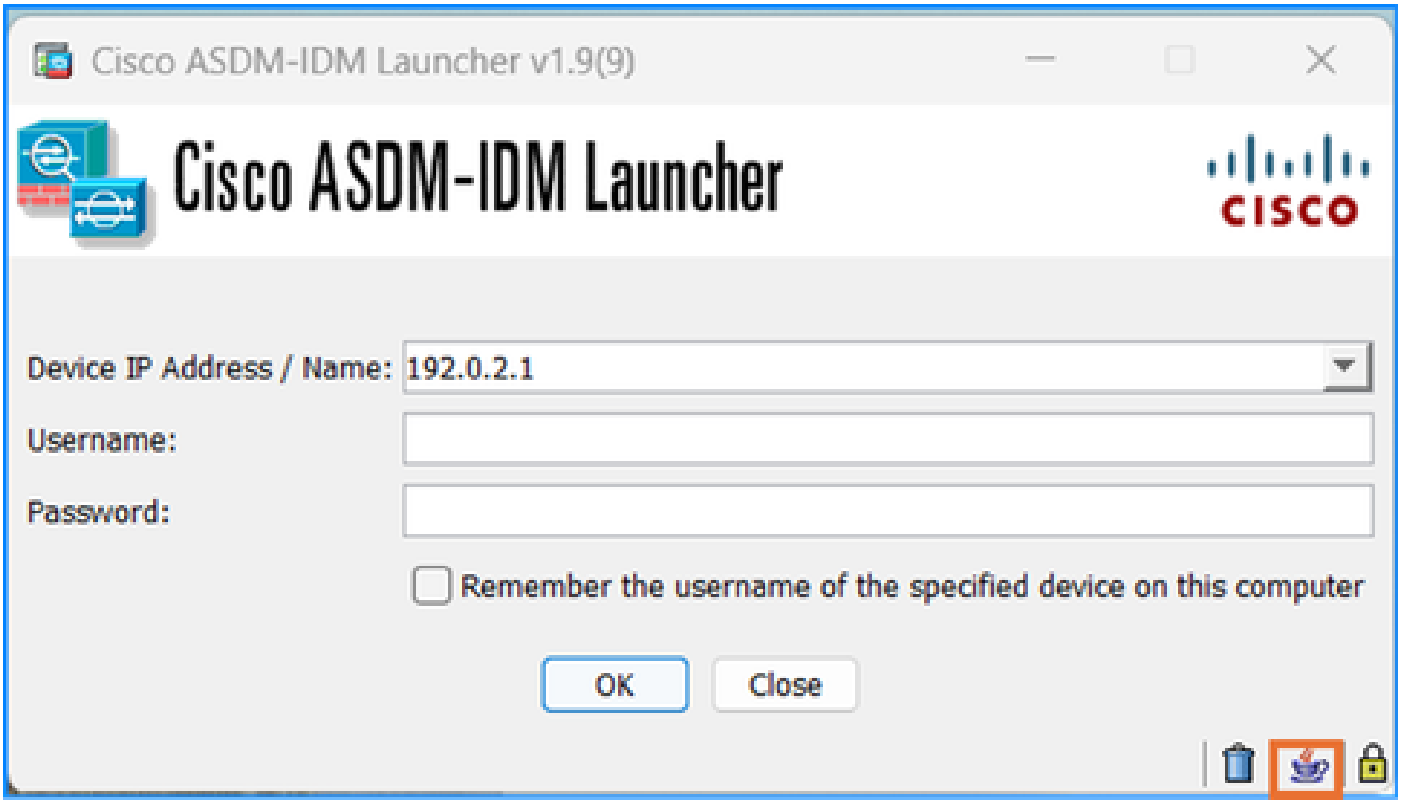
Nei log della console Java viene visualizzato il messaggio "Impossibile connettersi a FirePower, continuare senza":

<#root>

```
2023-05-08 16:55:10,564 [ERROR] CLI-PASSTHROUGH-DEBUG Inside doInitialProcessing:
0 [SGZ Loader: launchSgzApplet] ERROR com.cisco.pdm.headless.startup  - CLI-PASSTHROUGH-DEBUG Inside do
CLI-PASSTHROUGH-DEBUG Inside doInitialProcessing:
2023-05-08 16:55:10,657 [ERROR] CLI-PASSTHROUGH-DEBUG Inside doInitialProcessing messenger: cpl@18c4cb7
93 [SGZ Loader: launchSgzApplet] ERROR com.cisco.pdm.headless.startup  - CLI-PASSTHROUGH-DEBUG Inside d
CLI-PASSTHROUGH-DEBUG Inside doInitialProcessing messenger: cpl@18c4cb75
com.jidesoft.plaf.LookAndFeelFactory not loaded.
2023-05-08 17:15:31,419 [ERROR]  Unable to login to DC-Lite. STATUS CODE IS 502
1220855 [SGZ Loader: launchSgzApplet] ERROR com.cisco.dmcommon.util.DMCommonEnv  -  Unable to login to
May 08, 2023 10:15:31 PM vd cx

INFO: Failed to connect to FirePower, continuing without it.
May 08, 2023 10:15:31 PM vd cx
INFO: If the FirePower is NATed, clear the cache (C:/Users/user1/.asdm/data/firepower.conf) and try agai
Env.isAsdmInHeadlessMode()------------->false
java.lang.InterruptedException
```

```
        at java.lang.Object.wait(Native Method)
```

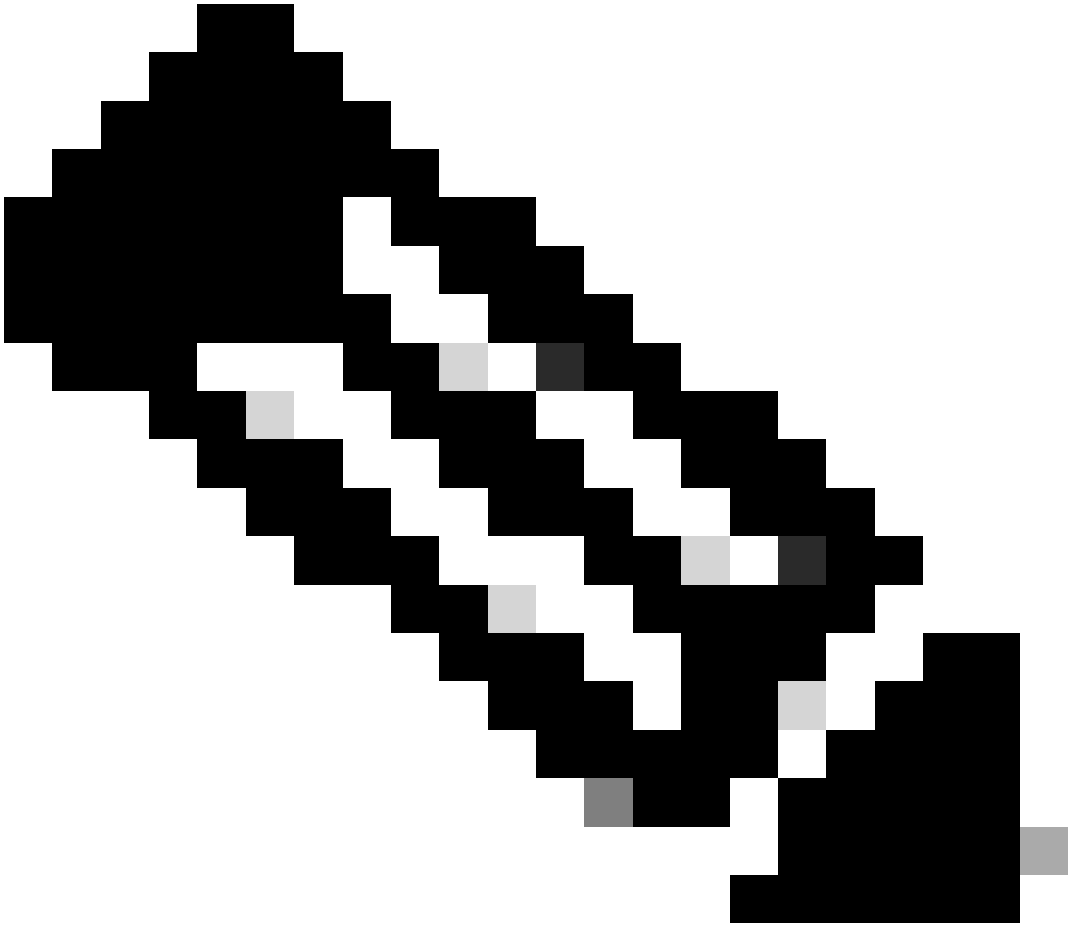
Per verificare questo sintomo, abilitare i log della console Java:



Risoluzione dei problemi - Azioni consigliate

Fare riferimento all'ID bug Cisco CSCwe15164 "ASA: ASDM non può visualizzare le schede SFR fino a quando non è "riattivata" dalla CLI." Fasi della soluzione:

1. Chiudere ASDM Manager.
2. Ottenere l'accesso SSH a SFR e passare dall'utente alla directory principale (sudo su).
3. Dopo aver eseguito la procedura descritta sopra, riavviare nuovamente l'ASDM e caricare le schede Firepower (SFR).



Nota: Questo problema è stato risolto nelle recenti versioni del software Firepower. Per ulteriori informazioni, controllare i dettagli del difetto.

Problema 14. ASDM non mostra la gestione/configurazione del modulo Firepower

La configurazione del modulo Firepower non è disponibile su ASDM.

Risoluzione dei problemi - Azioni consigliate

1. Verificare che le versioni ASA, ASDM, Firepower module e del sistema operativo siano compatibili. Fare riferimento alle note di rilascio di Cisco Secure Firewall ASA, note di rilascio di Cisco Secure Firewall ASDM, compatibilità di Cisco Secure Firewall ASA:

- ASA 9.14/ASDM 7.14/Firepower 6.6 è la versione finale del modulo ASA FirePOWER su ASA 5525-X, 5545-X e 5555-X.

- ASA 9.12/ASDM 7.12/Firepower 6.4.0 è la versione finale del modulo ASA FirePOWER sulle appliance ASA 5515-X e 5585-X.
- ASA 9.9/ASDM 7.9(2)/Firepower 6.2.3 è la versione finale del modulo ASA FirePOWER sulle appliance ASA serie 5506-X e 5512-X.
- Le versioni ASDM sono compatibili con tutte le versioni ASA precedenti, a meno che non sia specificato diversamente. Ad esempio, ASDM 7.13(1) può gestire un'ASA 5516-X su ASA 9.10(1).
- ASDM non è supportato per la gestione dei moduli FirePOWER con ASA 9.8(4.45)+, 9.12(4.50)+, 9.14(4.14)+ e 9.16(3.19)+; è necessario utilizzare FMC per gestire il modulo con queste versioni. Queste versioni ASA richiedono ASDM 7.18(1.152) o versioni successive, ma il supporto ASDM per il modulo ASA FirePOWER è terminato con 7.16.
- ASDM 7.13(1) e ASDM 7.14(1) non supportano ASA 5512-X, 5515-X, 5585-X e ASASM; per ripristinare il supporto ASDM, è necessario eseguire l'aggiornamento a ASDM 7.13(1.101) o 7.14(1.48).

2. Se le versioni sono compatibili, verificare che il modulo sia attivo e in esecuzione:

<#root>

```
firewall#

show module sfr details


Getting details from the Service Module, please wait...

Card Type:          FirePOWER Services Software Module
Model:              ASA5508
Hardware version:   N/A
Serial Number:      AAAABBBB1111
Firmware version:   N/A
Software version:   7.0.6-236
MAC Address Range:  006b.f18e.dac6 to 006b.f18e.dac6
App. name:          ASA FirePOWER

App. Status:        Up


App. Status Desc:   Normal Operation
App. version:       7.0.6-236

Data Plane Status:  Up



Console session:    Ready



Status:             Up


DC addr:            No DC Configured
Mgmt IP addr:       192.0.2.1
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.0.2.254
Mgmt web ports:     443
Mgmt TLS enabled:   true
```

Se il modulo non è attivo, è possibile usare il comando sw-module reset per reimpostare il modulo e quindi ricaricare il software del modulo.

Riferimenti

- Note sulla release di Cisco Secure Firewall ASA
- Note sulla release di Cisco Secure Firewall ASDM
- Compatibilità ASA Cisco Secure Firewall

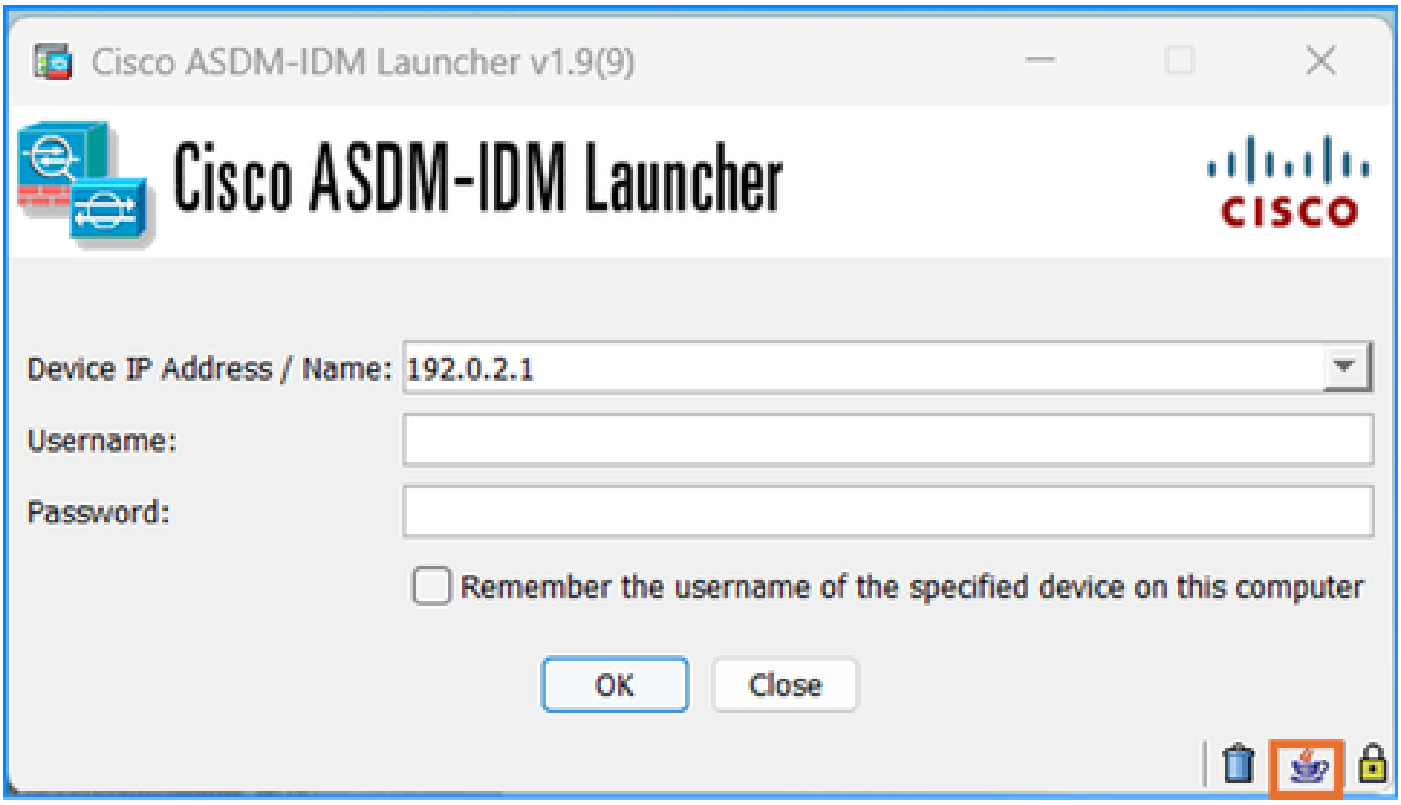
Problema 15. I profili client sicuri non sono accessibili su ASDM

Nei log della console Java viene visualizzata l'eccezione "java.lang.ArrayIndexOutOfBoundsException: Messaggio di errore 3":

<#root>

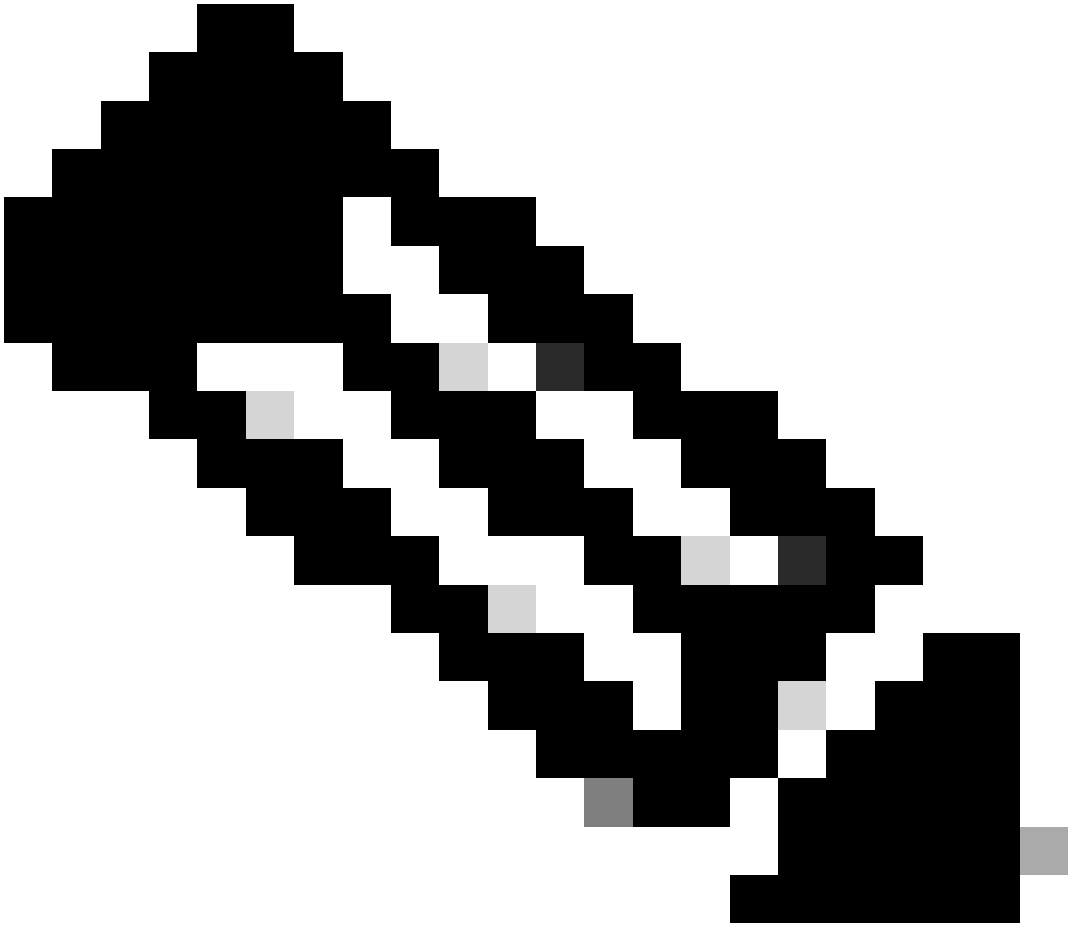
```
LifeTime value : -1 HTTP Enable Status : nps-servers-ige

java.lang.ArrayIndexOutOfBoundsException: 3


   at doz.a(doz.java:1256)
   at doz.a(doz.java:935)
   at doz.l(doz.java:1100)
```

Per verificare questo sintomo, abilitare i log della console Java:



Risoluzione dei problemi - Azioni consigliate

Fare riferimento all'ID bug Cisco CSCwi56155 del software "Unable to access Secure Client Profile on ASDM" (Impossibile accedere a Secure Client Profile su ASDM).



Nota: Questo problema è stato risolto nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

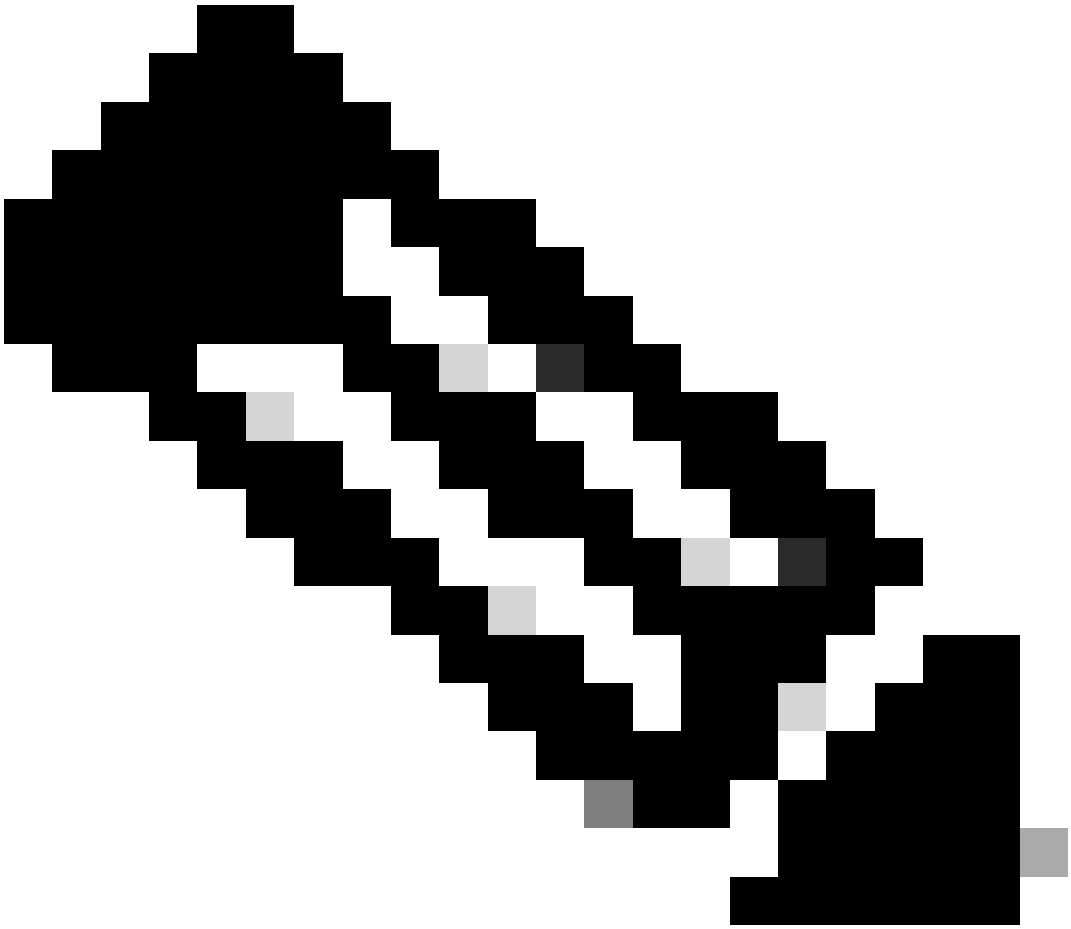
Problema 16. Impossibile modificare i profili XML Secure Client Profile in ASDM

I profili XML Secure Client Profile in ASDM Configuration > Remote Access VPN > Network (Client) Access non possono essere modificati su un dispositivo ASA se sul disco è presente un'immagine AnyConnect precedente alla versione 4.8.

Viene visualizzato il messaggio di errore "Non è presente alcun plug-in dell'editor di profili nell'immagine client sicura sul dispositivo. Accedere alla rete (Client) > Secure Client Software e installare Secure Client Image versione 2.5 o successiva, quindi riprovare".

Risoluzione dei problemi - Azioni consigliate

Fare riferimento all'ID bug Cisco CSCwk64399 "ASDM-Unable to edit Secure Client Profile" (ASDM - impossibile modificare il profilo client sicuro). Per risolvere il problema, impostare un'altra immagine AnyConnect con una priorità inferiore.



Nota: Questo problema è stato risolto nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

Problema 17. Immagini client protette mancanti dopo le modifiche alla configurazione

Dopo aver apportato modifiche in Configurazione ASDM > Accesso di rete (client) > Profilo client protetto, le immagini in Configurazione > Accesso di rete (client) > Software client protetto risultano mancanti.

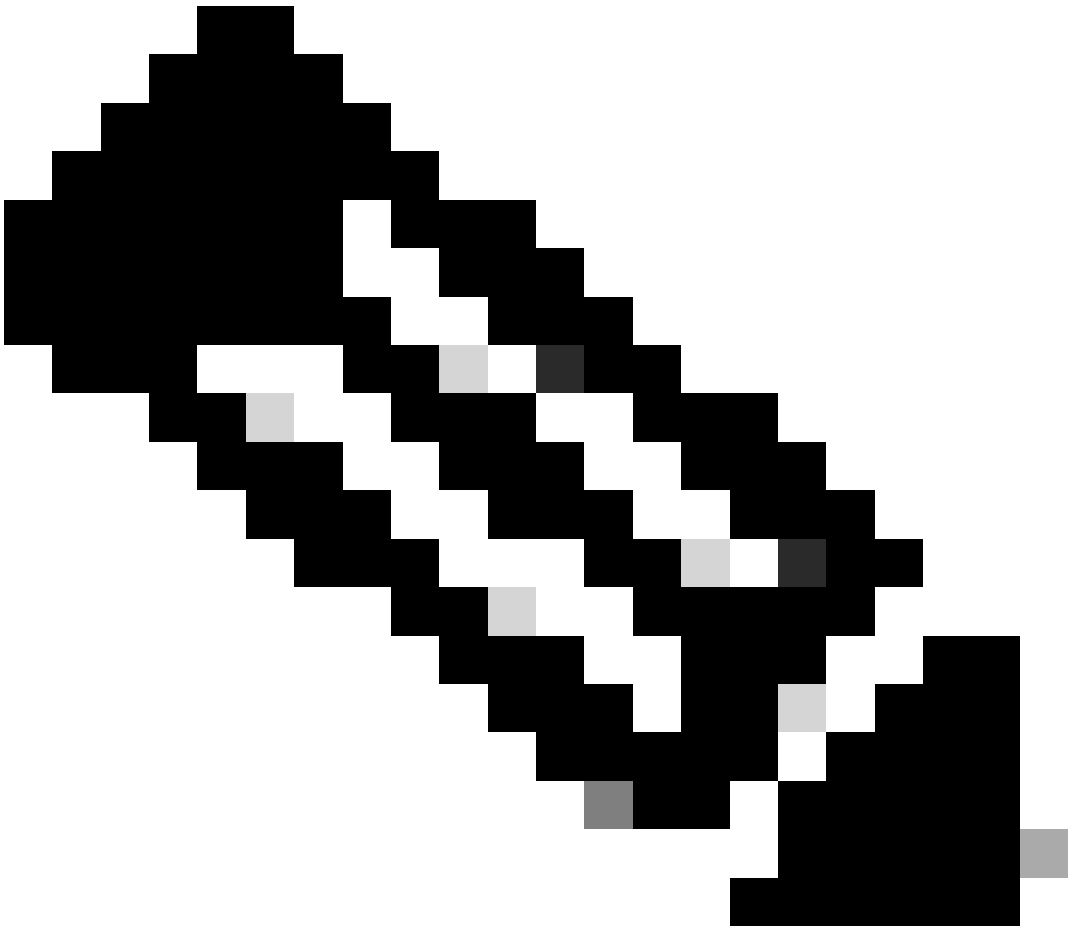
Risoluzione dei problemi - Azioni consigliate

Fare riferimento all'ID bug Cisco CSCwf23826 "Secure Client Software is not display after modifying the Secure Client Profile Editor in ASDM" (Il software Secure Client Software non viene visualizzato dopo aver modificato Secure Client Profile Editor in ASDM). Le opzioni per la soluzione alternativa:

- Fare clic sull'icona Aggiorna in ASDM

O

- Chiudere e riaprire ASDM



Nota: Questo problema è stato risolto nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

Problema 18. Comandi session-timeout e idle-timeout del server http inefficaci

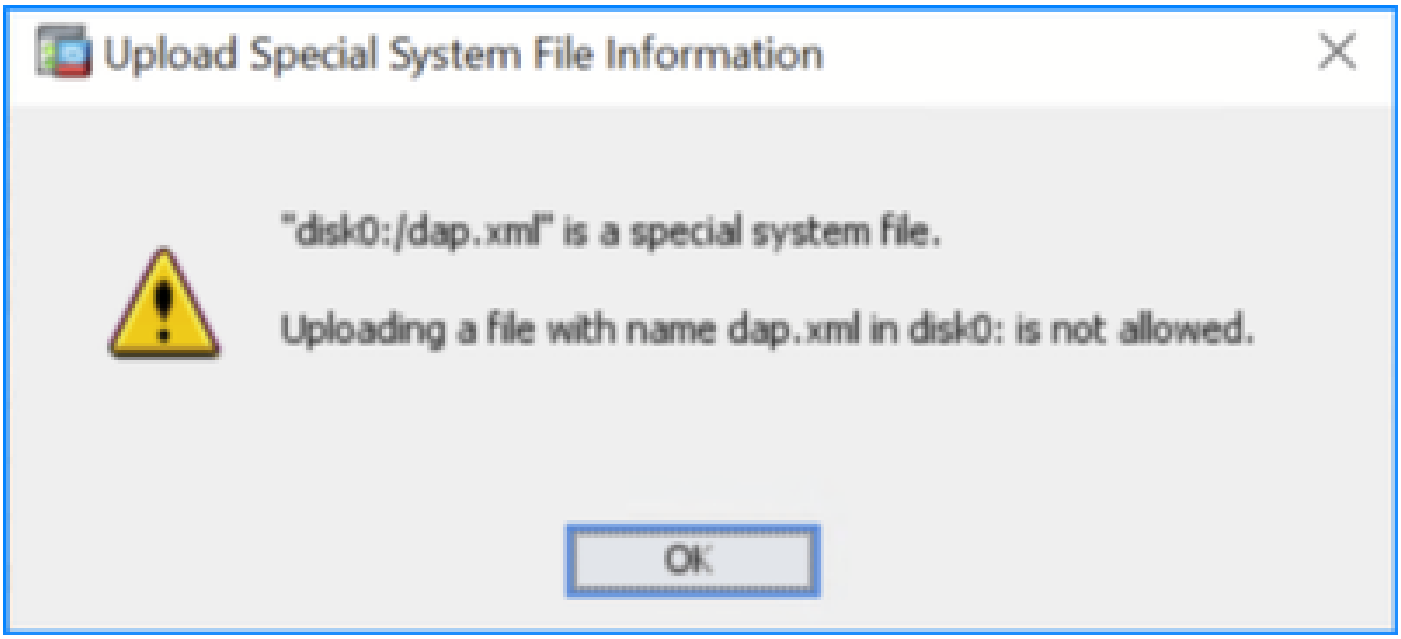
I comandi http server session-timeout e http server idle-timeout non hanno alcun effetto nella modalità multi-contesto dell'ASA.

Risoluzione dei problemi - Azioni consigliate

Fare riferimento all'ID bug Cisco CSCtx41707 software "Support for http server timeout command in multi-context mode" (Supporto per il comando di timeout del server http in modalità multi-contesto). I comandi sono configurabili, ma non hanno alcun effetto.

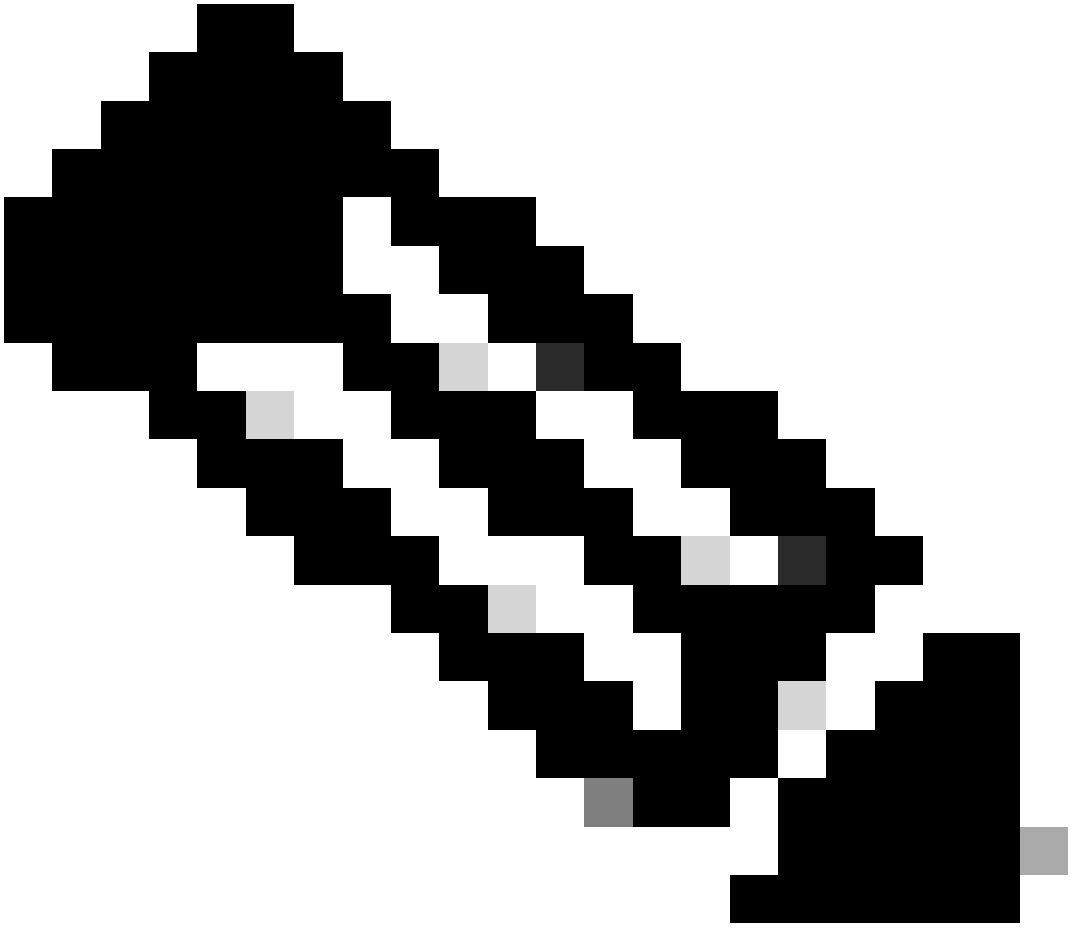
Problema 19. Errore di copia di Dap.xml su ASDM

La copia di dap.xml su ASA tramite la finestra Gestione file in ASDM ha esito negativo con l'errore "disk0:/dap.xml è un file di sistema speciale. Caricamento di un file denominato dap.xml in disco0: non è consentito":



Risoluzione dei problemi - Azioni consigliate

Fare riferimento all'ID bug software Cisco CSCvt62162 "Cannot copy dap.xml using File Management in ASDM 7.13.1" (Impossibile copiare il file dap.xml utilizzando Gestione file in ASDM 7.13.1). Per ovviare al problema, è possibile copiare il file direttamente sull'appliance ASA utilizzando protocolli come FTP o TFTP.



Nota: Questo problema è stato risolto nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

Problema 20. I criteri IKE e le proposte IPSEC non sono visibili su ASDM

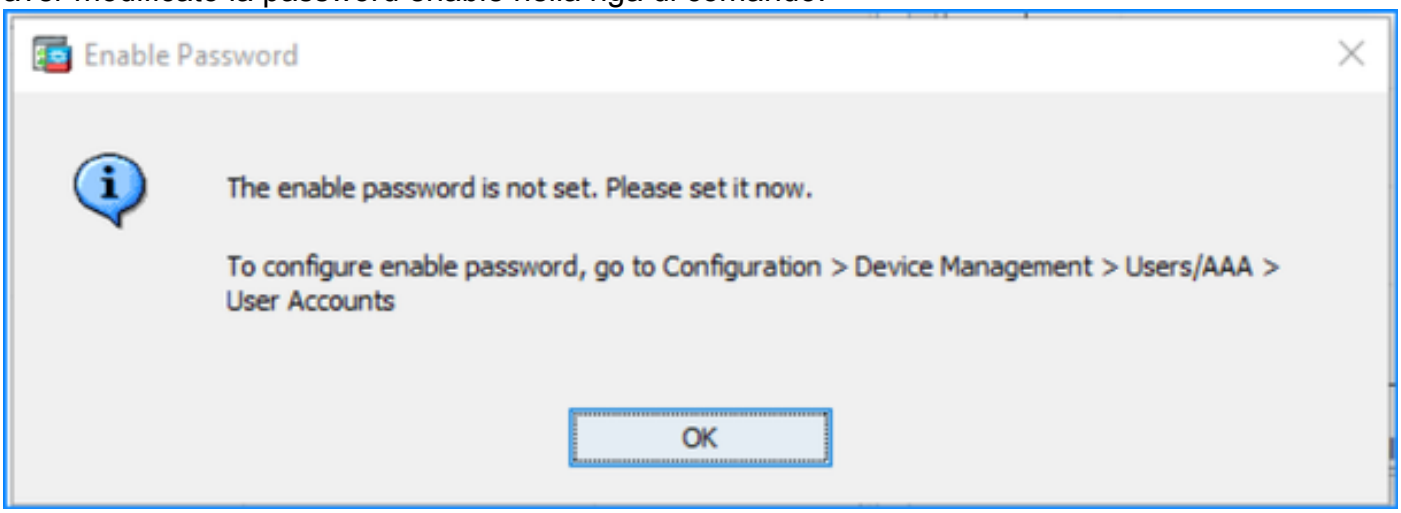
ASDM non visualizza i criteri IKE e le proposte IPSEC nella finestra Configurazioni > VPN da sito a sito.

Risoluzione dei problemi - Azioni consigliate

Fare riferimento all'ID bug Cisco CSCwm42701 "ASDM display blank in IKE policies and IPSEC PROPOSALS tab" (informazioni in lingua inglese).

Problema 21. ASDM visualizza il messaggio "The enable password is not set. Per favore, impostalo ora."

ASDM visualizza il messaggio "The enable password is not set. Per favore, impostalo ora." dopo aver modificato la password enable nella riga di comando:



Risoluzione dei problemi - Azioni consigliate

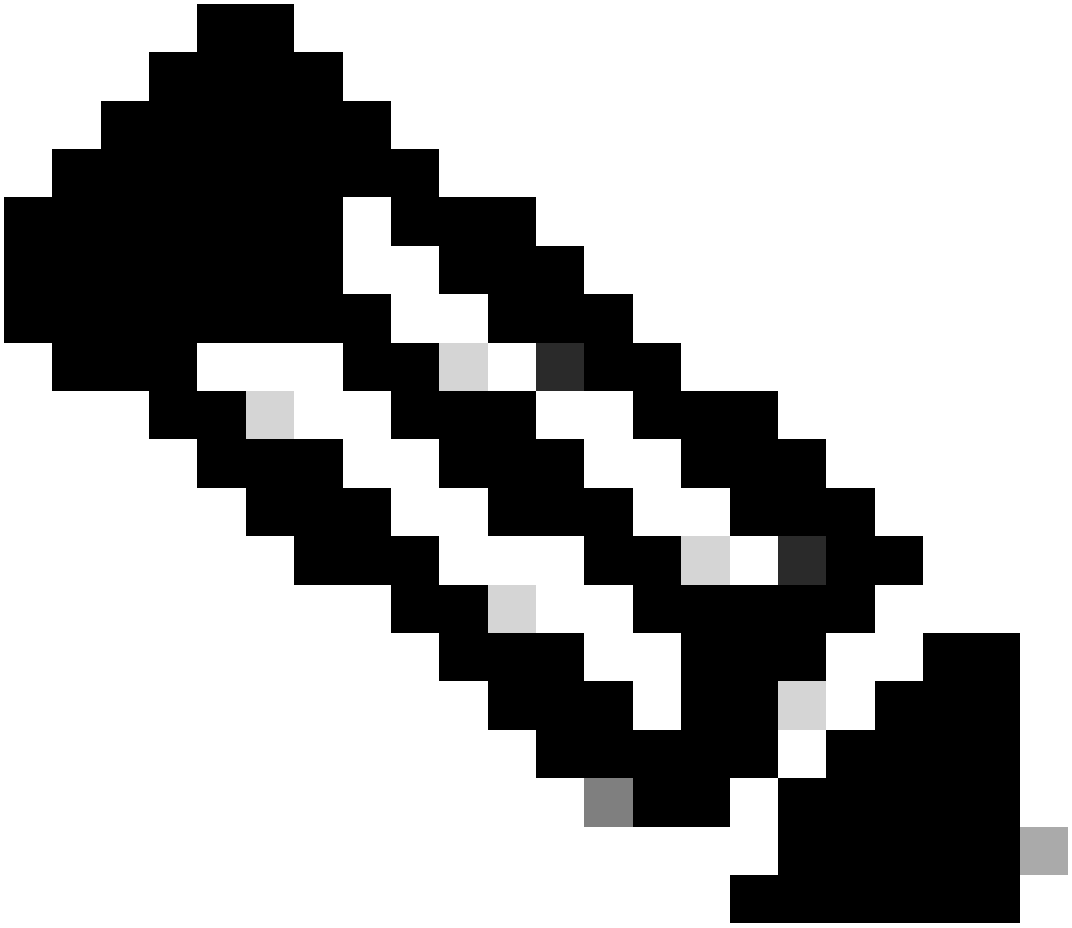
Fare riferimento all'ID bug software Cisco CSCvq42317 "ASDM prompt to change enable password after it was set on CLI" (ASDM richiede di modificare la password di abilitazione dopo l'impostazione sulla CLI).

Problema 22. L'oggetto ASDN scompare dopo l'aggiornamento dell'interfaccia utente ASDM

Quando si aggiunge un gruppo di oggetti e un host di oggetti a un gruppo di oggetti esistente e dopo aver aggiornato l'ASDM, il gruppo di oggetti scompare dalla lista ASDM. Affinché il difetto corrisponda, i nomi degli oggetti devono iniziare con numeri.

Risoluzione dei problemi - Azioni consigliate

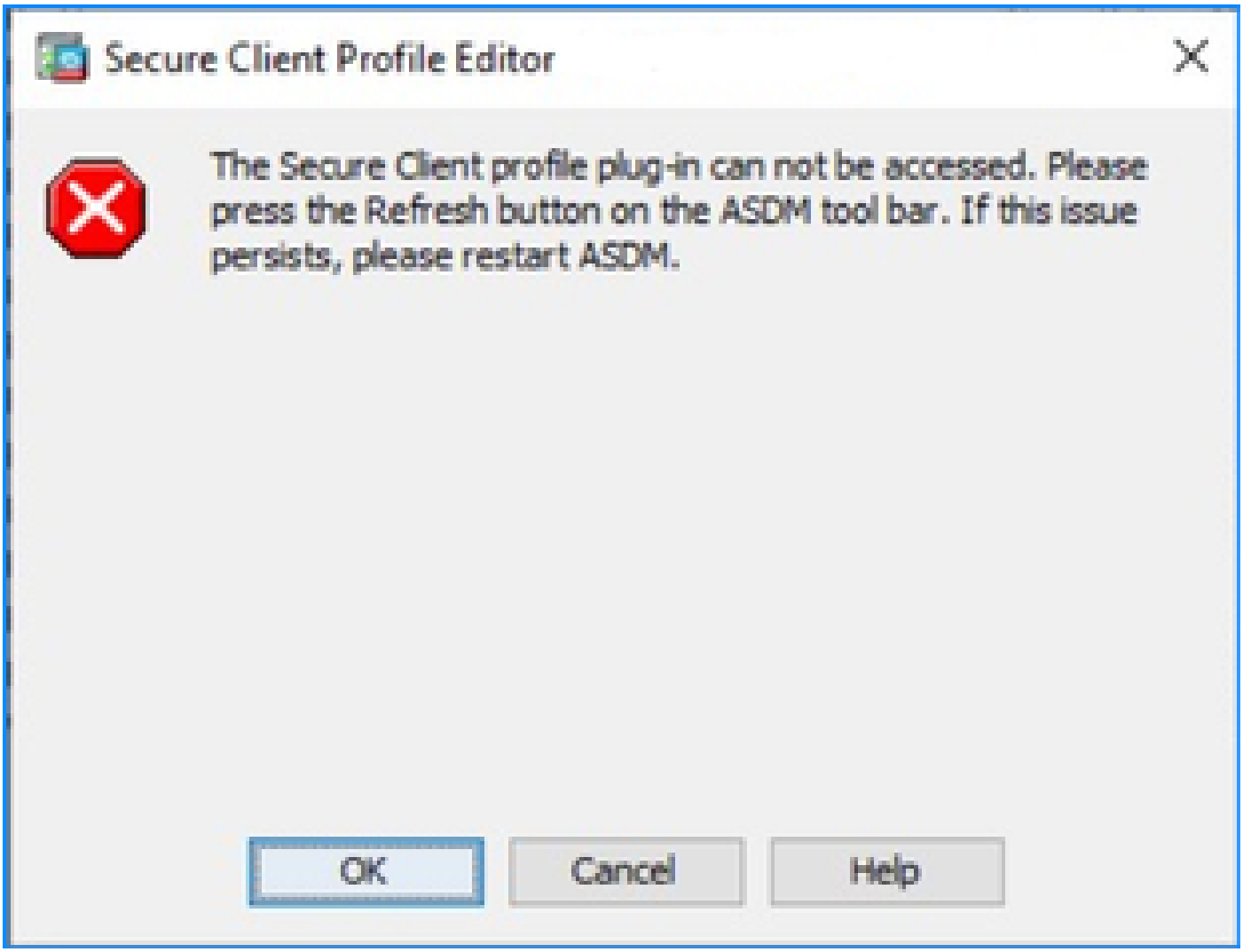
Fare riferimento all'ID bug Cisco CSCwf71723 del software "ASDM lose configure objects/object groups" (ASDM: perdita di oggetti/gruppi di oggetti configurati).



Nota: Questo problema è stato risolto nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

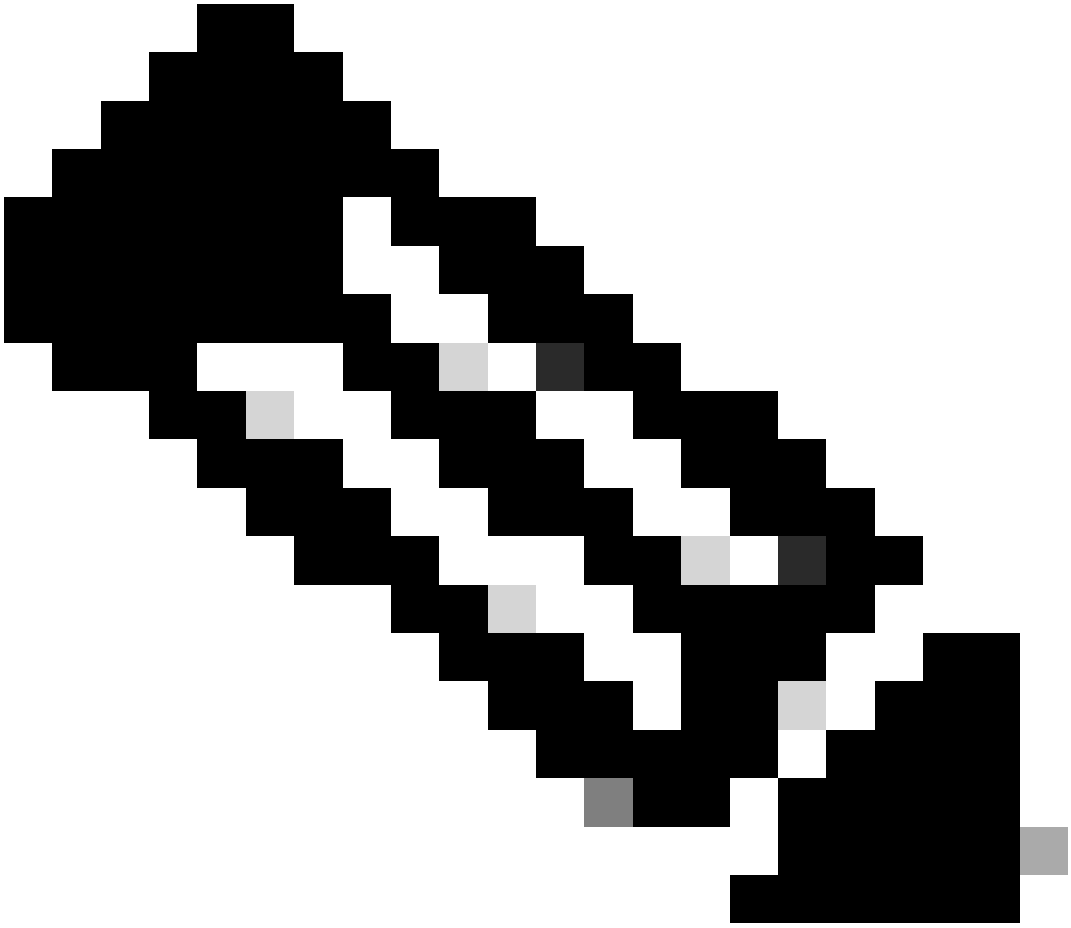
Problema 23. Impossibile modificare i profili client AnyConnect per le versioni precedenti alla 4.5

Impossibile modificare i profili client AnyConnect per AnyConnect Profile precedenti alla versione 4.5. Il messaggio di errore è "Impossibile accedere al plug-in Secure Client Profile. Premere il pulsante Refresh (Aggiorna) sulla barra degli strumenti ASDM. Se il problema persiste, riavviare ASDM.":



Risoluzione dei problemi - Azioni consigliate

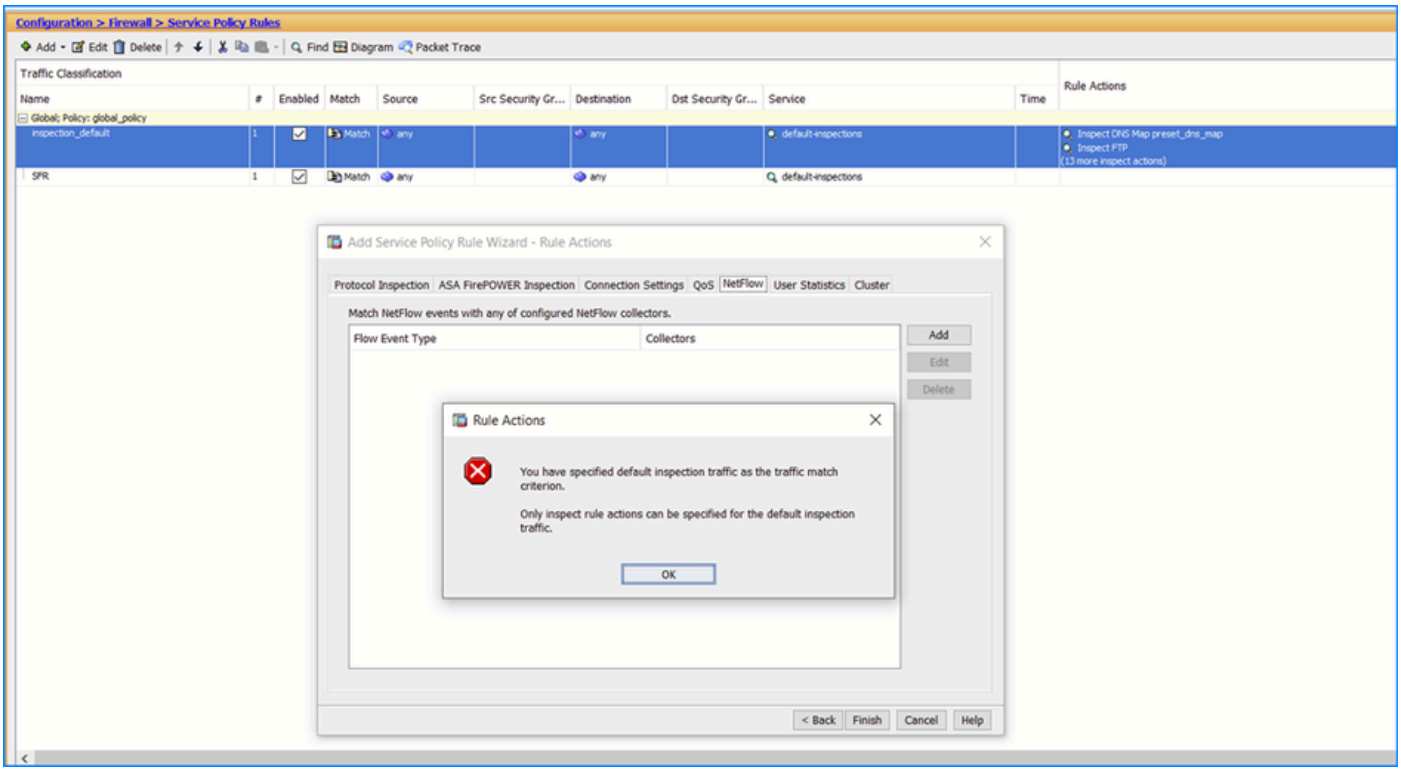
Fare riferimento all'ID bug Cisco CSCwf16947 del software "ASDM - Unable to load Anyconnect Profile Editor" (ASDM - Impossibile caricare l'Editor di profili Anyconnect).



Nota: Questo problema è stato risolto nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

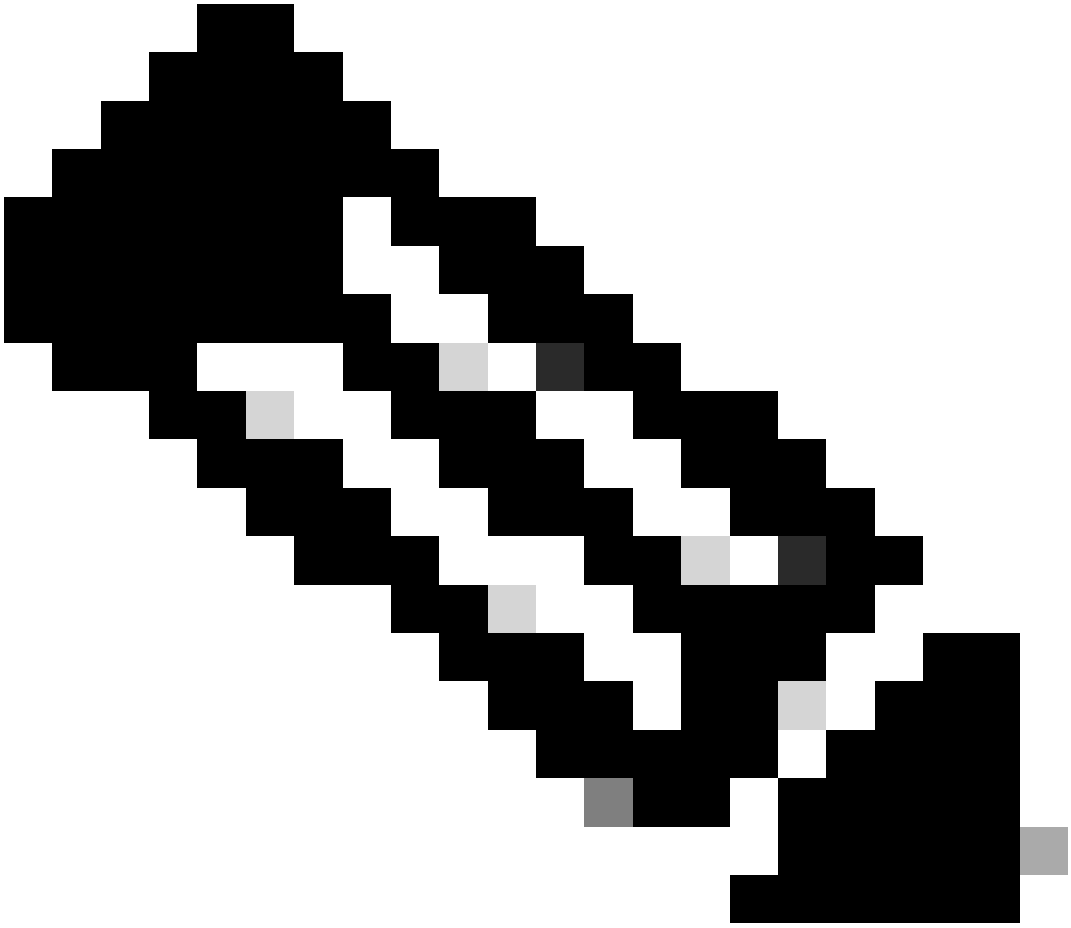
Problema 24. Impossibile passare alla scheda Edit Service Policy > Rule Actions > ASA FirePOWER Inspection

In ASDM versione 7.8.2, gli utenti non sono in grado di passare alla scheda Modifica criteri servizio > Azioni regola > Ispezione FirePOWER ASA e viene visualizzato l'errore: "È stato specificato il traffico di ispezione predefinito come criterio di corrispondenza del traffico. Per il traffico di ispezione predefinito è possibile specificare solo azioni regola di ispezione." Questo si verifica anche quando è stato selezionato un ACL per il reindirizzamento:



Risoluzione dei problemi - Azioni consigliate

Fare riferimento all'ID bug software Cisco CSCvg15782 "ASDM - Unable to view modify SFR traffic redirection after upgrade to version 7.8(2)" (ASDM - Impossibile visualizzare modificare il reindirizzamento del traffico SFR dopo l'aggiornamento alla versione 7.8(2)). Per risolvere il problema, è possibile utilizzare la CLI per modificare la configurazione della mappa dei criteri.



Nota: Questo problema è stato risolto nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

Problema 25. AnyConnect Image versione 5.1 e AnyConnect Profile Editor su ASDM

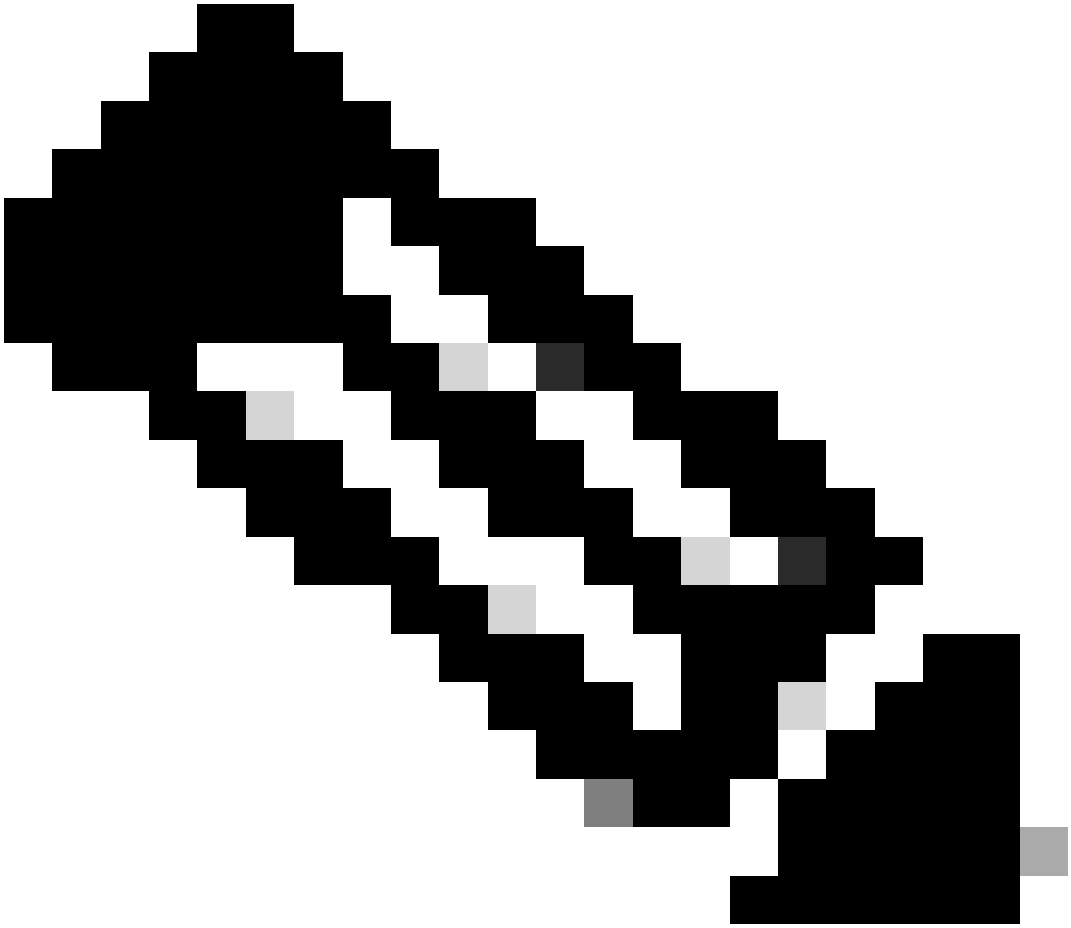
Questi sintomi vengono osservati nel software Secure Client versione 5.1:

1. Nomi dei moduli di Criteri di gruppo non elencati durante il caricamento dei pacchetti Win/Mac/Linux
2. ASDM non riesce ad aprire AnyConnect Profile Editor.

Risoluzione dei problemi - Azioni consigliate

Fare riferimento all'ID bug Cisco CSCwh74417 del software "ASDM: Impossibile caricare

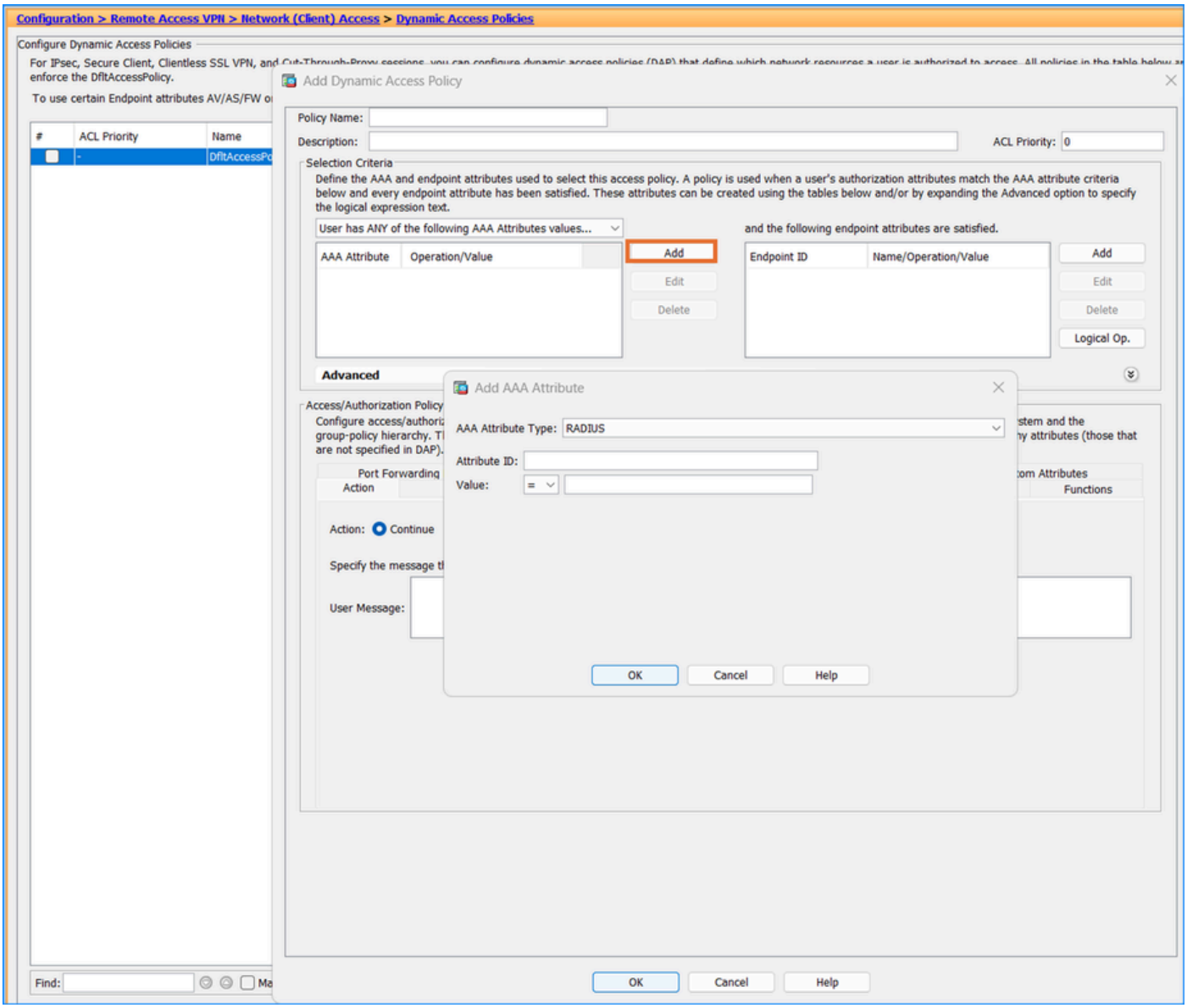
AnyConnect Profile Editor e Criteri di gruppo quando si utilizza CSC Image 5.1". Per ovviare al problema, usare versioni inferiori di Secure Client.



Nota: Questo problema è stato risolto nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

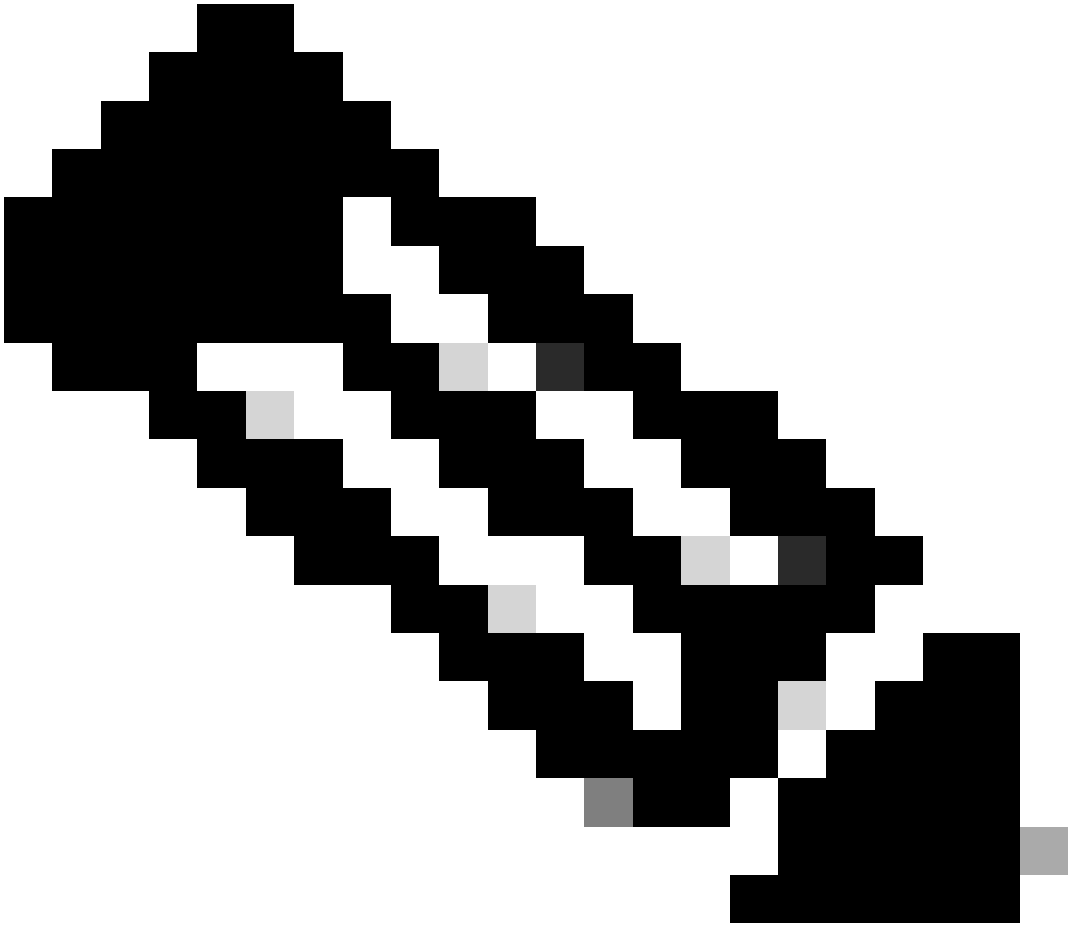
Problema 26. Il tipo di attributi AAA (Radius/LDAP) non è visibile in ASDM

Il tipo di attributi AAA (Radius/LDAP) non è visibile in ASDM > Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Campo Aggiungi > Attributo AAA > Aggiungi > Seleziona Radius o LDAP:



Risoluzione dei problemi - Azioni consigliate

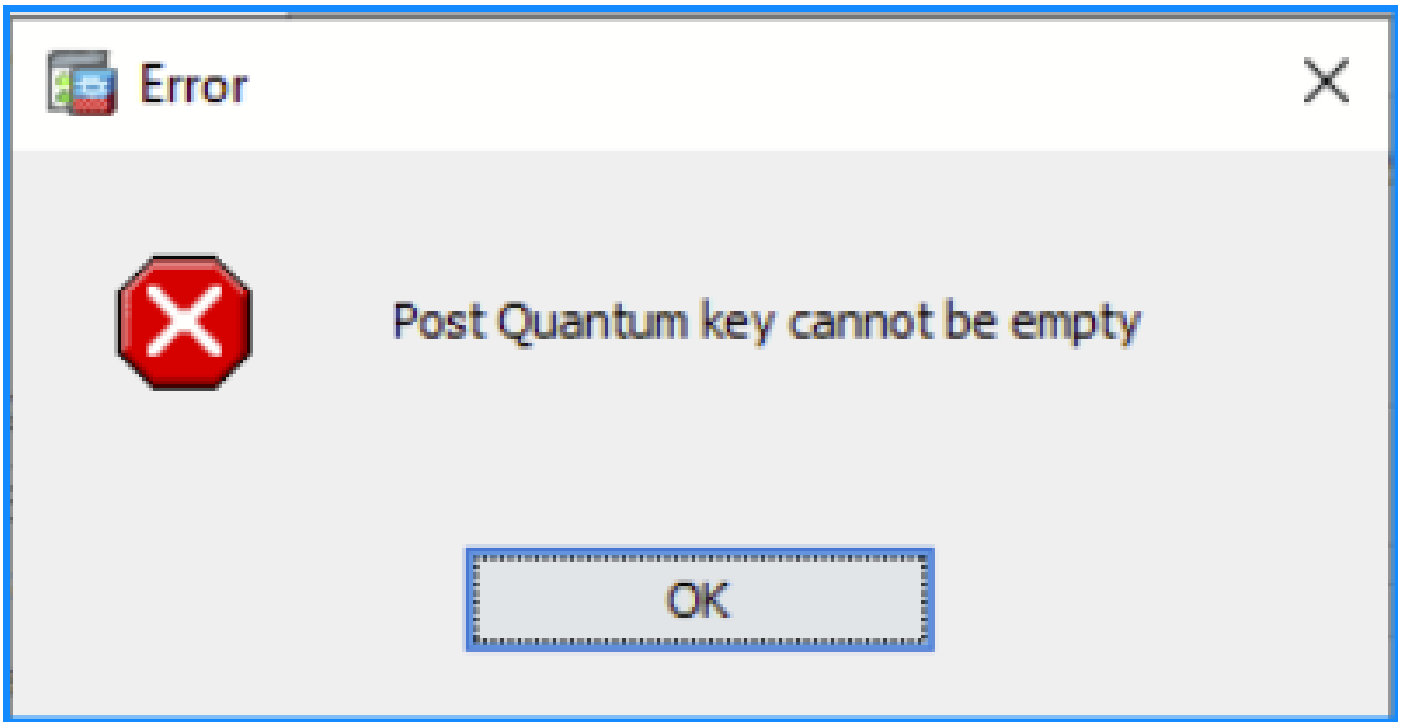
Fare riferimento all'ID bug Cisco CSCwa9370 del software "ASDM: ASDM:DAP config missing AAA Attributes type (Radius/LDAP)" e Cisco bug ID CSCwd16386 "ASDM:DAP config missing AAA Attributes type (Radius/LDAP)".



Nota: Questi problemi sono stati risolti nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

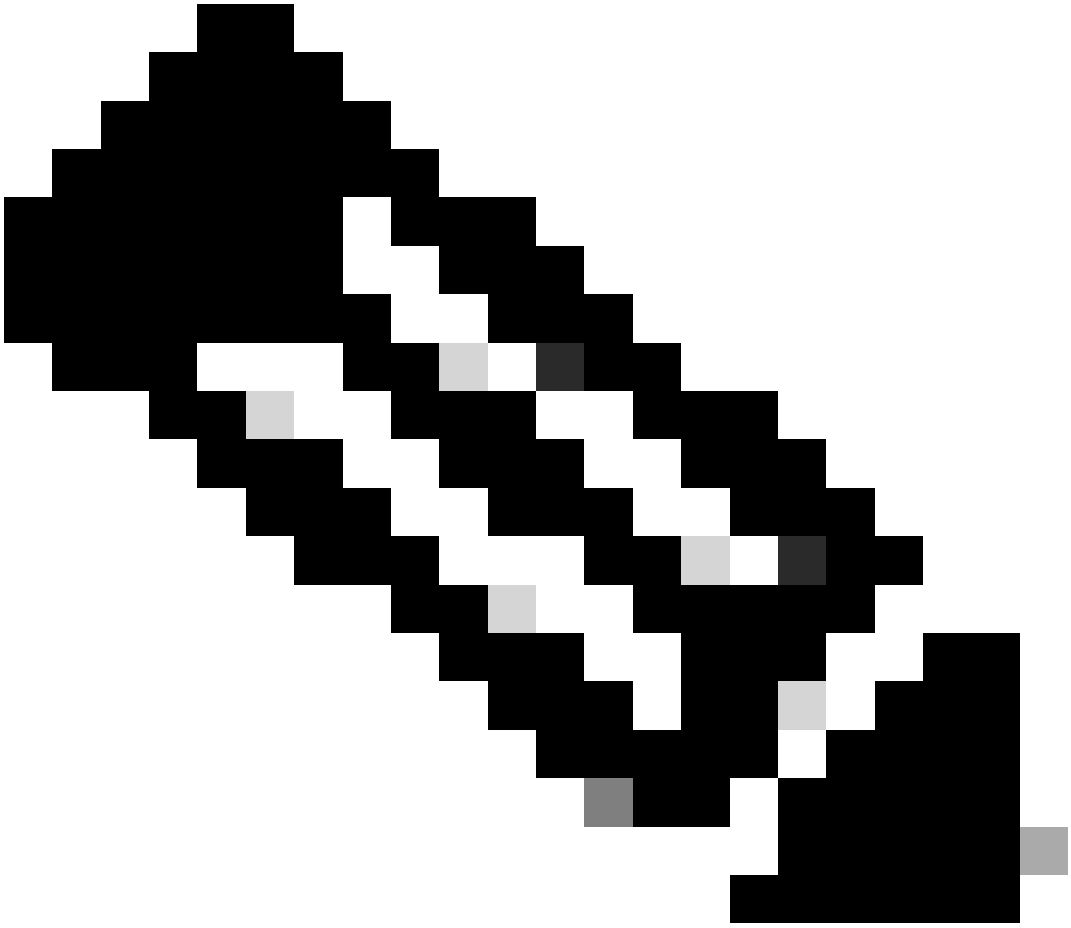
Problema 27. L'errore 'La chiave Quantum post non può essere vuota' viene visualizzato su ASDM

Quando si modifica la sezione Avanzate in ASDM > Configurazione > VPN ad accesso remoto >Profili di connessione di rete (client) > IPsec (IKEv2), viene visualizzato il messaggio di errore 'Post Quantum key cannot be blank':



Risoluzione dei problemi - Azioni consigliate

Fare riferimento al software Cisco bug ID CSCwe58266 "ASDM IKev2 configuration - Post Quantum Key cannot be blank error message" (Configurazione ASDM IKev2 - La chiave post quantum non può essere vuota).



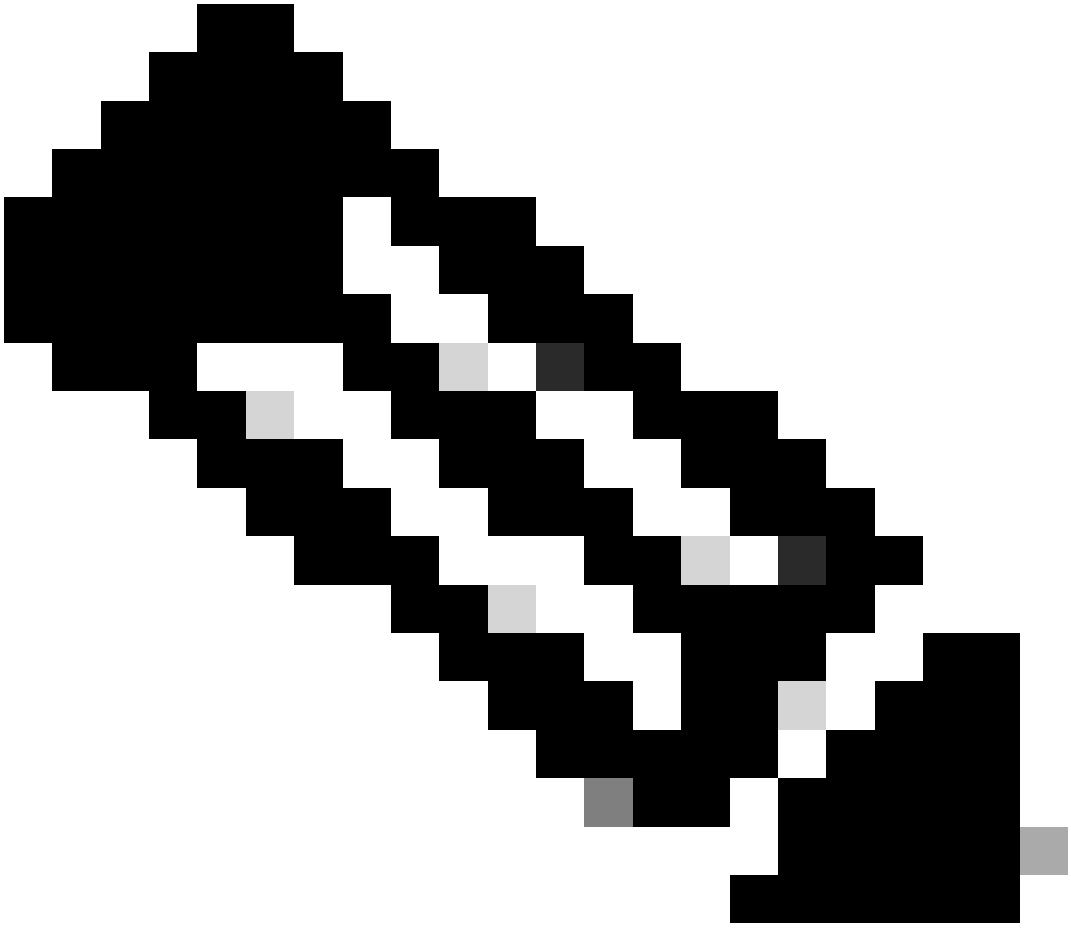
Nota: Questo problema è stato risolto nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

Problema 28. Quando si utilizza l'opzione "dove usato", ASDM non visualizza alcun risultato

ASDM non visualizza alcun risultato quando si utilizza l'opzione "dove usato" individuata selezionando Configurazione > Firewall > Oggetti > Oggetti/gruppi di rete e facendo clic con il pulsante destro del mouse su un oggetto.

Risoluzione dei problemi - Azioni consigliate

Fare riferimento all'ID bug Cisco CSCwd98702 "Dove usato" in ASDM non funziona".



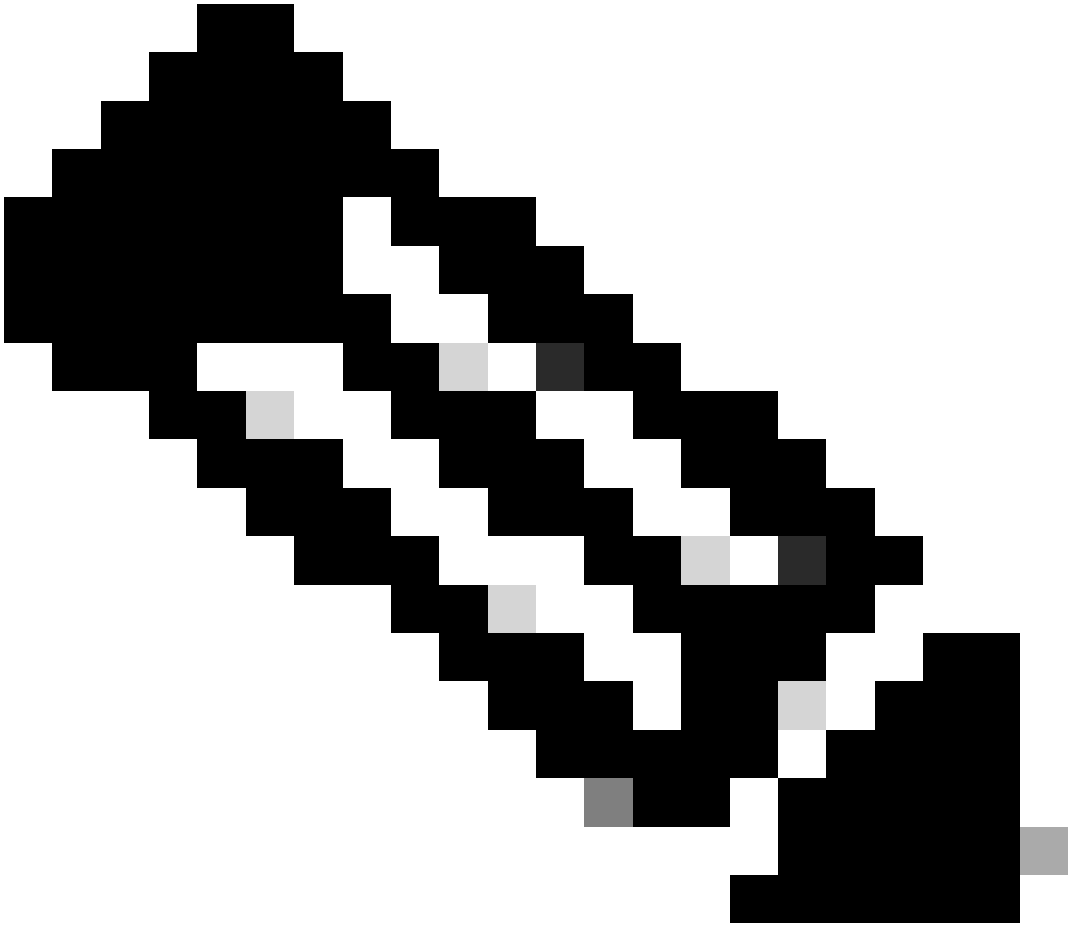
Nota: Questo problema è stato risolto nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

Problema 29. Il messaggio di avviso "[Oggetto di rete] non può essere eliminato perché è utilizzato nel seguente" durante l'eliminazione di un oggetto di rete

ASDM non visualizza il messaggio di avvertenza "[Network Object] cannot be Deleted perché è utilizzato negli elementi seguenti" quando si elimina un oggetto di rete a cui viene fatto riferimento in un gruppo di rete in Configurazione > Firewall > Oggetti > Network Objects/Groups.

Risoluzione dei problemi - Azioni consigliate

Per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCwe67056 "[Network Object] cannot be Deleted as it is used in the following" warning not displayed" (Impossibile eliminare l'oggetto di rete perché è utilizzato nel messaggio di avviso "non visualizzato").



Nota: Questo problema è stato risolto nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

Problema 30. Problemi di usabilità con la scheda Oggetti di rete/Gruppo in ASDM

Si osservano uno o più di questi sintomi:

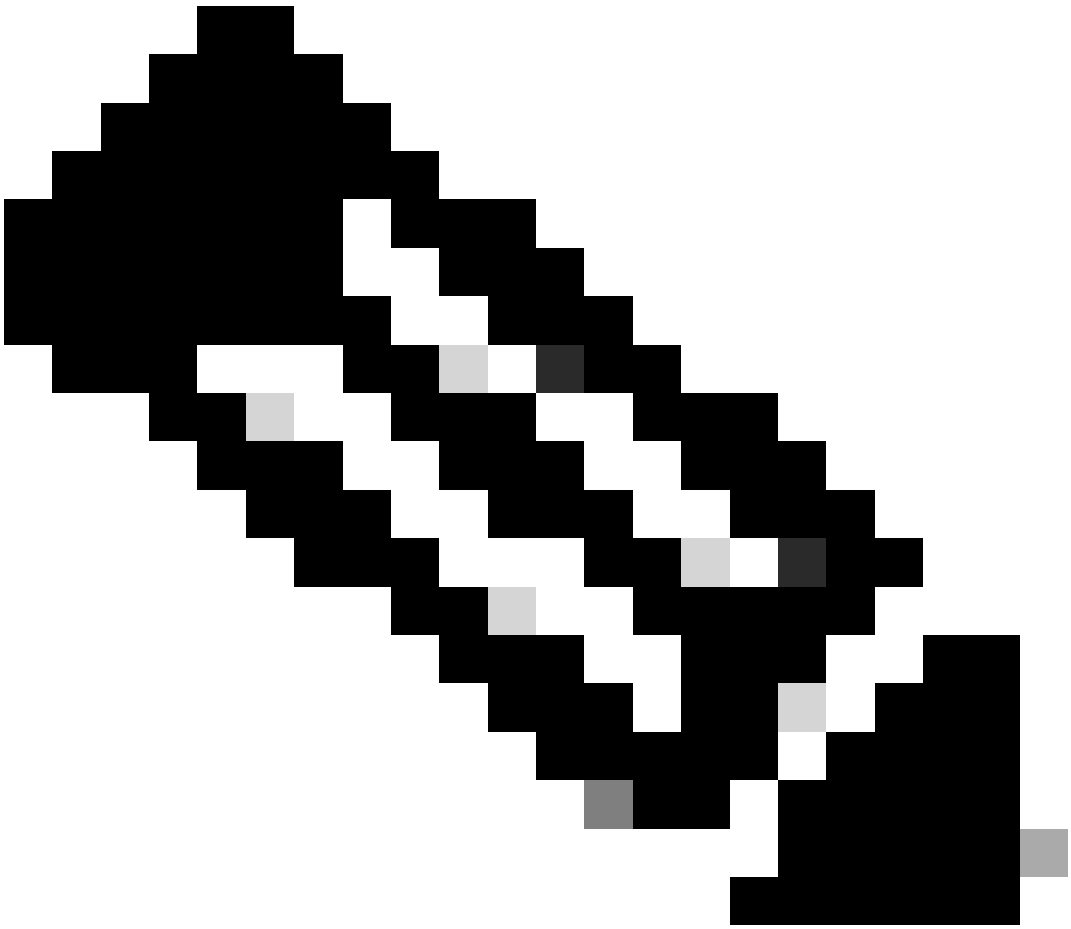
- L'input di testo "Nome" nella sezione "Crea nuovo membro oggetto" delle finestre "Aggiungi/Modifica gruppo di oggetti" è contrassegnato come "facoltativo". Tuttavia, il pulsante "Aggiungi>>" per creare e aggiungere l'oggetto è disattivato a meno che non venga immesso un nome.
- La scheda "Utilizzi" che viene visualizzata quando un utente fa clic su "Dove usato..." il menu di scelta rapida elenca solo le entità (ACL, route-map, object-group) che fanno riferimento direttamente all'oggetto. Deve inoltre elencare ricorsivamente il secondo, il terzo e così via. I riferimenti dell'ordine (ovvero un ACL che utilizza un gruppo di oggetti che contiene un oggetto deve essere elencato anche come "utilizzo" dell'oggetto).

- Anche l'operazione "Elimina" disponibile nel menu di scelta rapida visualizza questo comportamento. Elimina automaticamente qualsiasi entità che fa riferimento direttamente all'oggetto (se l'entità diventa vuota quando l'oggetto viene eliminato). Non funziona in questo modo quando un secondo, un terzo, e così via. il riferimento all'ordine diventerebbe vuoto a causa dell'eliminazione dell'oggetto e del riferimento al primo ordine.

L'utente può essere indotto a ritenere che ASDM impedisca alle entità che diventerebbero vuote a causa dell'eliminazione dell'oggetto dalla configurazione rimanente. Tuttavia, ciò non avviene necessariamente.

Risoluzione dei problemi - Azioni consigliate

Fare riferimento all'ID bug Cisco CSCwe86257 "Usability of Network Objects/Group Tab in ASDM" (Usibilità degli oggetti di rete/scheda gruppo in ASDM).

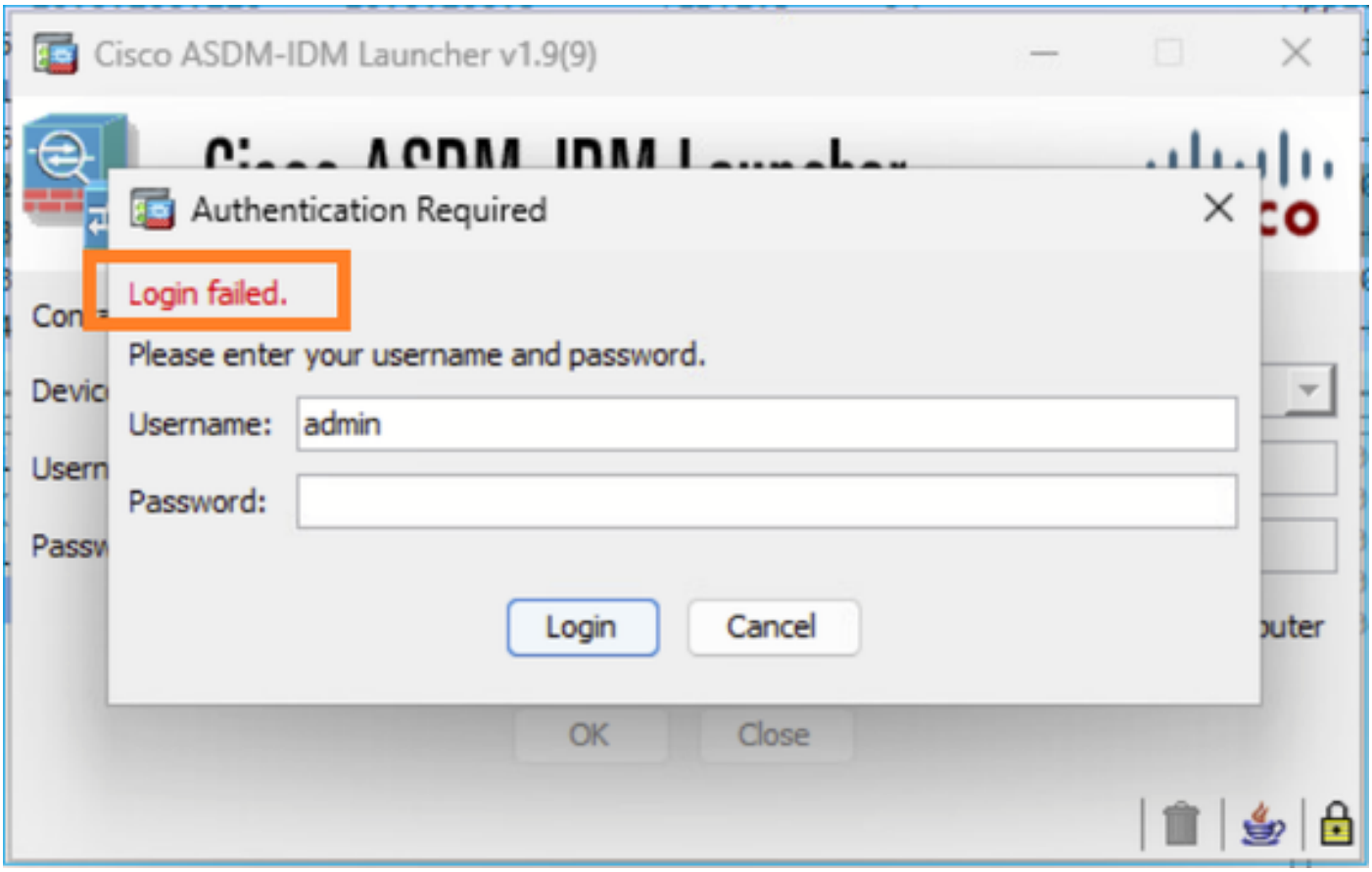


Nota: Questo problema è stato risolto nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

Risoluzione dei problemi di autenticazione ASDM

Problema 1. Accesso ASDM non riuscito

L'errore visualizzato sull'interfaccia utente di ASDM è:



Risoluzione dei problemi - Azioni consigliate

Questo errore si verifica quando si hanno entrambi i protocolli HTTP e Webvpn Cisco Secure Client (AnyConnect) abilitati sulla stessa interfaccia. Pertanto, devono essere soddisfatte tutte le condizioni:

1. AnyConnect/Cisco Secure Client è abilitato su un'interfaccia
2. Il server HTTP è abilitato sulla stessa interfaccia e sulla stessa porta di AnyConnect/Cisco Secure Client

Esempio:

<#root>

```
asa#
configure terminal

asa(config)#
```

webvpn

asa(config-webvpn)#

enable outside <-

default port in use (443)

and
asa(config)#

http server enable

<-

default port in use (443)

asa(config)#

http 0.0.0.0 0.0.0.0 outside

<- HTTP server configured on the same interface as Webvpn

Suggerimento per la risoluzione dei problemi: Abilitare 'debug http 255' per verificare il conflitto tra ASDM e Webvpn:

<#root>

ciscoasa#

debug http 255

debug http enabled at level 255.
ciscoasa# ewaURLHookVCARedirect
...addr: 192.0.2.5
ewaURLHookHTTPRedirect: url = /+webvpn+/index.html

HTTP: ASDM request detected [ASDM/] for [/+webvpn+/index.html]   <--------

webvpnhook: got '/+webvpn+' or '/+webvpn+/': Sending back "/+webvpn+/index.html"   <-----

HTTP 200 OK (192.0.2.110)HTTP: net_handle->standalone_client [1]
webvpn_admin_user_agent: buf: ASDM/ Java/1.8.0_431
ewsStringSearch: no buffer
Close 0

Come nota rapida, nonostante l'errore di accesso, i syslog dell'ASA mostrano che l'autenticazione ha avuto esito positivo:

<#root>

```
asa#
```

show logging

```
Oct 28 2024 07:42:44: %ASA-6-113012: AAA user authentication Successful : local database : user = user2
Oct 28 2024 07:42:44: %ASA-6-113009: AAA retrieved default group policy (DfltGrpPolicy) for user = user
Oct 28 2024 07:42:44: %ASA-6-113008: AAA transaction status ACCEPT : user = user2
Oct 28 2024 07:42:44: %ASA-6-605005: Login permitted from 192.0.2.110/60316 to NET50:192.0.2.5/https fo
Oct 28 2024 07:42:44: %ASA-6-611101:
```

User authentication succeeded: IP address: 192.0.2.110, Uname: user2

Soluzioni

Soluzione 1

Modificare la porta TCP per il server HTTP ASA, ad esempio:

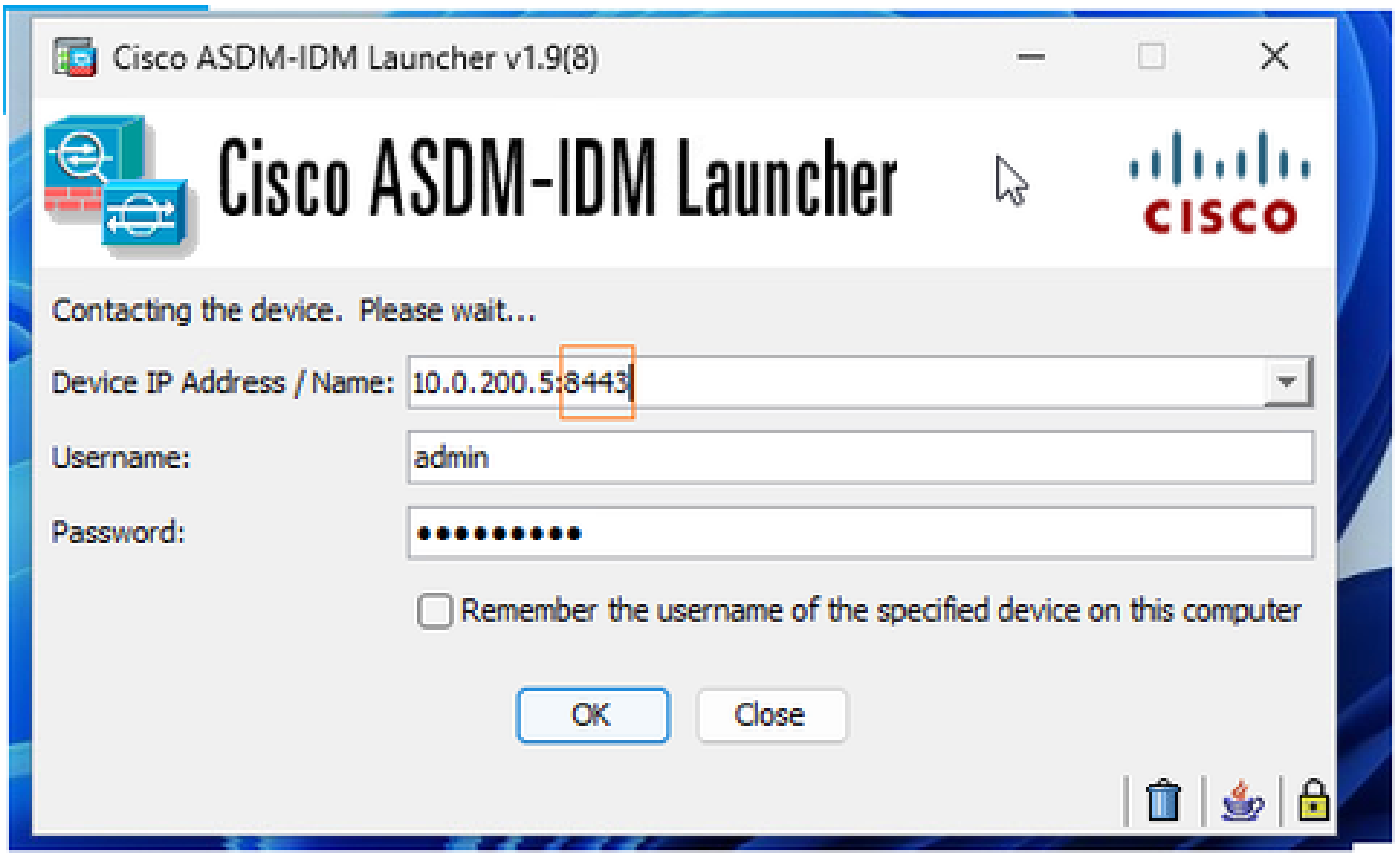
<#root>

```
ciscoasa#
```

configure terminal

```
ciscoasa(config)#
```

http server enable 8443



Soluzione 2

Modificare la porta TCP per AnyConnect/Cisco Secure Client, ad esempio:

<#root>

```
ciscoasa#
configure terminal

ciscoasa(config)#
webvpn

ciscoasa(config-webvpn)#
no enable outside
 <-- first you have disable WebVPN for all interfaces before changing the port
ciscoasa(config-webvpn)#
port 8443

ciscoasa(config-webvpn)#
enable outside
```

Soluzione 3

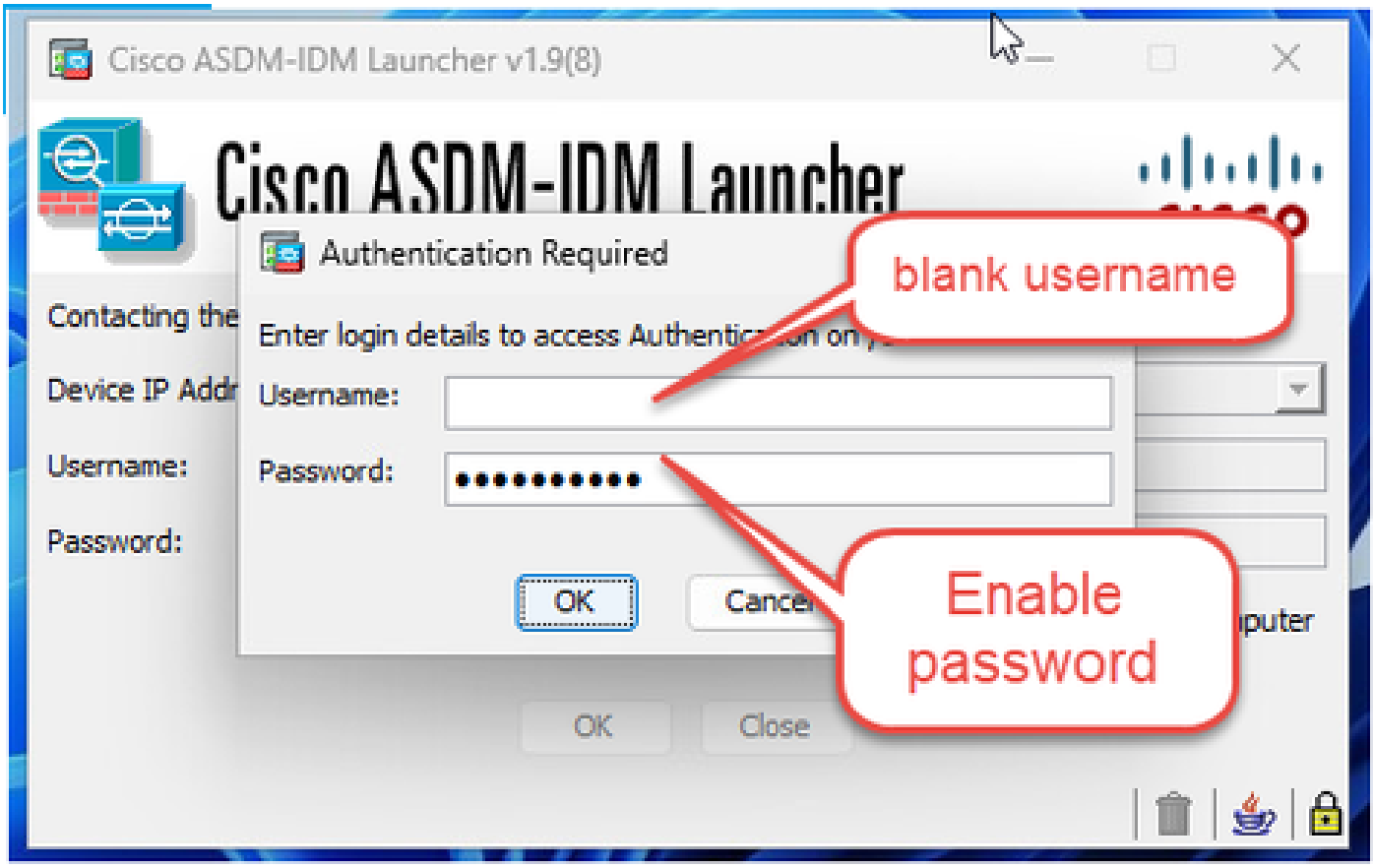
Per ovviare al problema, rimuovere la configurazione della "console http di autenticazione aaa":

<#root>

```
ciscoasa(config)#
```

no aaa authentication http console LOCAL

In questo caso, è possibile accedere ad ASDM solo utilizzando la password enable:



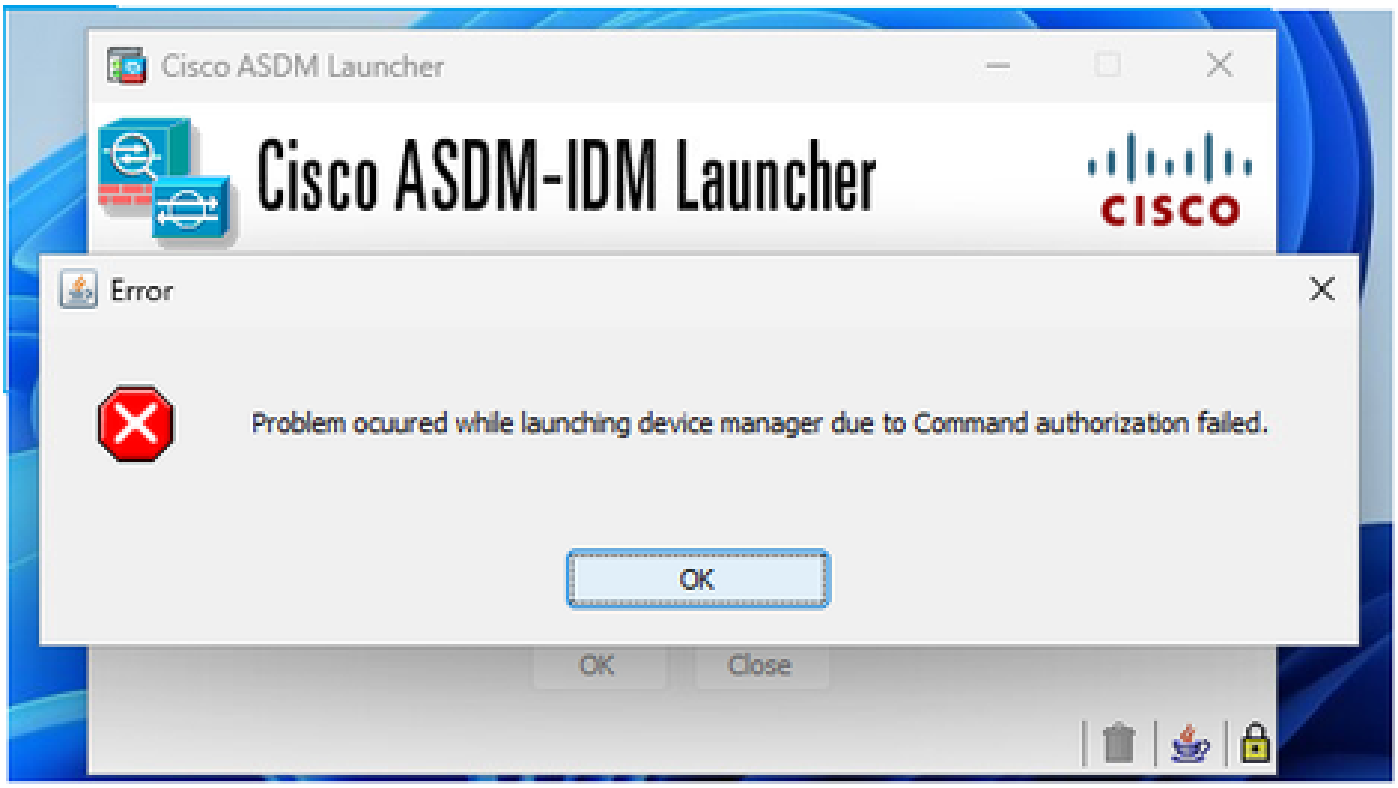
Difetto correlato

ID bug Cisco CSCwb67583

Aggiungi avviso quando webvpn e ASDM sono abilitati sulla stessa interfaccia

Problema 2. Autorizzazione del comando ASDM non riuscita

L'errore visualizzato sull'interfaccia utente di ASDM è:



Risoluzione dei problemi - Passi consigliati

Controllare la configurazione AAA sull'appliance ASA e verificare che:

- È stata configurata anche l'autenticazione aaa.
- Se si utilizza un server di autenticazione remota, sarà raggiungibile e autorizzerà i comandi.

Riferimento

https://www.cisco.com/c/en/us/td/docs/security/asa/asa922/configuration/general/asa-922-general-config/aaa-local.html

Problema 3. Configurare l'accesso in sola lettura ad ASDM

Talvolta si desidera consentire l'accesso in sola lettura agli utenti ASDM.

Risoluzione dei problemi - Passi consigliati

Creare un nuovo utente con un livello di privilegi personalizzato (5), ad esempio:

<#root>

```
asa(config)#
```

username [username] password [password] privilege 5

Con questo comando viene creato un utente con un livello di privilegio pari a 5, ovvero il livello "solo monitoraggio". Sostituire `[nomeutente]` e `[password]` con il nome utente e la password desiderati.

Dettagli

L'autorizzazione Comando locale consente di assegnare comandi a uno dei 16 livelli di privilegio (da 0 a 15). Per impostazione predefinita, ogni comando è assegnato al livello di privilegio 0 o 15. È possibile definire ogni utente in modo che si trovi a un livello di privilegio specifico e ogni utente può immettere qualsiasi comando al livello di privilegio assegnato o a un livello inferiore. L'appliance ASA supporta i livelli di privilegi utente definiti nel database locale, in un server RADIUS o in un server LDAP (se si mappano gli attributi LDAP agli attributi RADIUS).

Procedura

Passaggio 1	Scegliere Configurazione > Gestione dispositivi > Utenti/AAA > Accesso AAA > Autorizzazione.
Passaggio 2	Selezionare la casella di controllo Abilita autorizzazione per accesso comando ASA > Abilita.
Passaggio 3	Selezionare LOCAL (LOCALE) dall'elenco a discesa Server Group (Gruppo server).
Passaggio 4	Quando si abilita l'autorizzazione dei comandi locali, è possibile assegnare manualmente i livelli di privilegio a singoli comandi o gruppi di comandi oppure abilitare i privilegi di account utente predefiniti. · Fare clic su Set ASDM Defined User Roles (Imposta ruoli utente definiti ASDM) per utilizzare i privilegi di account utente predefiniti. Viene visualizzata la finestra di dialogo Impostazione ruoli utente definiti ASDM. Fare clic su Sì per utilizzare i privilegi di account utente predefiniti: Admin (livello privilegi 15, con accesso completo a tutti i comandi CLI; Sola lettura (livello privilegio 5, con accesso in sola lettura); e Solo monitoraggio (livello di privilegio 3, con accesso solo alla sezione Monitoraggio). · Fare clic su Configura privilegi di comando per configurare manualmente i livelli di comando. Verrà visualizzata la finestra di dialogo Impostazione privilegi di comando. È possibile visualizzare tutti i comandi scegliendo Tutte le modalità dall'elenco a discesa Modalità di comando oppure scegliere una modalità di configurazione per visualizzare i comandi disponibili in tale modalità. Ad esempio, se si sceglie contesto, è possibile visualizzare tutti i comandi disponibili in modalità di configurazione contesto. Se è possibile

	immettere un comando in modalità di esecuzione utente o in modalità di esecuzione privilegiata nonché in modalità di configurazione e il comando esegue diverse azioni in ciascuna modalità, è possibile impostare separatamente il livello di privilegio per queste modalità. Nella colonna Variant viene visualizzato show, clear o cmd. È possibile impostare il privilegio solo per la forma show, clear o configure del comando. La forma di configurazione del comando è in genere la forma che causa una modifica della configurazione, ovvero il comando non modificato (senza il prefisso show o clear) o la forma no. Per modificare il livello di un comando, fare doppio clic su di esso o fare clic su Modifica. È possibile impostare un livello compreso tra 0 e 15. È possibile configurare solo il livello di privilegio del comando principale. Ad esempio, è possibile configurare il livello di tutti i comandi aaa, ma non il livello dei comandi aaa authentication e aaa authorization separatamente. Per modificare il livello di tutti i comandi visualizzati, fare clic su Seleziona tutto, quindi su Modifica. Fare clic su OK per accettare le modifiche.
Passaggio 5	Fare clic su Apply (Applica). Le impostazioni di autorizzazione vengono assegnate e le modifiche vengono salvate nella configurazione in esecuzione.

Riferimento

https://www.cisco.com/c/en/us/td/docs/security/asa/asa922/asdm722/general/asdm-722-general-config/admin-management.html#ID-2111-00000650

Problema 4. ASDM Multi-Factor Authentication (MFA)

Risoluzione dei problemi - Passi consigliati

Al momento della stesura di questo documento, ASDM non supporta l'autenticazione a più fattori (o 2FA). Questa limitazione include l'autenticazione a più fattori con soluzioni quali PingID e così via.

Riferimento

Cisco Bug ID CSCvs85995

ENH: Accesso ASDM con autenticazione a due fattori o MFA

Problema 5. Configurazione dell'autenticazione esterna ASDM

Risoluzione dei problemi - Passi consigliati

È possibile utilizzare LDAP, RADIUS, RSA SecurID o TACACS+ per configurare l'autenticazione esterna su ASDM.

Riferimenti

- https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/112967-acs-aaa-tacacs-00.html
- https://www.cisco.com/c/en/us/td/docs/security/asa/asa922/configuration/general/asa-922-general-config/aaa-radius.html
- https://www.cisco.com/c/en/us/td/docs/security/asa/asa922/configuration/general/asa-922-general-config/aaa-tacacs.html
- https://www.cisco.com/c/en/us/td/docs/security/asa/asa922/configuration/general/asa-922-general-config/aaa-ldap.html

Problema 6. L'autenticazione ASDM LOCAL non riesce

Risoluzione dei problemi - Passi consigliati

Se si utilizza l'autenticazione esterna e l'autenticazione LOCALE come fallback, l'autenticazione locale funziona solo se il server esterno è inattivo o non funziona. Solo in questo caso l'autenticazione LOCAL subentra ed è possibile connettersi con gli utenti LOCAL.

Questo perché l'autenticazione esterna ha la precedenza sull'autenticazione LOCALE.

Esempio:

<#root>

```
asa(config)# aaa authentication ssh console RADIUS_AUTH LOCAL
```

Riferimento

- https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/A-H/asa-command-ref-A-H/aa-ac-commands.html#wp6184732320

Problema 7. Password temporanea ASDM

Risoluzione dei problemi - Passi consigliati

- Il supporto dell'autenticazione OTP (one-time-password) ASDM è stato aggiunto nella versione 8.x - 9.x di ASA e solo in modalità a routing singolo.
- L'autenticazione OTP ASDM per la modalità trasparente di ASA Firewall e/o la modalità multi-contesto non entra in questa categoria.

Fare riferimento all'ID bug Cisco CSCtf23419
ENH: Supporto dell'autenticazione OTP ASDM in modalità multi-contesto e trasparente

Problema 8. Il profilo di connessione non visualizza tutti i metodi

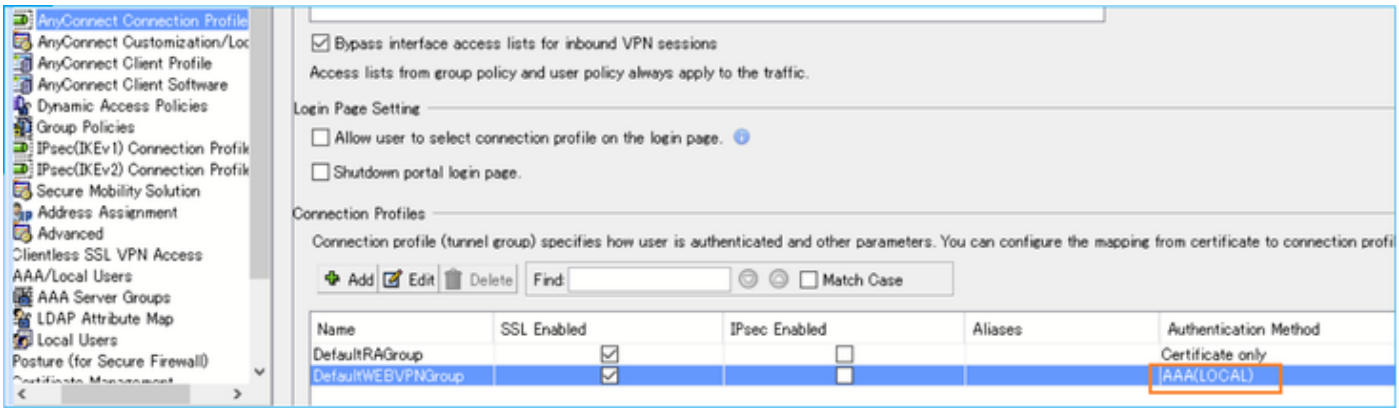
In questo caso, il problema è una mancata corrispondenza tra la configurazione CLI dell'ASA e l'interfaccia utente di ASDM.

In particolare, la CLI ha:

<#root>

```
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication aaa certificate
```

Mentre l'interfaccia utente di ASDM non menziona il metodo del certificato:



Risoluzione dei problemi - Passi consigliati

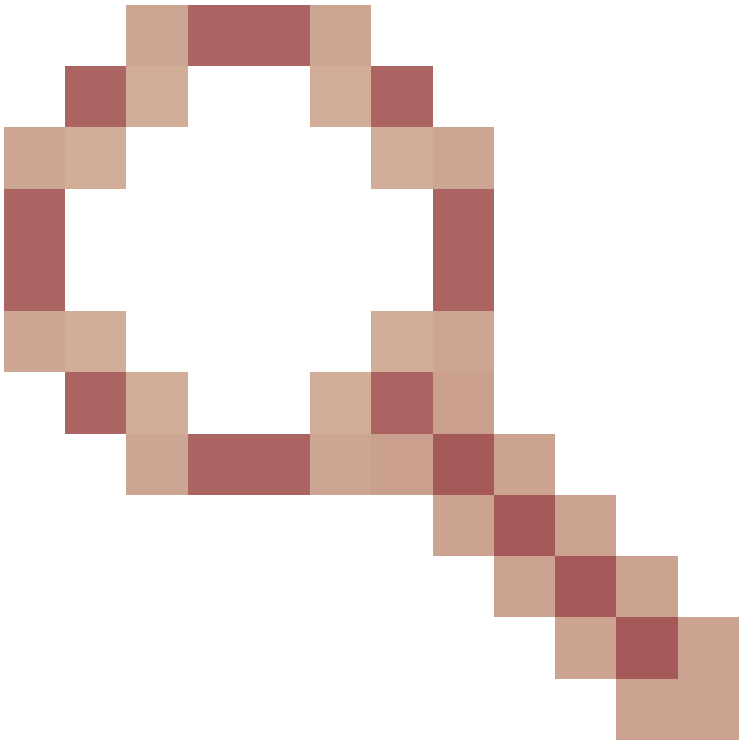
Si tratta di una questione cosmetica. Il metodo non viene visualizzato in ASDM, ma viene utilizzata l'autenticazione del certificato.

Problema 9. La sessione ASDM non scade

Il problema è che il timeout della sessione GUI ASDM non viene preso in considerazione.

Risoluzione dei problemi - Passi consigliati

Questo si verifica quando il comando "aaa authentication http console LOCAL" non è impostato sull'appliance ASA gestita.



Fare riferimento all'ID bug Cisco CSCwj70826
ENH: aggiungi un avviso: impostazione del timeout della sessione, richiede "aaa authentication http console LOCAL"

Soluzione alternativa

Configurare il comando "aaa authentication http console LOCAL" sull'appliance ASA gestita.

Problema 10. L'autenticazione LDAP ASDM non riesce

Risoluzione dei problemi - Passi consigliati

Passaggio 1

Accertarsi che la configurazione sia presente, ad esempio:

<#root>

```
aaa-server ldap_server protocol ldap
aaa-server ldap_server (inside) host 192.0.2.1
 ldap-base-dn OU=ldap_ou,DC=example,DC=com
 ldap-scope subtree
 ldap-naming-attribute cn
 ldap-login-password *****
 ldap-login-dn CN=example, DC=example,DC=com
 server-type microsoft
asa(config)#
```

aaa authentication http console ldap_server LOCAL

Passaggio 2

Controllare lo stato del server LDAP:

<#root>

```
asa#
```

show aaa-server

Scenario positivo:

<#root>

```
Server status:
```

ACTIVE

```
, Last transaction at 11:45:23 UTC Tue Nov 19 2024
```

Scenario non valido:

<#root>

```
Server status:
```

FAILED

```
, Server disabled at 11:45:23 UTC Tue Nov 19 2024
```

Passaggio 3

Verificare che l'autenticazione LOCALE funzioni correttamente disattivando temporaneamente l'autenticazione LDAP.

Passaggio 4

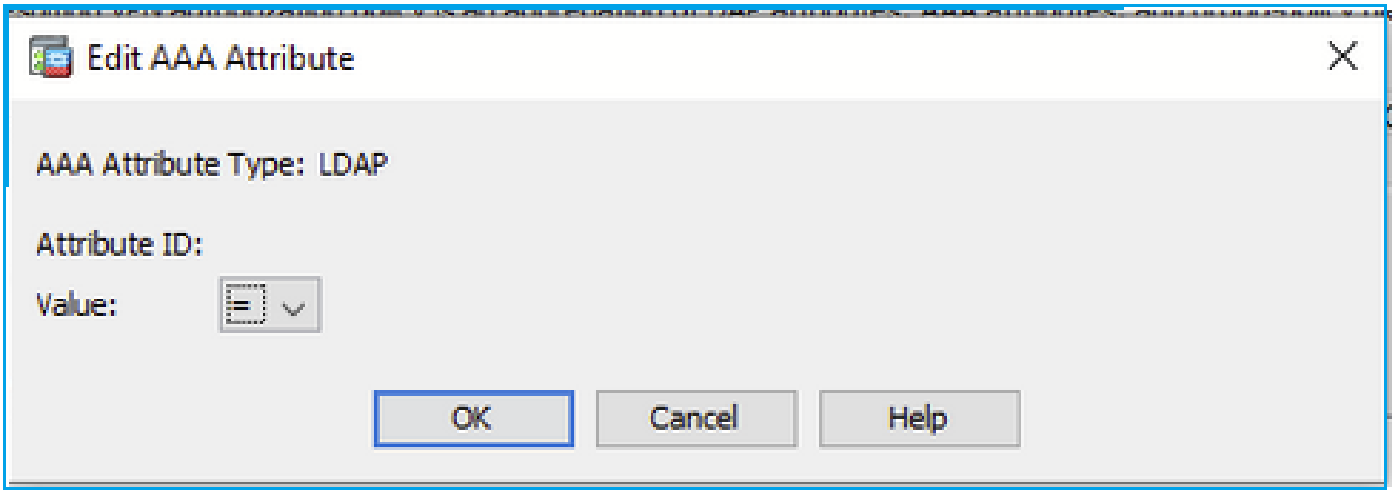
Sull'appliance ASA, eseguire i debug LDAP e provare ad autenticare l'utente:

```
<#root>

#

debug ldap 255
```

Nei debug vengono cercate le righe che contengono suggerimenti come "Non riuscito".

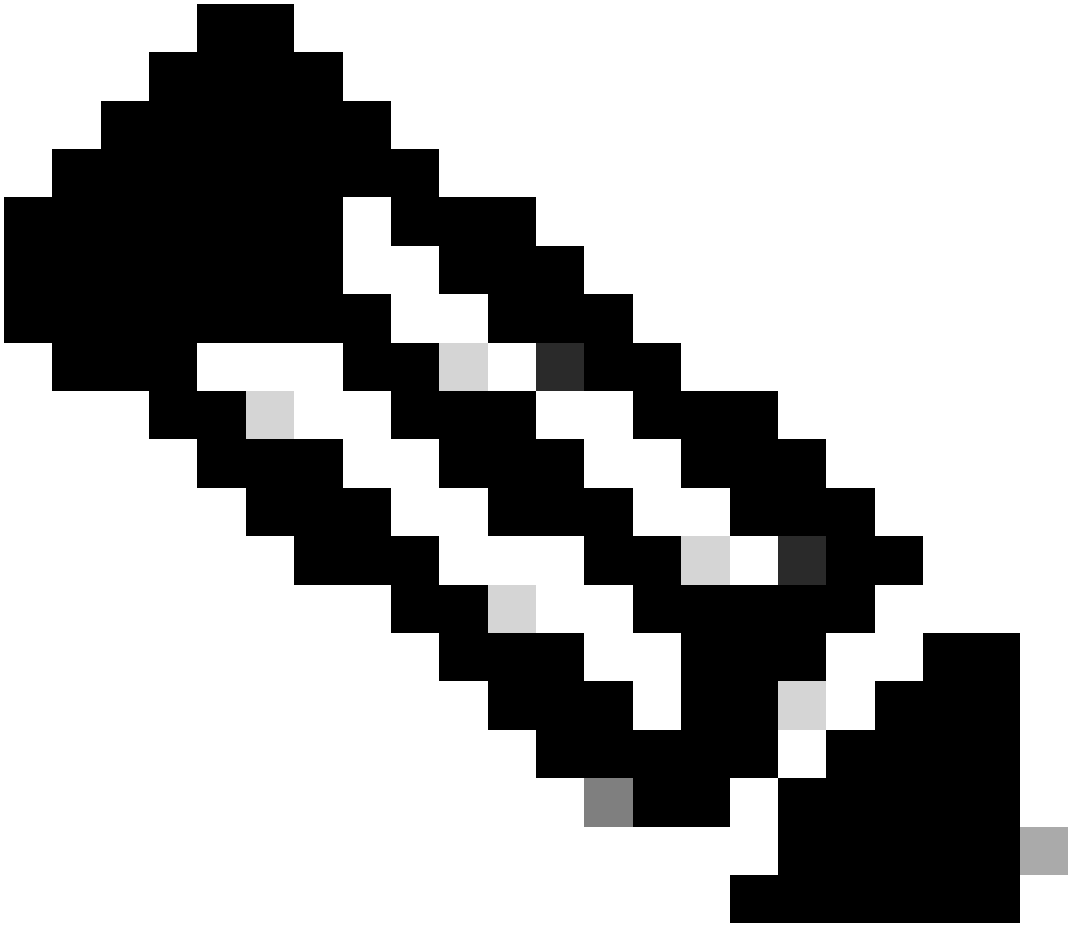
Problema 11. Configurazione DAP Webvpn ASDM mancante

In Configurazione DAP su ASDM AAA, il tipo di attributi (Radius/LDAP) non è visibile solo quando si visualizza = e != nell'elenco a discesa:



Risoluzione dei problemi - Passi consigliati

Questo è un problema software tracciato dall'ID bug Cisco CSCwa9370 ASDM:configurazione DAP senza tipo di attributi AAA (Radius/LDAP)

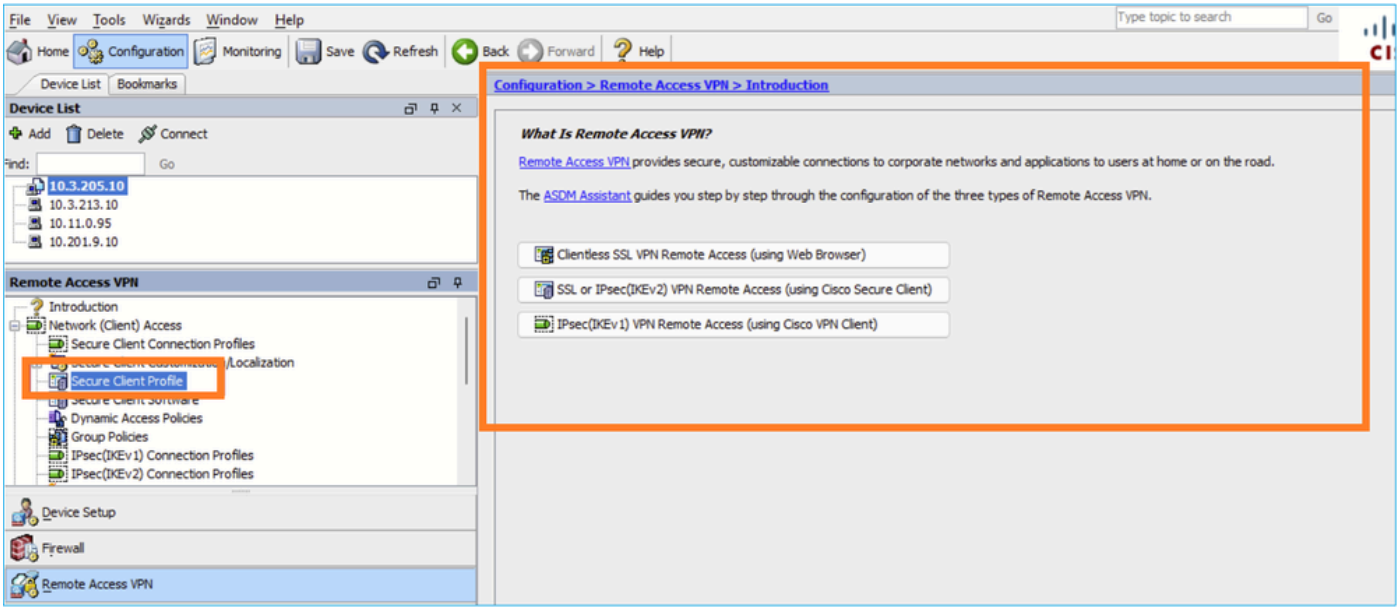


Nota: Questo problema è stato risolto nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

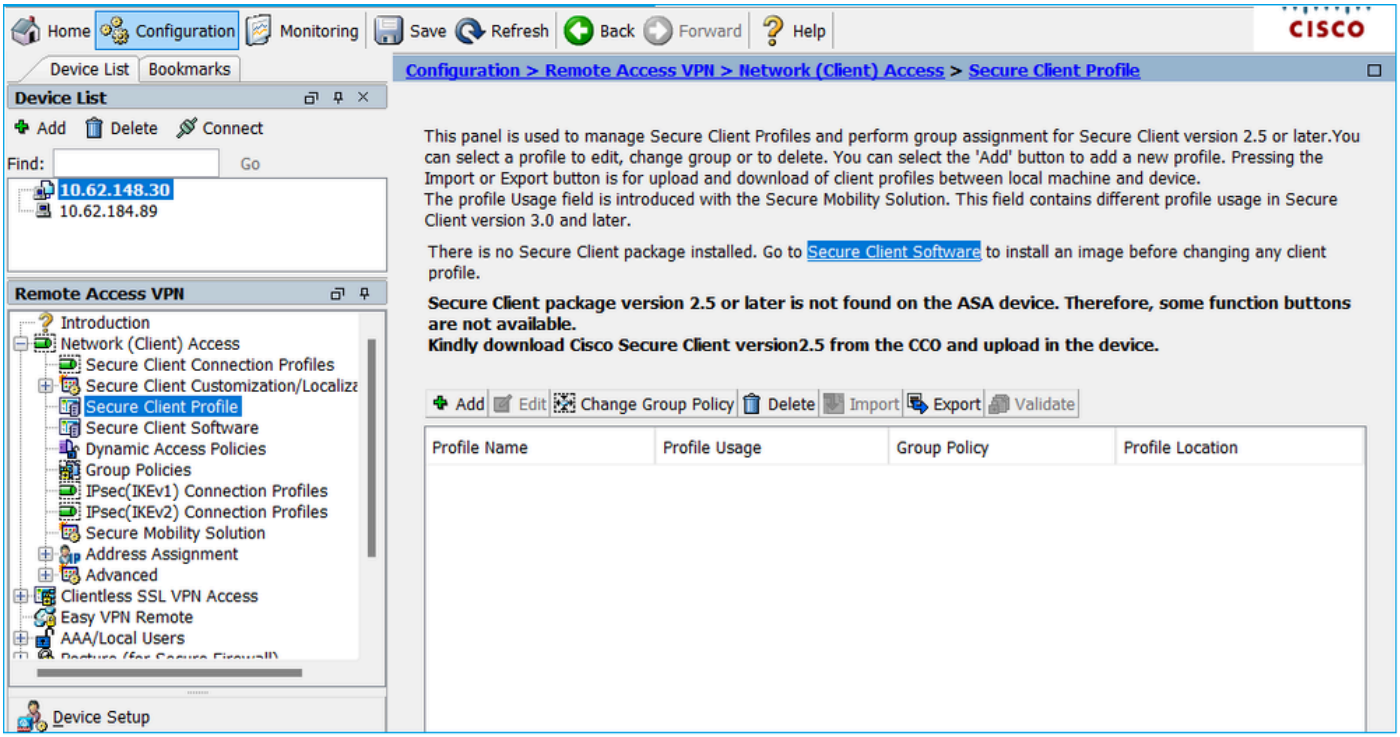
Risoluzione degli altri problemi di ASDM

Problema 1. Impossibile accedere a Secure Client Profile su ASDM

L'interfaccia utente di ASDM mostra quanto segue:



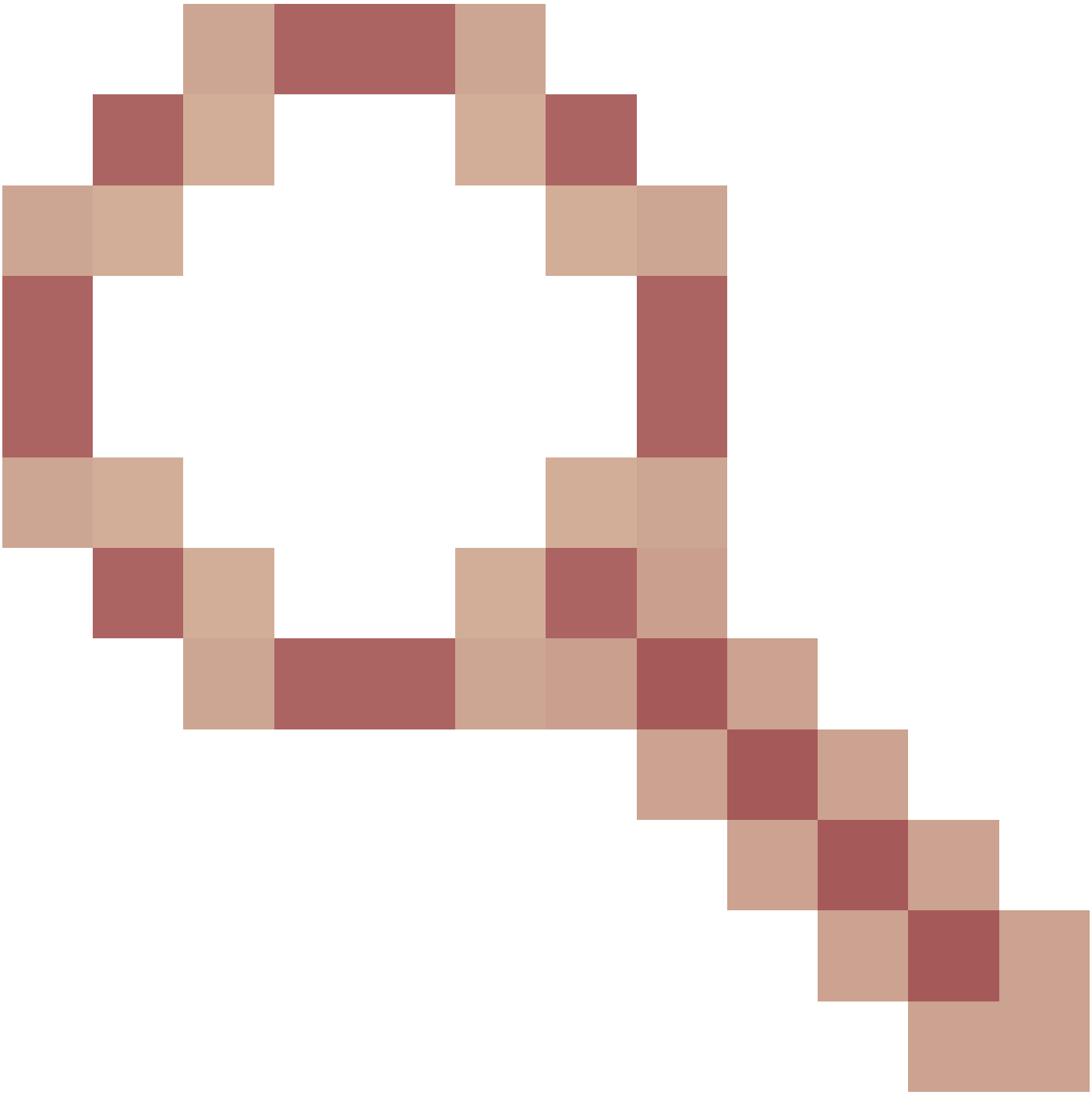
Mentre l'output previsto dell'interfaccia utente è:



Risoluzione dei problemi - Passi consigliati

Questo è un difetto noto:

Cisco, ID bug CSCwi56155



Impossibile accedere a Secure Client Profile su ASDM

Soluzioni:

Declassa AnyConnect

o

Aggiornamento di ASDM alla versione 7.20.2

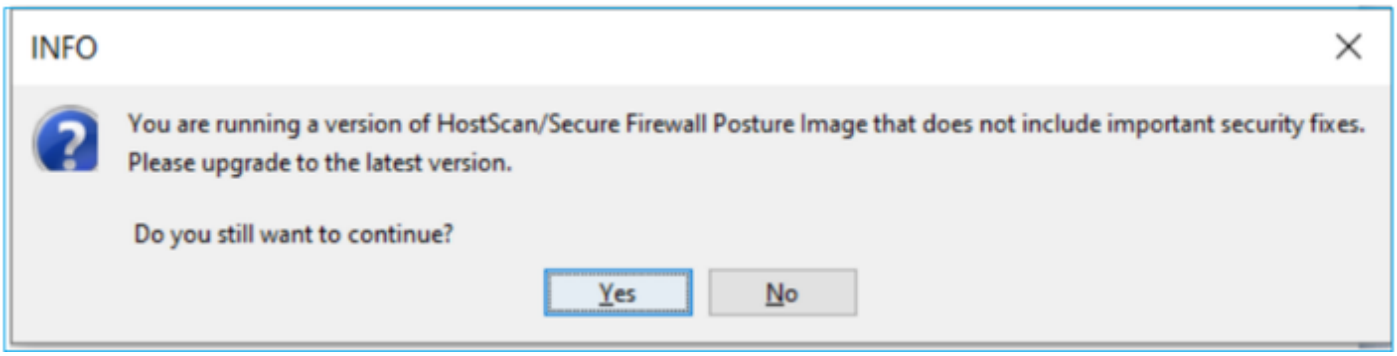
Per ulteriori informazioni, consultate le note sui difetti. È inoltre possibile effettuare la sottoscrizione al difetto in modo da ricevere una notifica sugli aggiornamenti relativi al difetto.

Problema 2. L'ASDM visualizza la schermata popup per hostscan - l'immagine non

include importanti correzioni alla sicurezza

L'interfaccia utente di ASDM mostra quanto segue:

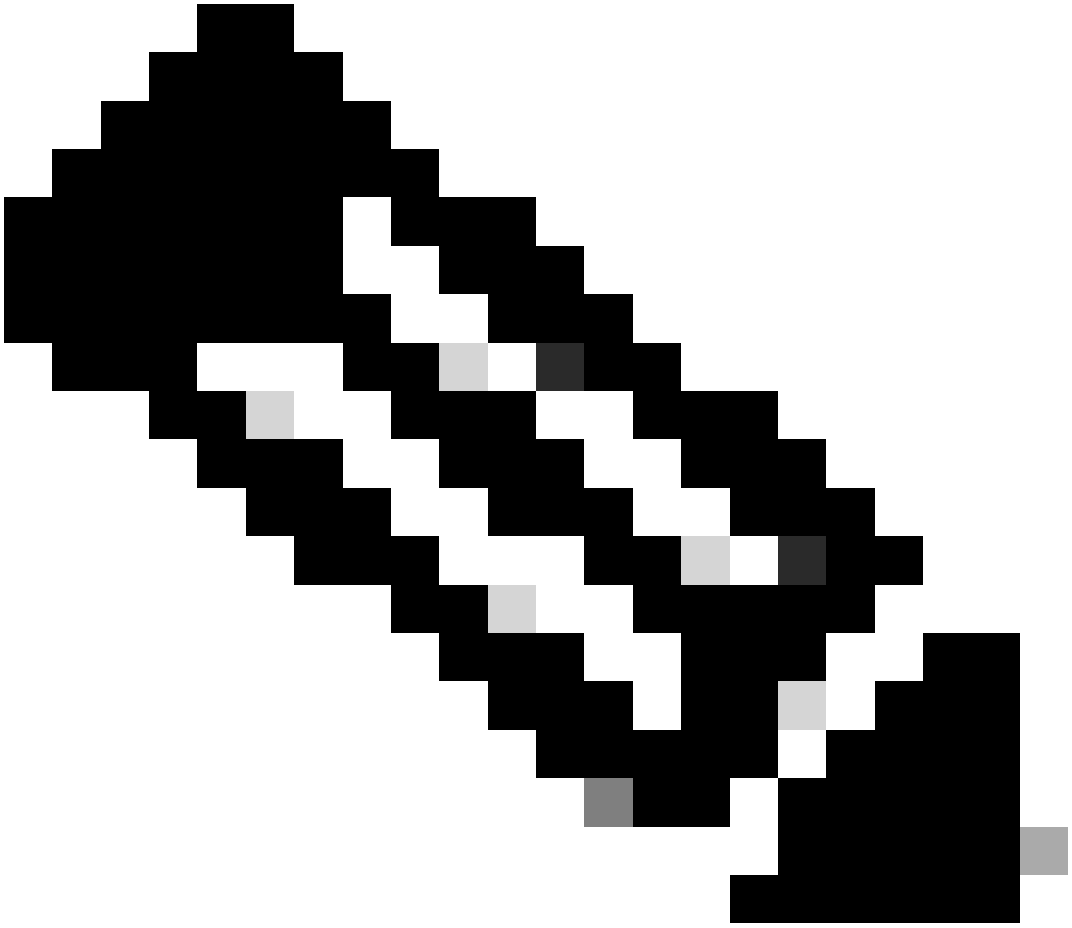
"Si sta eseguendo una versione dell'immagine HostScan/SecureFirewall Posture che non include importanti correzioni per la sicurezza. Eseguire l'aggiornamento alla versione più recente. Vuoi ancora continuare?"



Risoluzione dei problemi - Passi consigliati

Questo è un difetto noto:

Cisco, ID bug CSCwc62461
Quando si accede alla schermata popup ASDM per hostscan (l'immagine non include importanti correzioni alla sicurezza)



Nota: Questo problema è stato risolto nelle recenti versioni del software ASDM. Per ulteriori informazioni, controllare i dettagli del difetto.

Soluzione temporanea:

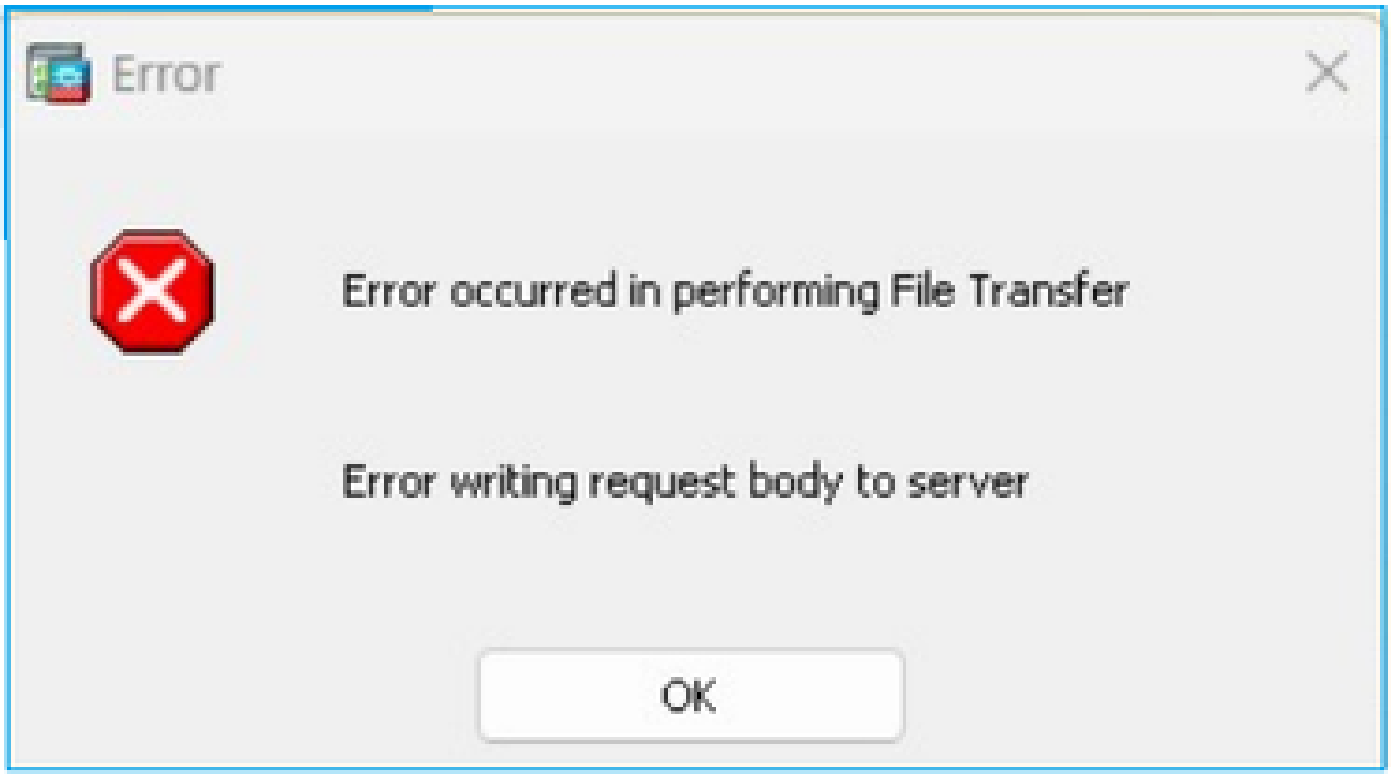
Fare clic su 'Sì' nella finestra di messaggio popup per continuare.

Problema 3. ASDM "Errore durante la scrittura del corpo della richiesta sul server" durante la copia di un'immagine su ASDM

L'interfaccia utente di ASDM mostra quanto segue:

Errore durante il trasferimento dei file

Errore durante la scrittura del corpo della richiesta nel server



Risoluzione dei problemi - Azioni consigliate

Questo è un difetto noto rilevato da:

Cisco, ID bug CSCtf74236

ASDM "Errore durante la scrittura del corpo della richiesta sul server" durante la copia dell'immagine

Soluzione alternativa

Utilizzare SCP/TFTP per trasferire il file.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).