Problemen met ASDM-configuratie, -verificatie en andere problemen oplossen

Inhoud

Inleiding

Achtergrond

Problemen met ASDM-configuratie oplossen

- Probleem 1. ASDM toont geen toegangscontrolelijsten (ACL) die op een interface worden toegepast
- Probleem 2. Inconsistentie in aantal treffers tussen ASA CLI en ASDM UI
- Probleem 3. "FOUT: % Ongeldige invoer gedetecteerd bij '^'-markering." foutbericht bij bewerken van een ACL in ASDM
- Probleem 4. De "FOUT: ACL is gekoppeld aan routekaart en inactief niet ondersteund. in plaats daarvan verwijder de "acl" foutmelding in specifieke gevallen
- Probleem 5. Geen logbestanden in ASDM Real-time Log Viewer voor impliciet ontkende verbindingen
- Probleem 6. ASDM bevriest wanneer u een netwerkobject of object-groep probeert aan te passen
- Probleem 7. ASDM kan extra regels voor toegangscontrolelijsten voor verschillende interfaces tonen
- Probleem 8. Real-time logbestanden zijn niet beschikbaar in de Real-time logviewer
- Probleem 9. De kolommen Datum en Tijd zijn leeg in de Real Time log ViewerProbleemoplossing - Aanbevolen acties
- Probleem 10. Vastlegging op ASDM kan mislukken na overschakeling op een andere context in een multi-context ASA
- Probleem 11. ASDM-sessie abrupt beëindigd bij overschakelen tussen verschillende contexten
- Probleem 12. ASDM sluit willekeurig af/eindigt met het bericht "ASDM heeft een bericht ontvangen van het ASA-apparaat dat moet worden losgemaakt. ASDM sluit nu af."
- Probleem 13. ASDM-lading hangt met het bericht "Verificatie FirePOWER login"
- Probleem 14. ASDM toont het beheer/de configuratie van de FirePOWER-module niet
- Probleem 15. De beveiligde clientprofielen zijn niet toegankelijk op ASDM
- Probleem 16. Kan de XML-profielen van beveiligd clientprofiel niet bewerken op ASDM
- Probleem 17. Beveiligde clientafbeeldingen ontbreken na configuratiewijzigingen
- Probleem 18. Ondoelmatige opdrachten voor http server sessie-timeout en http server idle-timeout
- Probleem 19. Fout in Dap.xml-kopie op ASDM
- Probleem 20. Op ASDM zichtbare IKE-beleidslijnen en IPSEC-voorstellen
- Probleem 21. ASDM toont het bericht "Het wachtwoord voor inschakelen is niet ingesteld. Stel het nu in."
- Probleem 2. ASDN-object verdwijnt na het vernieuwen van ASDM UI
- Probleem 23. Kan clientprofielen voor AnyConnect niet bewerken voor versies eerder dan 4.5
- Probleem 24. Kan niet naar het tabblad Servicebeleid bewerken > Handelingen regels > ASA FirePOWER Inspection navigeren
- Probleem 25. AnyConnect Image versie 5.1 en AnyConnect-profieleditor op ASDM
- Probleem 26. Type AAA-kenmerken (Radius/LDAP) zijn niet zichtbaar in ASDM
- Probleem 27. 'De Post Quantum sleutel kan niet leeg zijn' fout wordt getoond op ASDM

Probleem 28. ASDM geeft geen resultaten weer bij gebruik van de optie "waar gebruikt"

Probleem 29. Waarschuwingsbericht "[Network Object] kan niet worden verwijderd omdat dit in het volgende" wordt gebruikt bij het verwijderen van een netwerkobject

Probleem 30. Gebruiksproblemen met het tabblad Network Objects/Group in ASDM

Problemen met ASDM-verificatie oplossen

Probleem 1. Aanmelden bij ASDM mislukt

Probleem 2. Opdrachtautorisatie ASDM is mislukt

Probleem 3. Configureer ASDM alleen-lezen toegang

Probleem 4. ASDM Multi-Factor Authenticatie (MFA)

Probleem 5. ASDM-configuratie voor externe verificatie

Probleem 6. ASDM LOKALE verificatie mislukt

Probleem 7. ASDM eenmalig wachtwoord

Probleem 8. Verbindingsprofiel toont niet alle methoden

Probleem 9. ASDM-sessie leidt niet tot time-out

Probleem 10. ASDM LDAP-verificatie mislukt

Probleem 11. ASDM WebVPN DAP-configuratie ontbreekt

Probleemoplossing voor ASDM Andere problemen

Probleem 1. Kan geen toegang krijgen tot beveiligd clientprofiel op ASDM

Probleem 2. ASDM toont pop-up voor hostscan - afbeelding bevat geen belangrijke beveiligingsoplossingen

Probleem 3. ASDM "Fout bij schrijven verzoek lichaam naar server" bij het kopiëren van een afbeelding via ASDM

Inleiding

In dit document wordt het proces voor het oplossen van problemen bij de configuratie, verificatie en andere problemen van Adaptieve Security Applicatie Apparaatbeheer (ASDM) beschreven.

Achtergrond

Het document maakt samen met deze documenten deel uit van de ASDM-serie probleemoplossing:

Link1<>

Link2<>

Link3<>

Problemen met ASDM-configuratie oplossen

Probleem 1. ASDM toont geen toegangscontrolelijsten (ACL) die op een interface worden toegepast

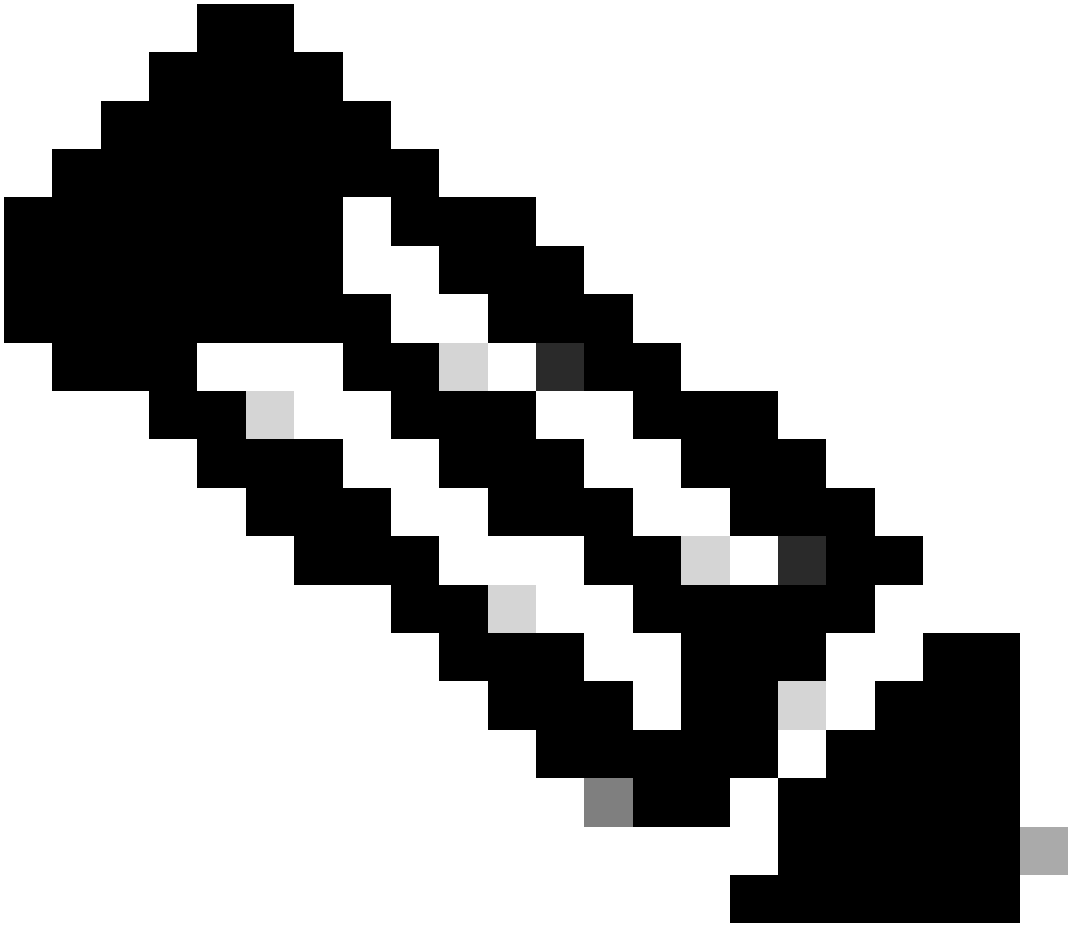
ASDM toont geen toegangscontrolelijsten (ACL) die op een interface worden toegepast, alhoewel er een geldige toegangsgroep is die op de interface in kwestie wordt toegepast. In plaats daarvan staat er "0 inkomende regels". Deze symptomen worden waargenomen L3 en L2 ACL zowel geconfigureerd in toegangsgroep configuratie voor een interface:

<#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
```

Probleemoplossing - Aanbevolen acties

Raadpleeg de software-id van Cisco bug-id CSCwj14147 "ASDM kan toegangsgroepsconfiguratie niet laden als L2- en L3-telefoons zijn gemengd."



Opmerking: Dit defect is verholpen in recente ASDM-softwarereleases. Controleer de gebreken voor meer informatie.

Probleem 2. Inconsistentie in aantal treffers tussen ASA CLI en ASDM UI

De vermeldingen voor het aantal treffers in de ASDM zijn niet consistent met het aantal treffers in de toegangslijst zoals gemeld door de opdracht toegangslijst tonen op uitvoer van de firewall.

Probleemoplossing - Aanbevolen acties

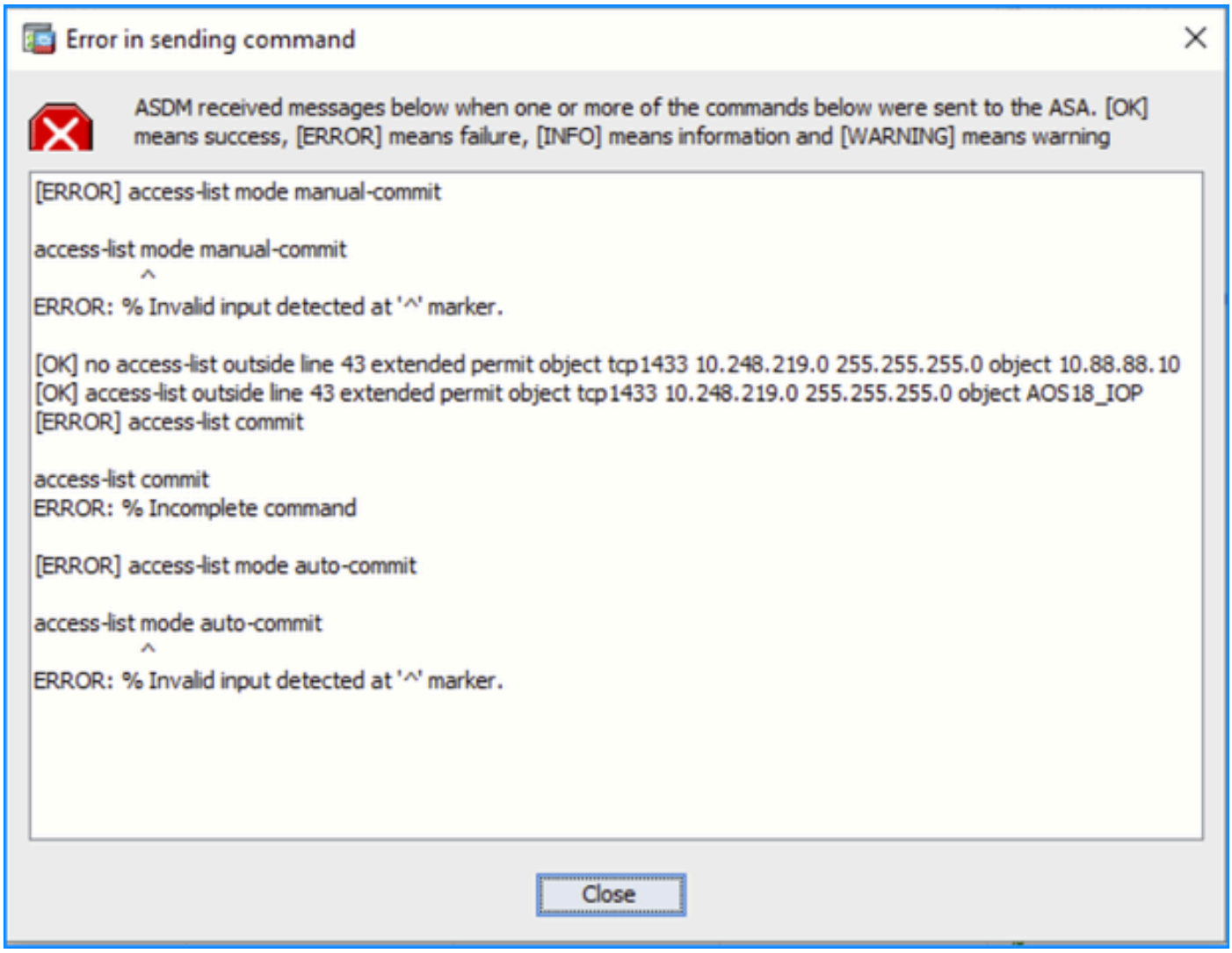
Raadpleeg de software-id van Cisco-bug CSC38377 "ENH: ASDM moet ACL-hash op de ASA gebruiken en niet lokaal calceren" en Cisco-bug-id CSCtq38405"ENH: ASA heeft een mechanisme nodig om ACL-hashinformatie aan ASD te geven"

Probleem 3. "FOUT: % Ongeldige invoer gedetecteerd bij '^'-markering." foutbericht

bij bewerken van een ACL in ASDM

De "FOUT: % Ongeldige invoer gedetecteerd bij '^'-markering." Er wordt een foutmelding weergegeven bij het bewerken van een ACL in ASDM:

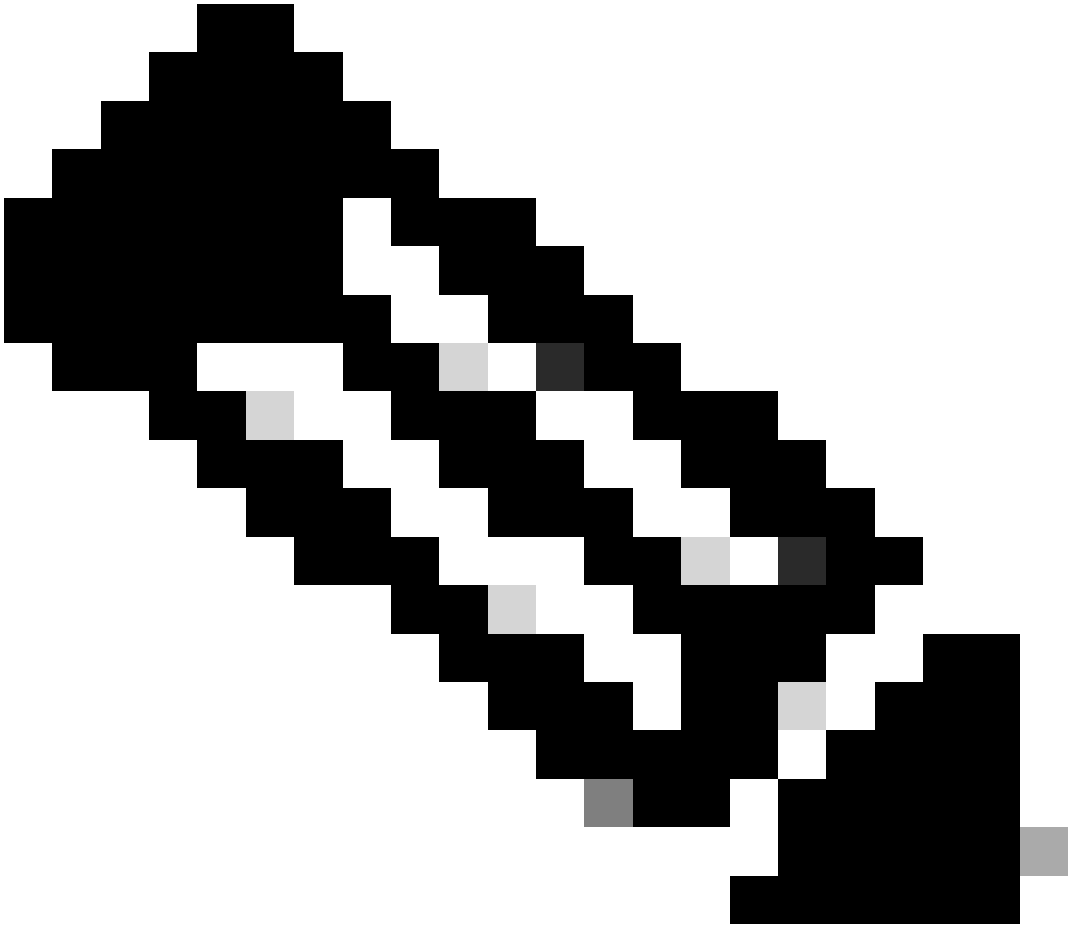
```
[ERROR] access-list mode manual-commit access-list mode manual-commit
                     ^
ERROR: % Invalid input detected at '^' marker.
[OK] no access-list ACL1 line 1 extended permit tcp object my-obj-1 object my-obj-2 eq 12345
[ERROR] access-list commit access-list commit
ERROR: % Incomplete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



Probleemoplossing - Aanbevolen acties

Raadpleeg de software CSC5064 van Cisco bug-id "Edit an entry (ACL) from ASDM geeft een

fout. Bij gebruik van ASDM met OpenJRE/Oracle - versie 7.12.2" en Cisco bug-id CSCvp8926 "Opdrachtopdrachten verzenden terwijl toegangslijst wordt verwijderd".



Opmerking: Deze tekortkomingen zijn verholpen in recente ASDM-softwarereleases. Controleer de gebreken voor meer informatie.

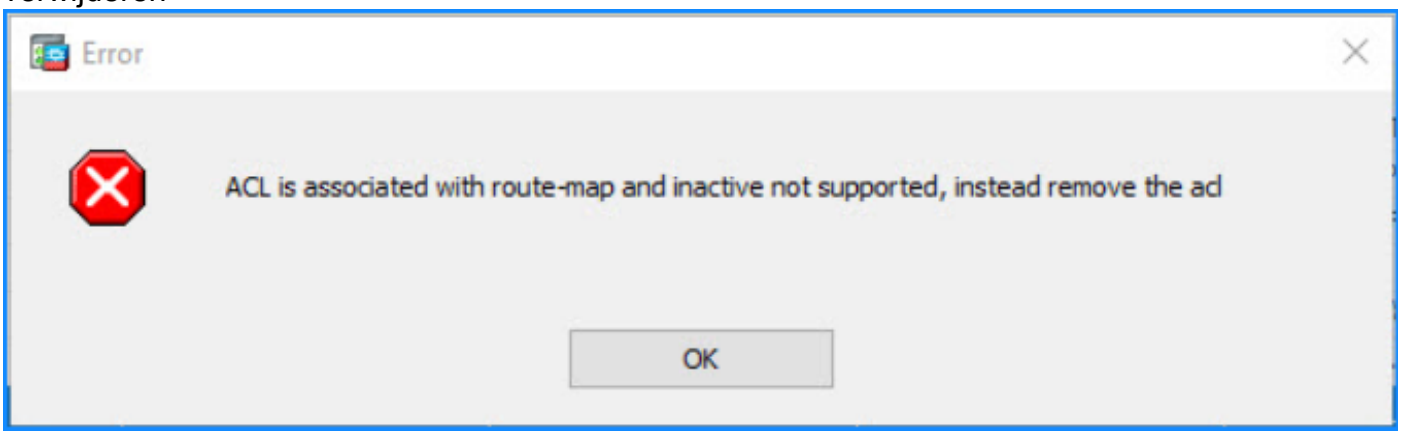
Probleem 4. De "FOUT: ACL is gekoppeld aan routekaart en inactief niet ondersteund, in plaats daarvan verwijder de "acl" foutmelding in specifieke gevallen

De "FOUT: ACL wordt geassocieerd met route-kaart en inactief niet ondersteund, in plaats daarvan verwijder de "acl" foutmelding wordt getoond in één van deze gevallen:

1. Bewerk een ACL in ASDM die wordt gebruikt in een op beleid gebaseerde routeringsconfiguratie:

firewall (config)# toegang-lijst pbr lijn 1 vergunning ip elke host 192.0.2.1

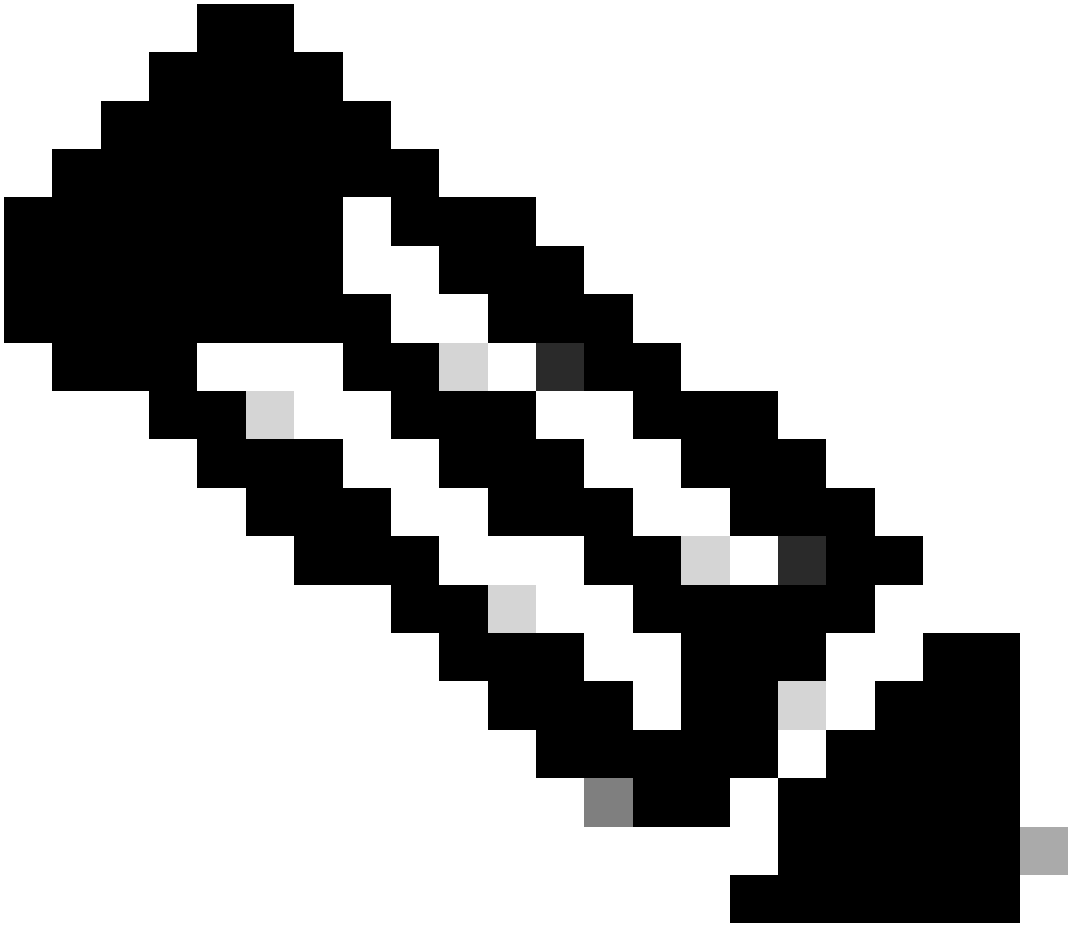
FOUT: ACL is gekoppeld aan routekaart en inactief niet ondersteund, in plaats daarvan de client verwijderen



2. Bewerk een ACL ASDM > Configuration -> Remote Access VPN -> Network (Client) Access > Dynamic Access policy

Probleemoplossing - Aanbevolen acties

1. Raadpleeg de software-id van Cisco-bug CSCwb57615 "PBR-toegangslijst configureren met lijnnummer mislukt." De tijdelijke oplossing is om de "line" parameter uit te sluiten van de configuratie.
2. Raadpleeg de software Cisco bug-id CSCwe34665 "Kan de ACL-objecten niet bewerken als deze al in gebruik is en de uitzondering krijgt".



Opmerking: Deze defects zijn hersteld in recente ASA softwarereleases. Controleer de gebreken voor meer informatie.

Probleem 5. Geen logbestanden in ASDM Real-time Log Viewer voor impliciet ontkende verbindingen

ASDM Real-time Log Viewer toont geen logbestanden voor impliciet ontkende verbindingen.

Probleemoplossing - Aanbevolen acties

Het impliciete ontkennen aan het eind van de toegangslijst genereert geen syslog. Als u al ontkend verkeer syslog wilt genereren, voegt u regel toe met het logwoord aan het eind van de ACL.

Probleem 6. ASDM bevriest wanneer u een netwerkobject of object-groep probeert aan te passen

ASDM blokkeert bij het wijzigen van een netwerkobject of een object-groep op de pagina Configuratie > Firewall > Toegangsregels onder het tabblad Adressen. De gebruiker kan geen van de parameters in het venster van het netwerkobject bewerken wanneer dit probleem zich voordoet.

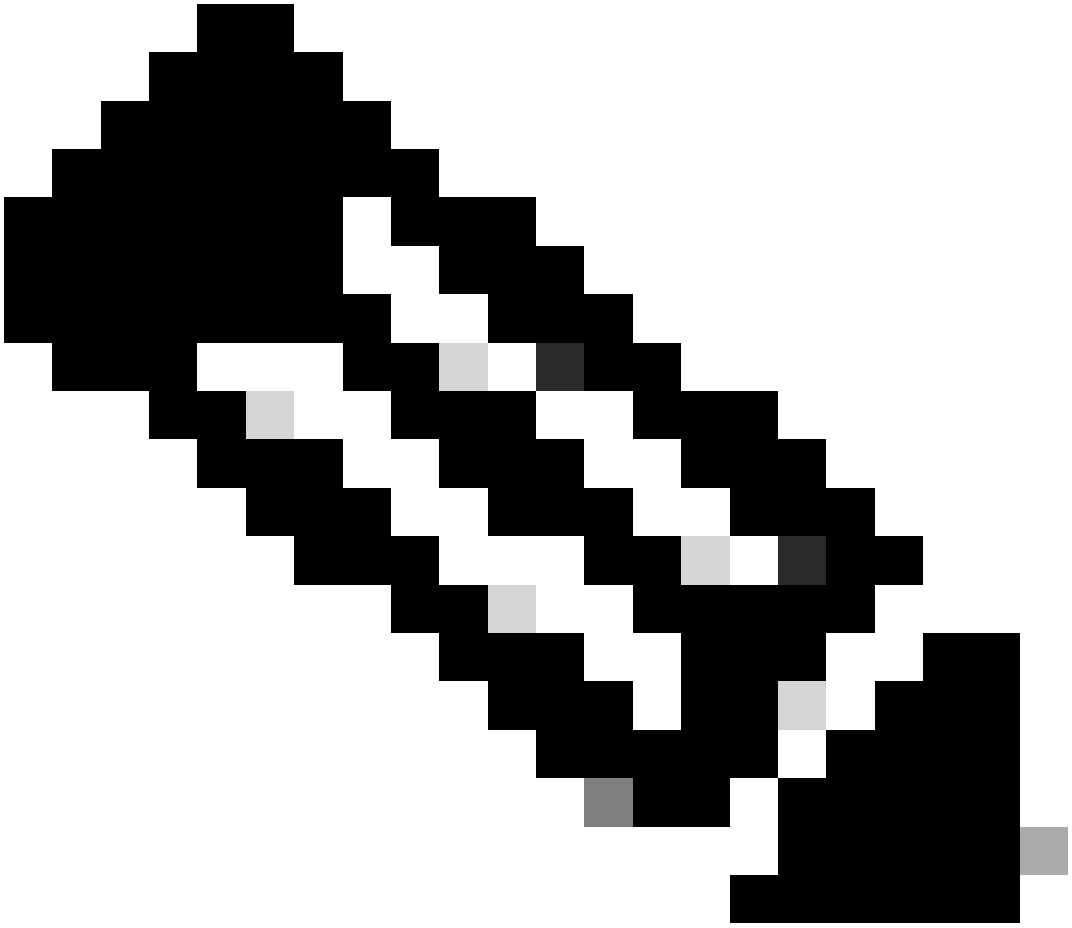
Probleemoplossing - Aanbevolen acties

Raadpleeg de software Cisco bug-id CSCwj1250 "ASDM bevriest bij het bewerken van netwerkobjecten of netwerkobjectgroepen". De tijdelijke oplossing is om de topN verzameling van hoststatistieken uit te schakelen:

<#root>

```
ASA(config)#
```

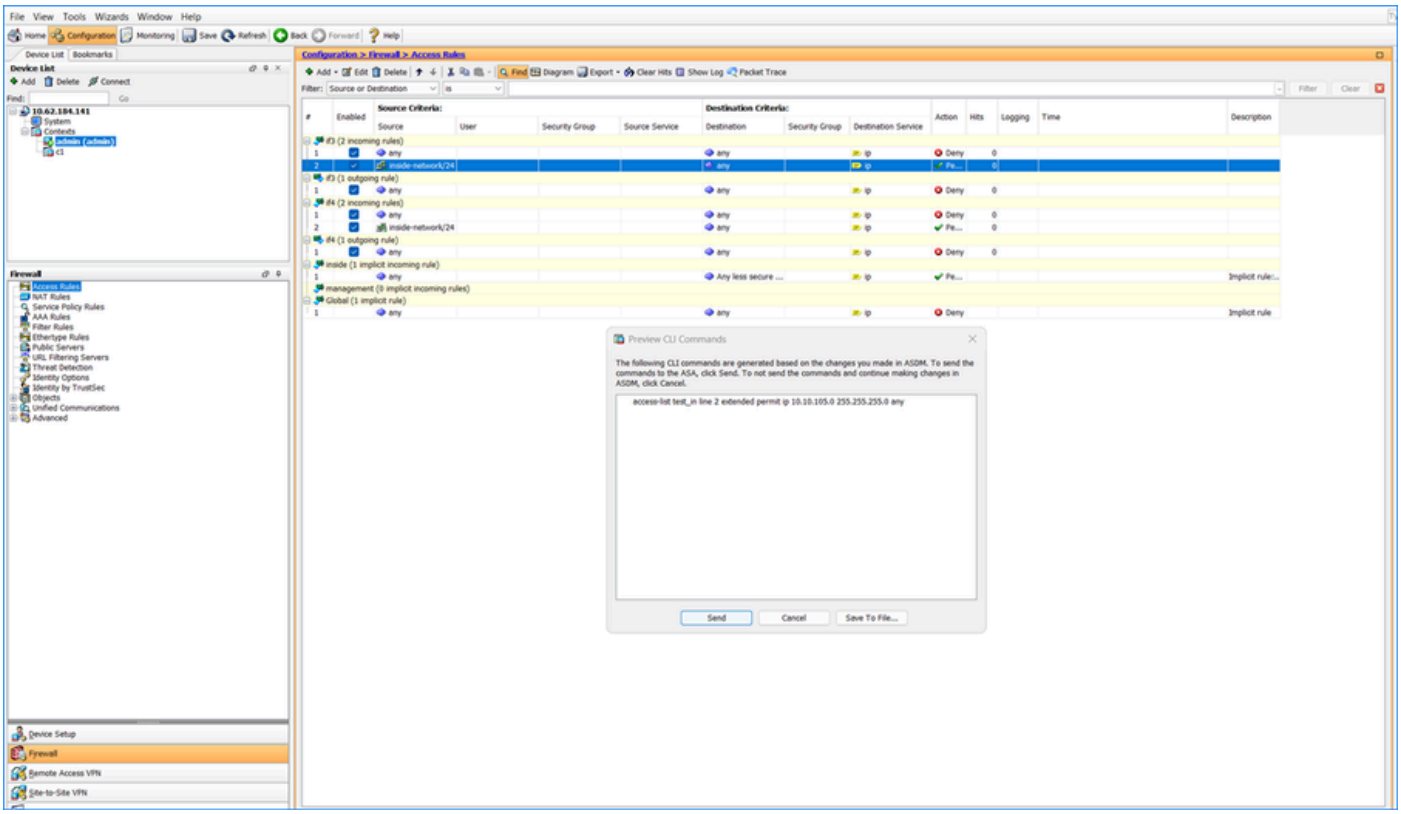
no hpm topN enable



Opmerking: Dit defect is verholpen in recente ASDM-softwarereleases. Controleer de gebreken voor meer informatie.

Probleem 7. ASDM kan extra toegangscontrolelijstregels voor verschillende interfaces tonen

ASDM kan extra regels van de toegangscontrolelijst voor verschillende interfaces tonen als een interface-level toegangscontrolelijst wordt gewijzigd. In dit voorbeeld, werd inkomende regel#2 toegevoegd aan interface if3 ACL. ASDM toont ook #2 voor de interface if4, terwijl deze regel niet door de gebruiker is geconfigureerd. De opdrachtvoorbeeld laat correct één wijziging zien die in behandeling is. Dit is een probleem met de gebruikersinterface.



Probleemoplossing - Aanbevolen acties

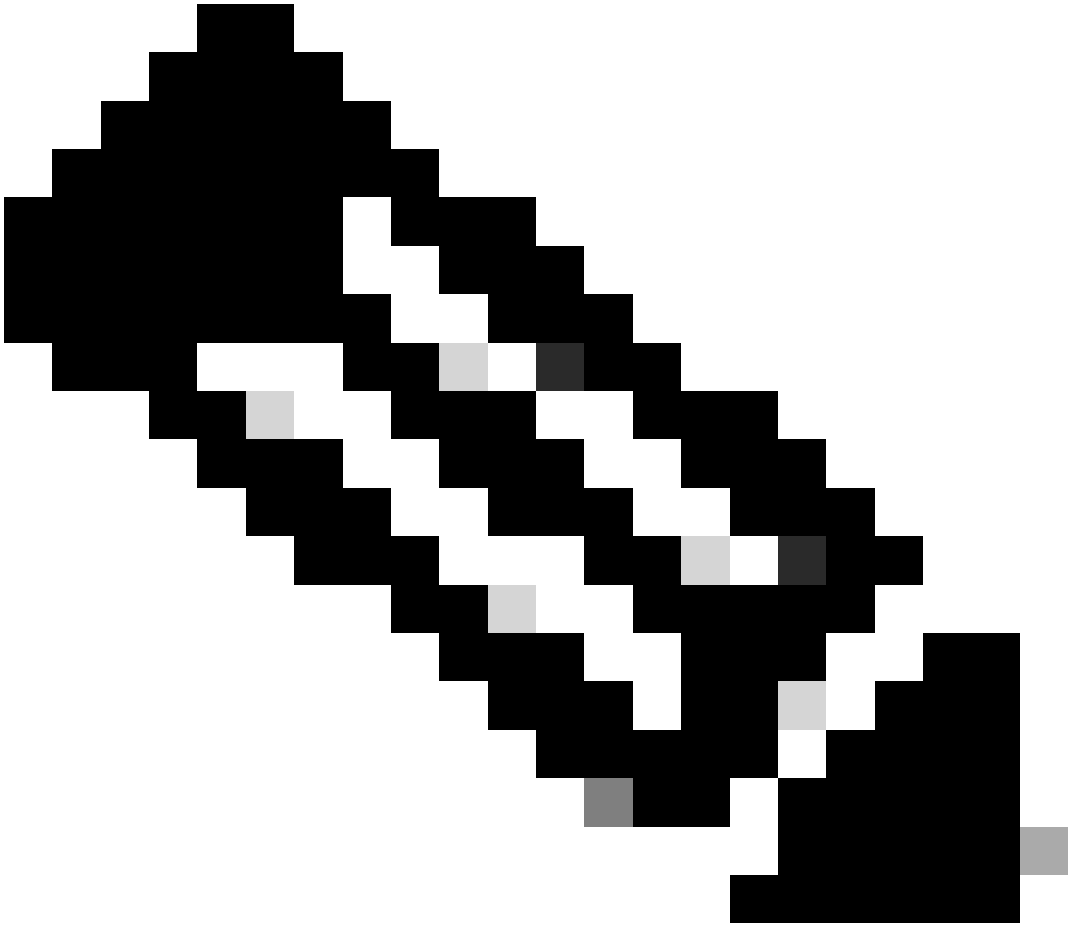
Raadpleeg de software-id van Cisco-bug CSCwm71434 "ASDM kan dubbele toegangslijsten voor de interface weergeven".

Probleem 8. Real-time logbestanden zijn niet beschikbaar in de Real-time logviewer

Er worden geen logbestanden weergegeven in de Real Time Log Viewer

Probleemoplossing - Aanbevolen acties

1. Zorg ervoor dat de logboekregistratie is geconfigureerd. Raadpleeg ASDM Book 1: Cisco ASA Series General Operations/ASDM-configuratiehandleiding, 7.22, hoofdstuk: Logboekregistratie.
2. Raadpleeg de software-id van Cisco bug CSCvf82966 "ASDM - Vastlegging: Kan realtime logbestanden niet bekijken".

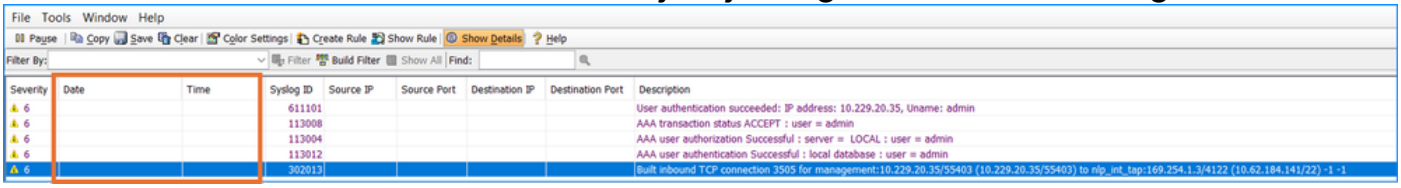


Opmerking: Dit defect is verholpen in recente ASDM-softwarereleases. Controleer de gebreken voor meer informatie.

Referenties

- ASDM-boek 1: Cisco ASA Series General Operations/ASDM-configuratiehandleiding, 7.22, hoofdstuk: Logboekregistratie.

Probleem 9. De kolommen Datum en Tijd zijn leeg in de Real Time log Viewer



Probleemoplossing - Aanbevolen acties

1. Controleer of het tijdstempelformaat RFC5424 voor vastlegging wordt gebruikt:

```
<#root>

#

show run logging


logging enable

logging timestamp rfc5424
```

2. Als de logindeling RFC5424 wordt gebruikt, raadpleegt u de software Cisco bug-id CSCvs52212 "ASDM ENH: mogelijkheid voor Event Log Viewers om ASA-syslogs met rfc5424 tijdstempelformaat weer te geven". De tijdelijke oplossing is te voorkomen dat het RFC5424-formaat wordt gebruikt:

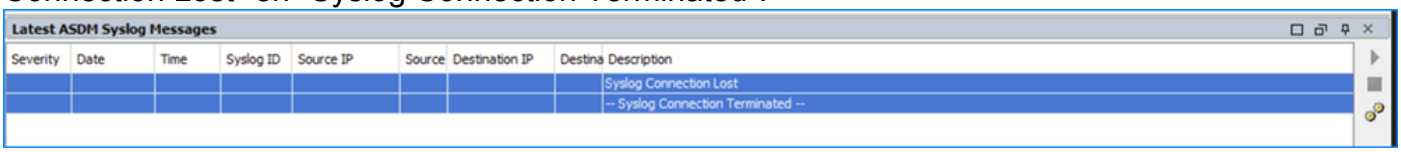
```
<#root>

firewall(config)#

no logging timestamp rfc5424


firewall(config)#

logging timestamp
```

3. Raadpleeg ook de software defect Cisco bug-id CSCwh70323 "Time-postzegel ontbreekt voor bepaalde syslog-berichten die naar syslog-server zijn verzonden".

Opmerking: Dit defect is verholpen in recente ASDM-softwarereleases. Controleer de gebreken voor meer informatie.

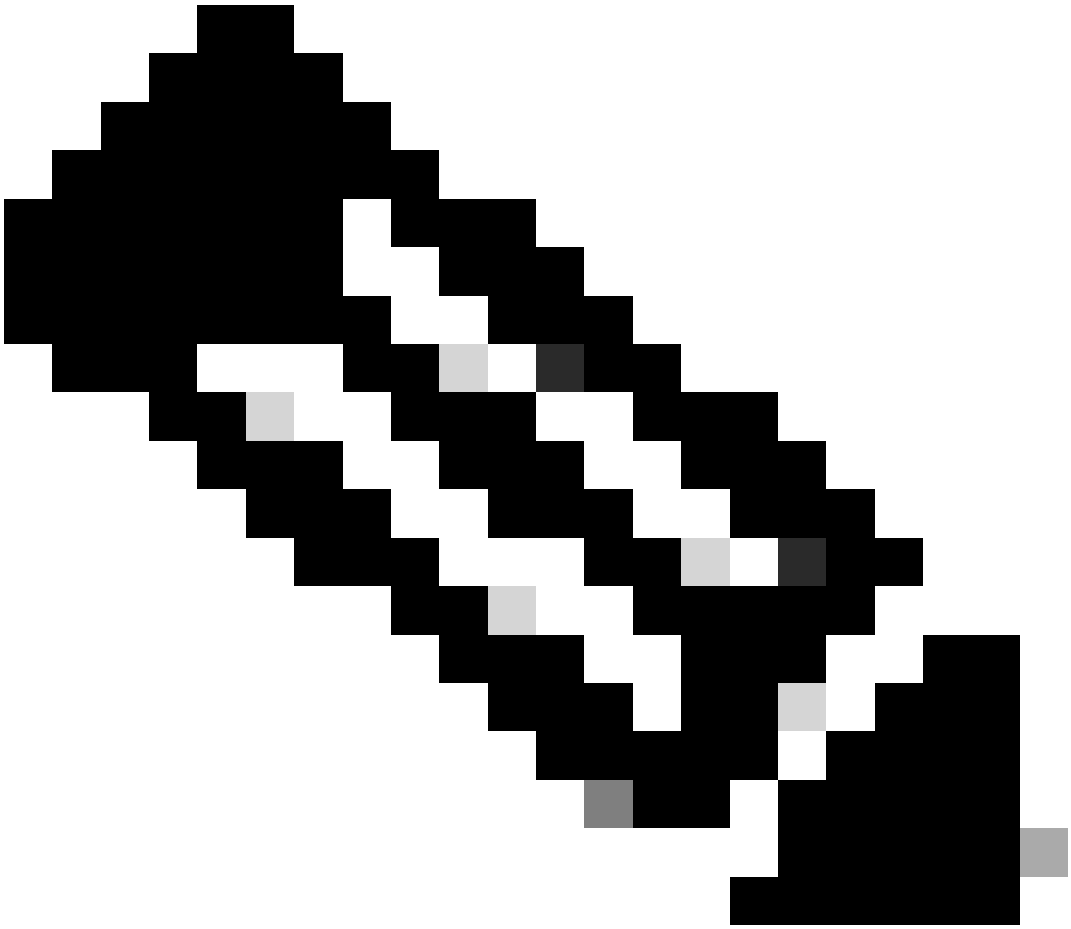
Probleem 10. Vastlegging op ASDM kan mislukken na overschakeling naar een andere context in een multi-context ASA

Op het tabblad Nieuwste ASDM Syslog Berichten op de pagina Home staan de berichten "Syslog Connection Lost" en "Syslog Connection Terminated":



Probleemoplossing - Aanbevolen acties

Zorg ervoor dat de logboekregistratie is geconfigureerd. Raadpleeg de software-id van Cisco bug CSCvz15404 "ASA: Meervoudige contextmodus : ASDM-vastlegging stopt, wanneer overgeschakeld op een andere context".



> Opmerking: Dit defect is verholpen in recente ASDM-softwarereleases. Controleer de gebreken voor meer informatie.

Probleem 11. ASDM-sessie abrupt beëindigd bij overschakeling tussen verschillende contexten

De ASDM-sessie wordt abrupt beëindigd wanneer er wordt overgeschakeld tussen verschillende contexten met de foutmelding "Het maximale aantal beheersessies voor protocol http of user bestaat al. Probeer het later opnieuw." Deze logboeken worden getoond in de syslogberichten:

```
%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
```

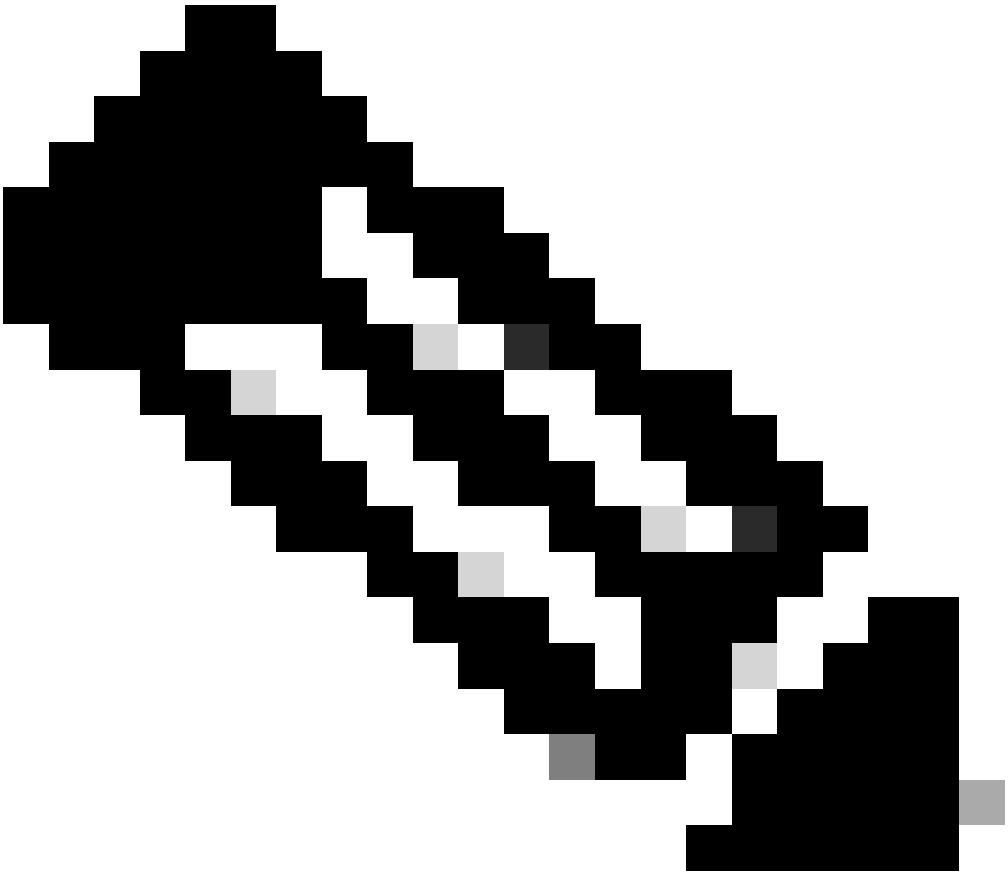
Probleemoplossing - Aanbevolen acties

1. Controleer of het huidige ASDM-brongebruik de limiet heeft bereikt. In dit geval wordt het aantal geweigerde tellers verhoogd:

<#root>

```
firewall #

show resource usage resource ASDM


Resource                Current        Peak      Limit        Denied Context
ASDM

5

           5

5


10

 admin
```

2. Raadpleeg de software-id van Cisco bug-id CSCvs72378 "ASDM-sessie wordt abrupt beëindigd bij het schakelen tussen verschillende contexten".



Opmerking: Dit defect is verholpen in recente ASA softwarereleases. Controleer de gebreken voor meer informatie.

3. Als de softwareversie de oplossing voor de Cisco bug ID CSCvs72378 heeft en de huidige bron de limiet heeft bereikt, koppel dan een aantal bestaande ASDM-sessies los. U kunt de ASDM sluiten of, als alternatief, HTTPS-verbindingen wissen voor het IP-adres van de host waarop ASDM wordt uitgevoerd. In dit voorbeeld wordt ervan uitgegaan dat de HTTP-server op ASDM op de standaard HTTPS-poort 443 draait:

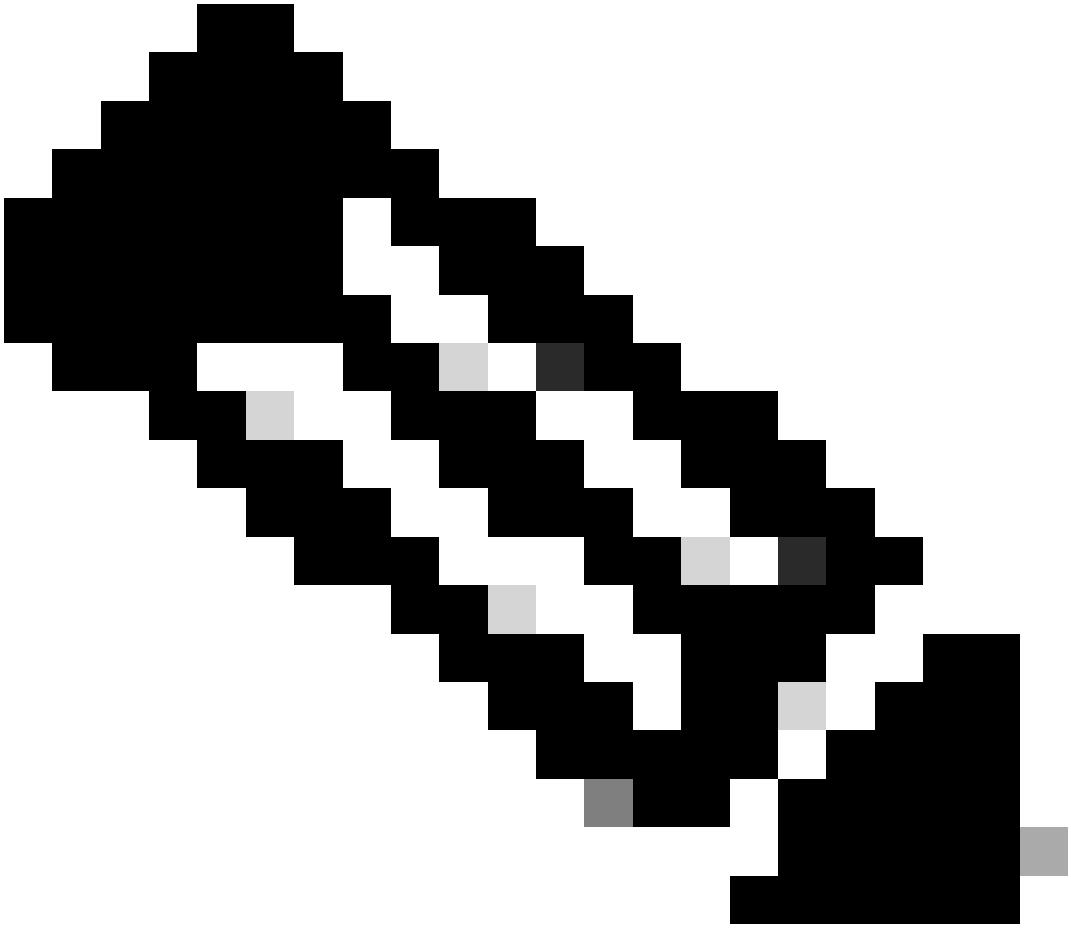
```
<#root>

#

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
```

Probleem 12. ASDM sluit/eindigt willekeurig met het bericht "ASDM heeft een bericht ontvangen van het ASA-apparaat om de verbinding te verbreken. ASDM sluit nu af."

Op multi-context ASA, sluit ASDM willekeurig/eindigt met het bericht "ASDM ontving een bericht van het ASA apparaat om los te koppelen. ASDM sluit nu af.".

Probleemoplossing - Aanbevolen acties

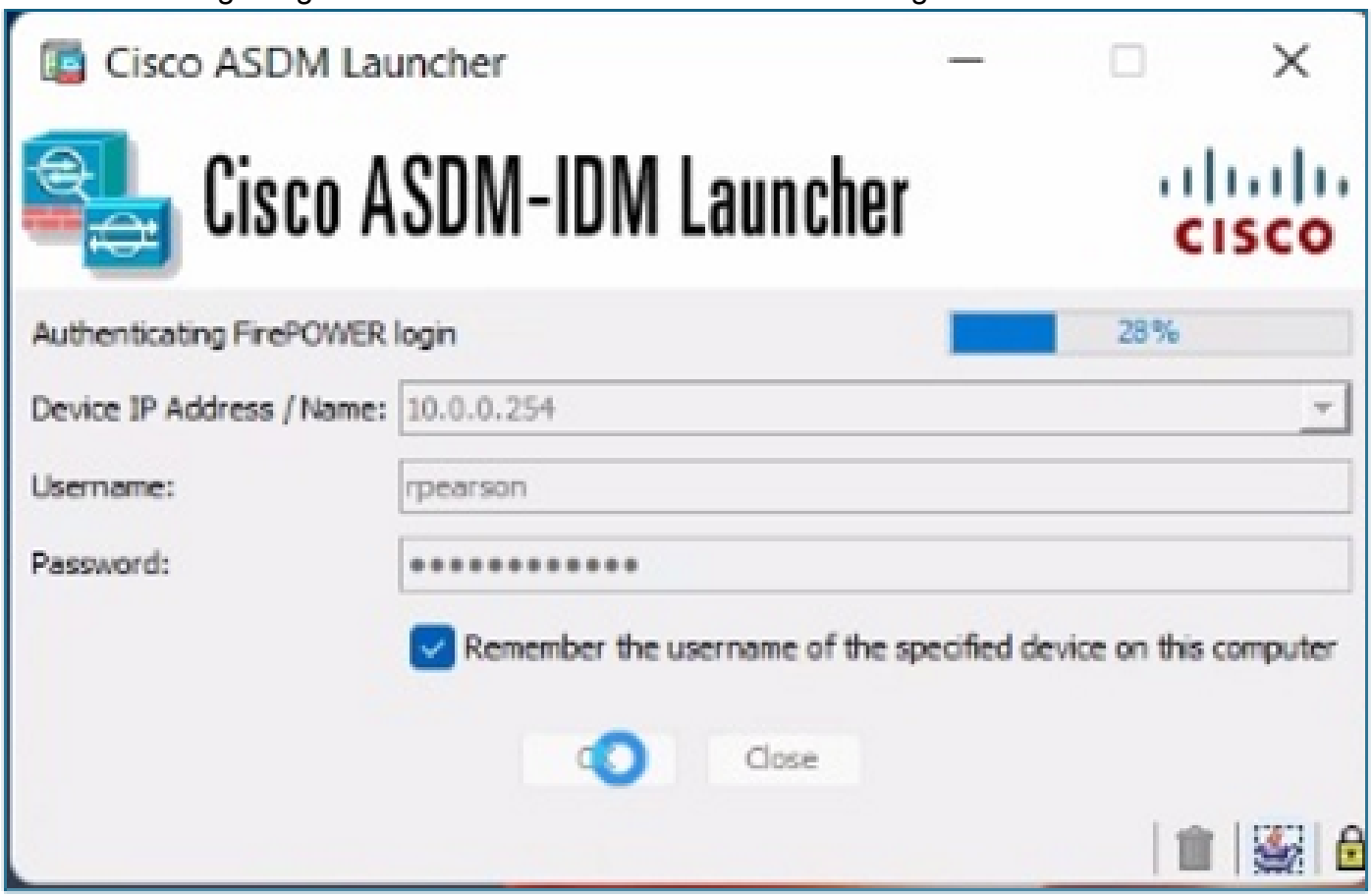
Raadpleeg het softwaredefect Cisco bug-id CSCwh04395 "ASDM-toepassing sluit willekeurig af/eindigt met een waarschuwingsbericht bij installatie in meerdere context".



Opmerking: Dit defect is verholpen in recente ASA softwarereleases. Controleer de gebreken voor meer informatie.

Probleem 13. ASDM-lading hangt met het bericht "Verificatie FirePOWER login"

De ASDM-lading hangt aan het bericht "Verificatie FirePOWER login":



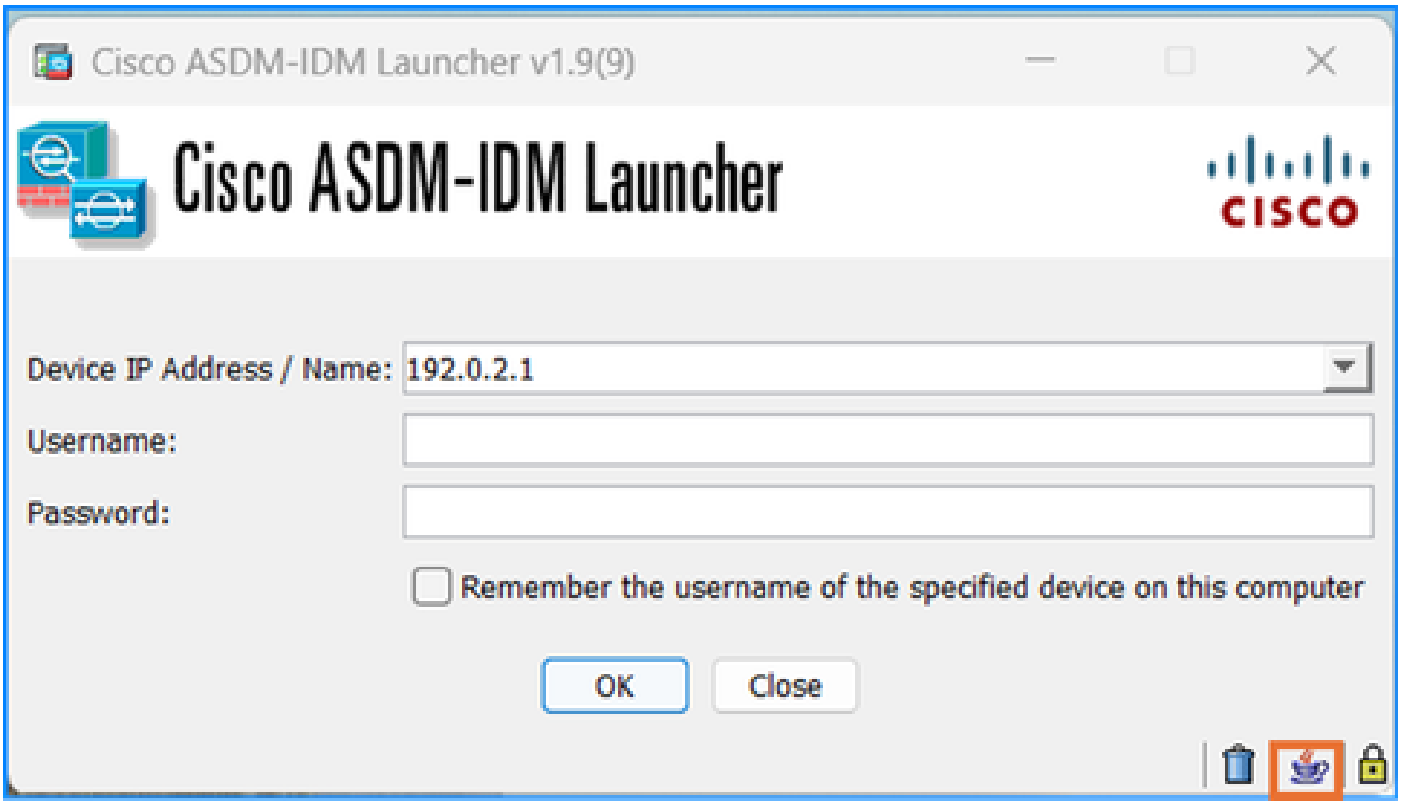
De Java-consolelogboeken tonen het bericht "Mislukt verbinding te maken met FirePower, doorgaan zonder het":

<#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)
```

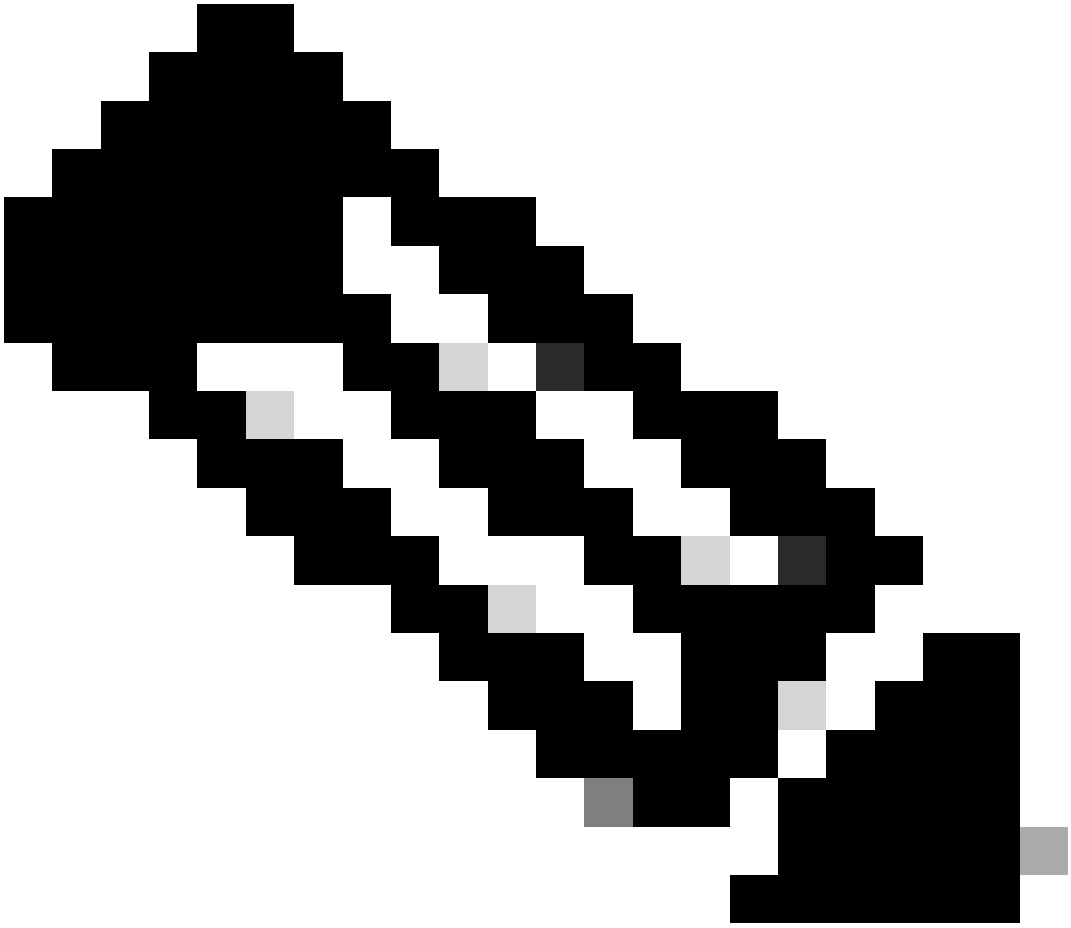
Om dit symptoom te verifiëren, activeert u Java console logs:



Probleemoplossing - Aanbevolen acties

Raadpleeg de software-id van Cisco-bug CSCwe15164 "ASA: ASDM kan geen SFR-tabbladen weergeven totdat deze via zijn CLI 'ontwaakt'." Workaround-stappen:

1. Sluit de ASDM-beheerder.
2. Krijg SSH toegang tot de SFR en switch gebruiker naar root (sudo su).
3. Nadat u de bovenstaande stappen hebt uitgevoerd, start u de ASDM opnieuw en kunt u de SFR-tabbladen (Firepower) laden.



Opmerking: Dit defect is verholpen in recente FirePOWER-softwarereleases. Controleer de gebreken voor meer informatie.

Probleem 14. ASDM toont het beheer/de configuratie van de FirePOWER-module niet

De Firepower module configuratie is niet beschikbaar op ASDM.

Probleemoplossing - Aanbevolen acties

1. Zorg ervoor dat de ASA, ASDM, Firepower module en besturingssysteemversies compatibel zijn. Raadpleeg de Cisco Secure Firewall ASA release Notes, Cisco Secure Firewall ASDM release Notes, Compatibiliteit met Cisco Secure Firewall ASA:

- ASA 9.14/ASDM 7.14/Firepower 6.6 is de definitieve versie voor de ASA FirePOWER-

module op de ASA 5525-X, 5545-X en 5555-X.
- ASA 9.12/ASDM 7.12/Firepower 6.4.0 is de definitieve versie voor de ASA FirePOWER-module op de ASA 5515-X en 5585-X.
- ASA 9.9/ASDM 7.9(2)/Firepower 6.2.3 is de definitieve versie voor de ASA FirePOWER-module op de ASA 5506-X-serie en 5512-X.
- ASDM-versies zijn achterwaarts compatibel met alle voorgaande ASA-versies, tenzij anders vermeld. ASDM 7.13(1) kan bijvoorbeeld een ASA 5516-X beheren op ASA 9.10(1).
- ASDM wordt niet ondersteund voor FirePOWER-modulebeheer met ASA 9.8(4.45)+, 9.12(4.50)+, 9.14(4.14)+ en 9.16(3.19)+; je moet FMC gebruiken om de module met deze releases te beheren. Deze ASA releases vereisen ASDM 7.18(1.152) of hoger, maar ASDM-ondersteuning voor de ASA FirePOWER-module eindigde met 7.16.
- ASDM 7.13(1) en ASDM 7.14(1) ondersteunen ASA 5512-X, 5515-X, 5585-X en ASM niet; u moet upgraden naar ASDM 7.13(1.101) of 7.14(1.48) om de ASDM-ondersteuning te herstellen.

2. Als de versies compatibel zijn, controleert u of de module actief is:

<#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
```

Als de module is uitgeschakeld, kan de sw-module module reset opdracht worden gebruikt om de module te resetten en vervolgens de module software opnieuw te laden.

Referenties

- Opmerkingen over Cisco Secure Firewall ASA release
- Opmerkingen over Cisco Secure Firewall ASDM-release
- Compatibiliteit met Cisco Secure Firewall ASA

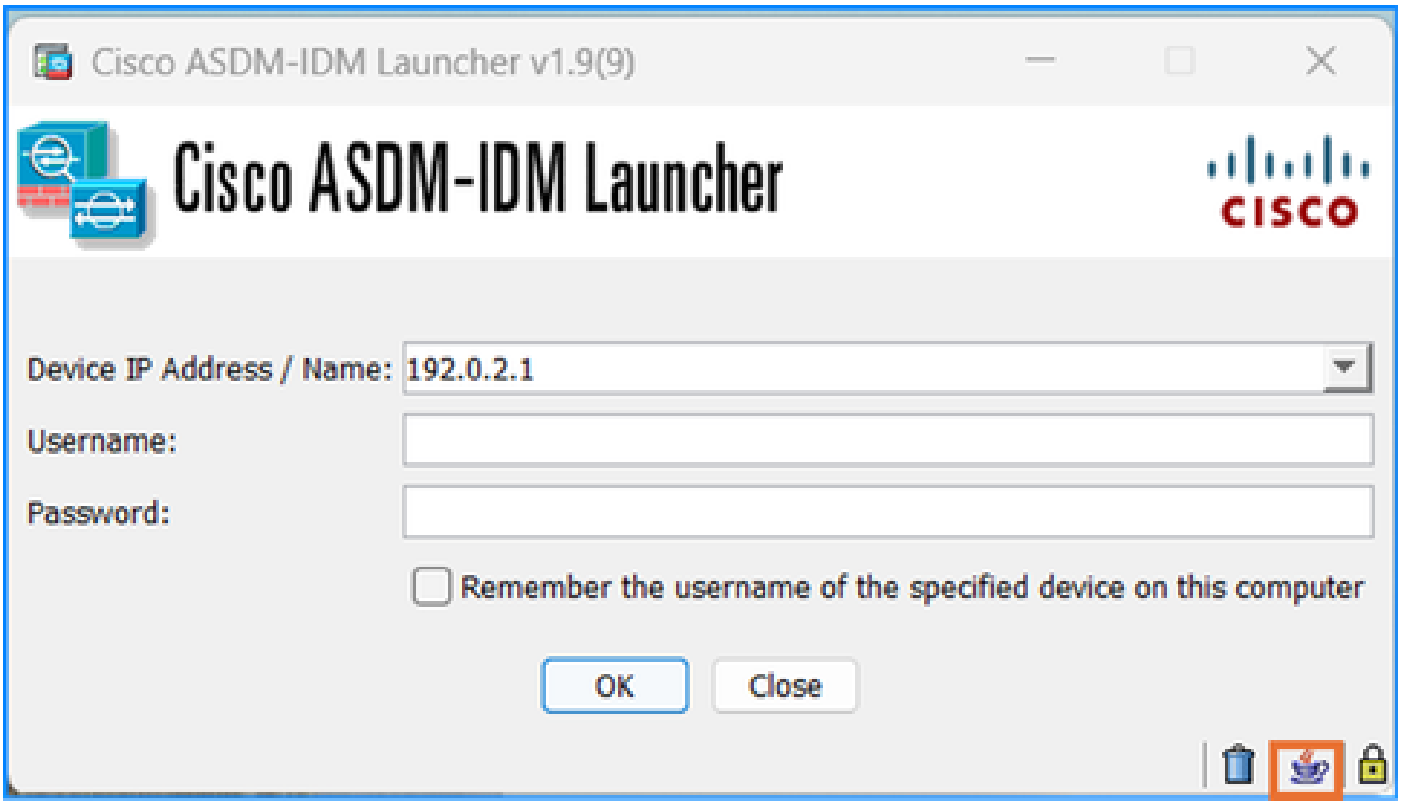
Probleem 15. De beveiligde clientprofielen zijn niet toegankelijk op ASDM

Java console logboeken tonen de "java.lang.ArrayIndexOutOfBoundsException: 3" foutbericht:

<#root>

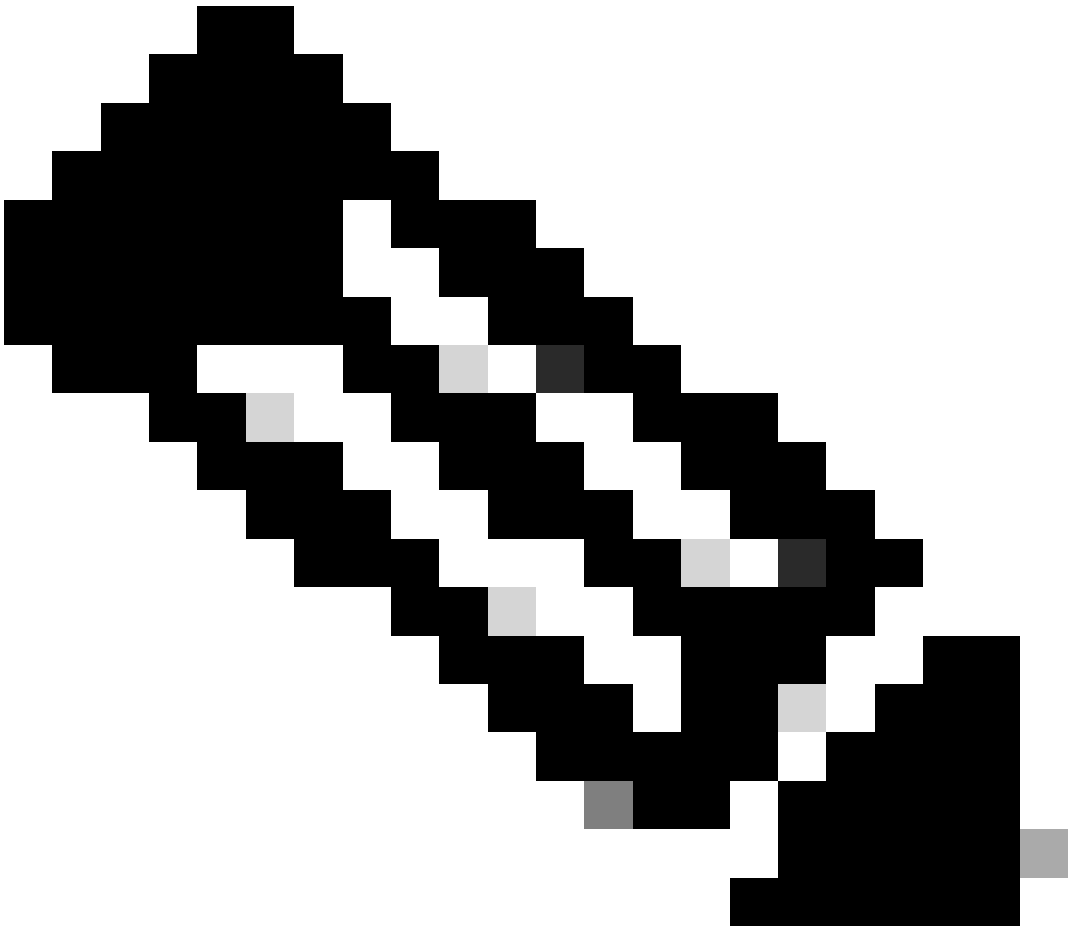
```
LifeTime value : -1 HTTP Enable Status : nps-servers-ige

java.lang.ArrayIndexOutOfBoundsException: 3


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

Om dit symptoom te verifiëren, activeert u Java console logs:



Probleemoplossing - Aanbevolen acties

Raadpleeg de software-id van Cisco bug-id CSC56155 "Kan geen toegang krijgen tot beveiligd clientprofiel op ASDM".



> Opmerking: Dit defect is verholpen in recente ASDM-softwarereleases. Controleer de gebreken voor meer informatie.

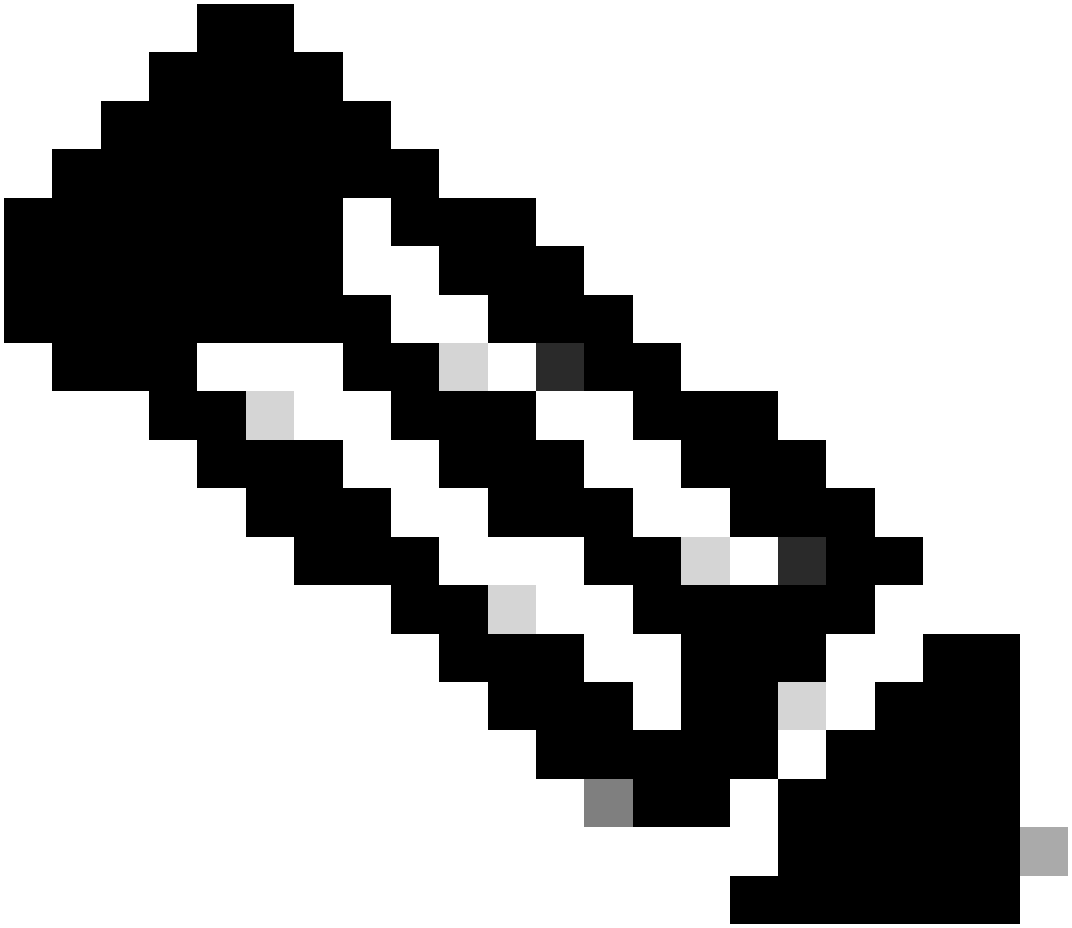
Probleem 16. Kan de XML-profielen van beveiligd clientprofiel niet bewerken op ASDM

De Secure Client Profile XML-profielen in ASDM Configuration > Remote Access VPN > Network (Client) Access kunnen niet worden bewerkt op een ASA-apparaat als er op de schijf een AnyConnect-afbeelding aanwezig is die ouder is dan versie 4.8.

De foutmelding "Er is geen profiel editor plugin in uw Secure Client Image op het apparaat. Ga naar Network (Client) Access > Secure Client Software en installeer de Secure Client Image versie 2.5 of hoger en probeer het nogmaals" wordt weergegeven.

Probleemoplossing - Aanbevolen acties

Raadpleeg de software-id van Cisco bug-id CSCwk64399 "ASDM - Kan beveiligde clientprofiel niet bewerken". De tijdelijke oplossing is om een ander AnyConnect-beeld met een lagere prioriteit in te stellen.



Opmerking: Dit defect is verholpen in recente ASDM-softwarereleases. Controleer de gebreken voor meer informatie.

Probleem 17. Beveiligde clientafbeeldingen ontbreken na configuratiewijzigingen

Nadat u wijzigingen hebt aangebracht in ASDM Configuration > Network (Client) Access > Secure Client Profile, ontbreken de afbeeldingen in Configuration > Network (Client) Access > Secure Client Software .

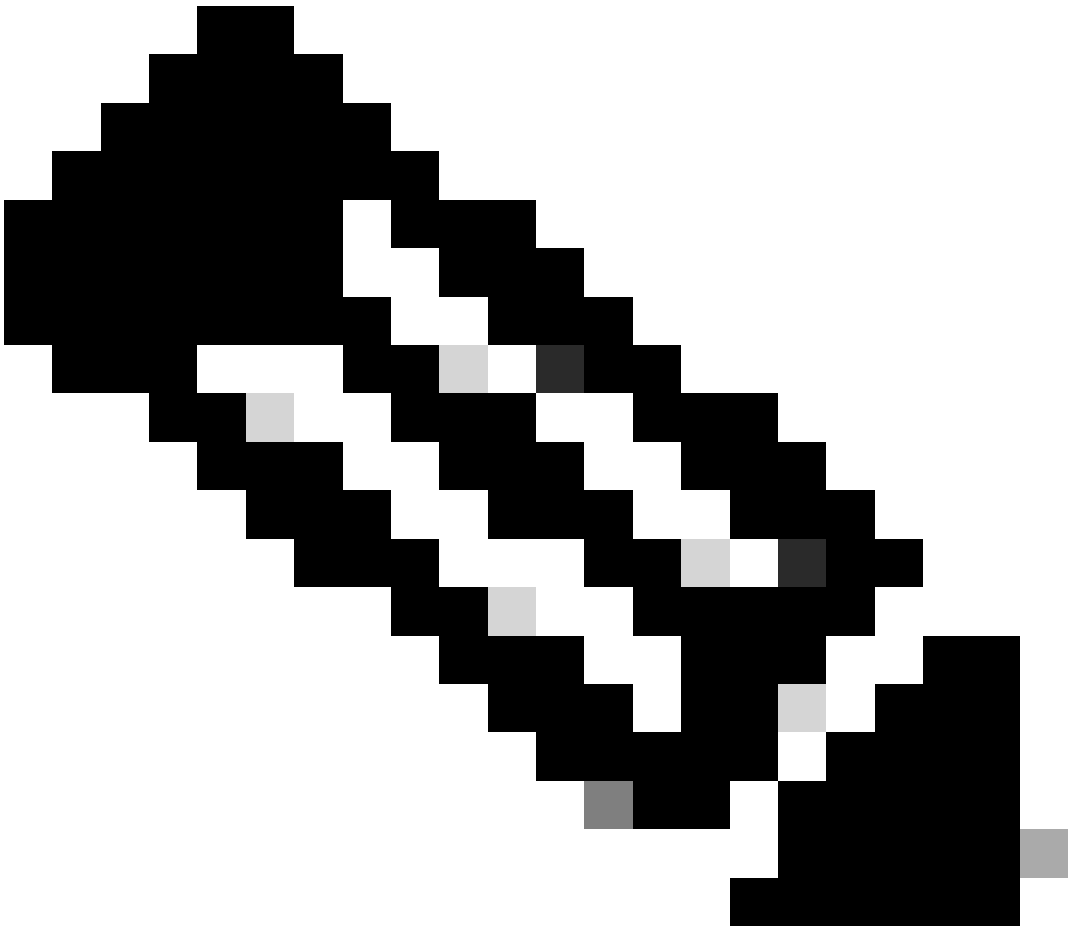
Probleemoplossing - Aanbevolen acties

Raadpleeg de software-id van Cisco-bug CSCwf23826 "Secure Client Software wordt niet weergegeven na wijziging van de Secure Client Profile Editor in ASDM". De tijdelijke opties:

- Klik op het pictogram Refresh in ASDM

OF

- ASDM sluiten en opnieuw openen



Opmerking: Dit defect is verholpen in recente ASDM-softwarereleases. Controleer de gebreken voor meer informatie.

Probleem 18. Ondoelmatige opdrachten voor http server sessie-timeout en http server idle-timeout

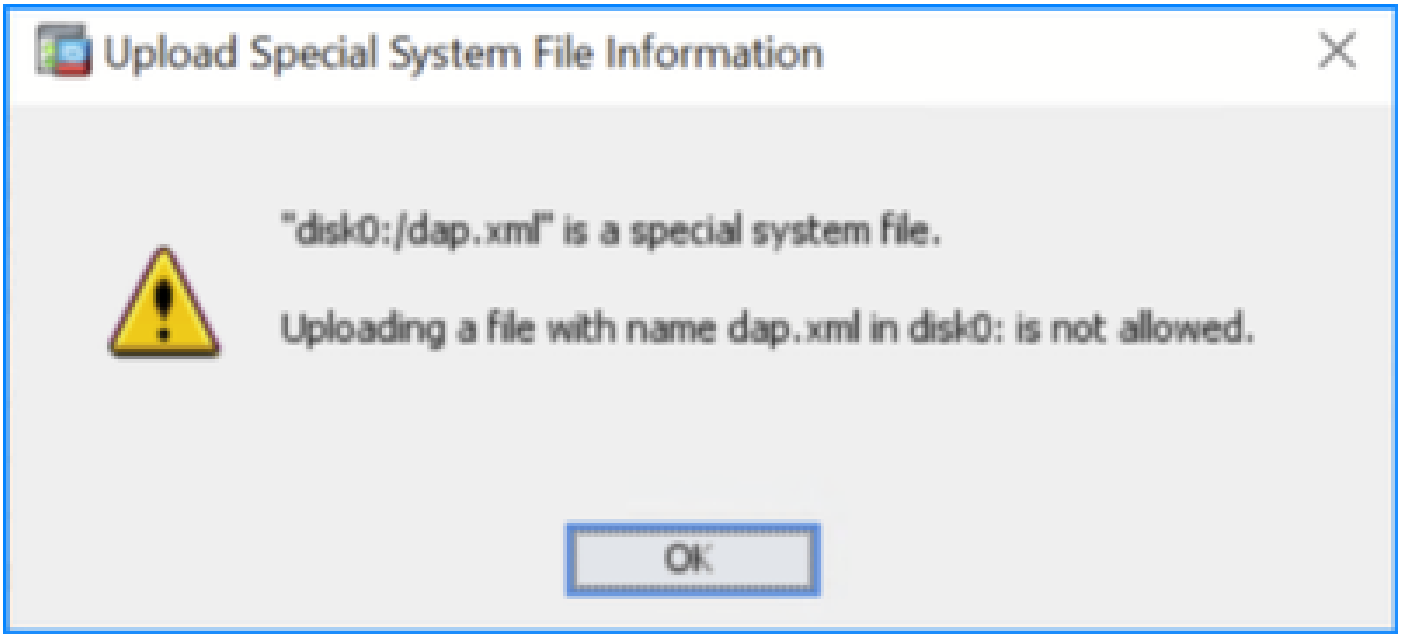
De opdrachten http server sessie-timeout en http server idle-timeout hebben geen effect in multi-context mode ASA.

Probleemoplossing - Aanbevolen acties

Raadpleeg de software Cisco bug-id CSC41707 "Support for http server timeout commando in multi-context modus". De opdrachten zijn configureerbaar, maar de waarden hebben geen effect.

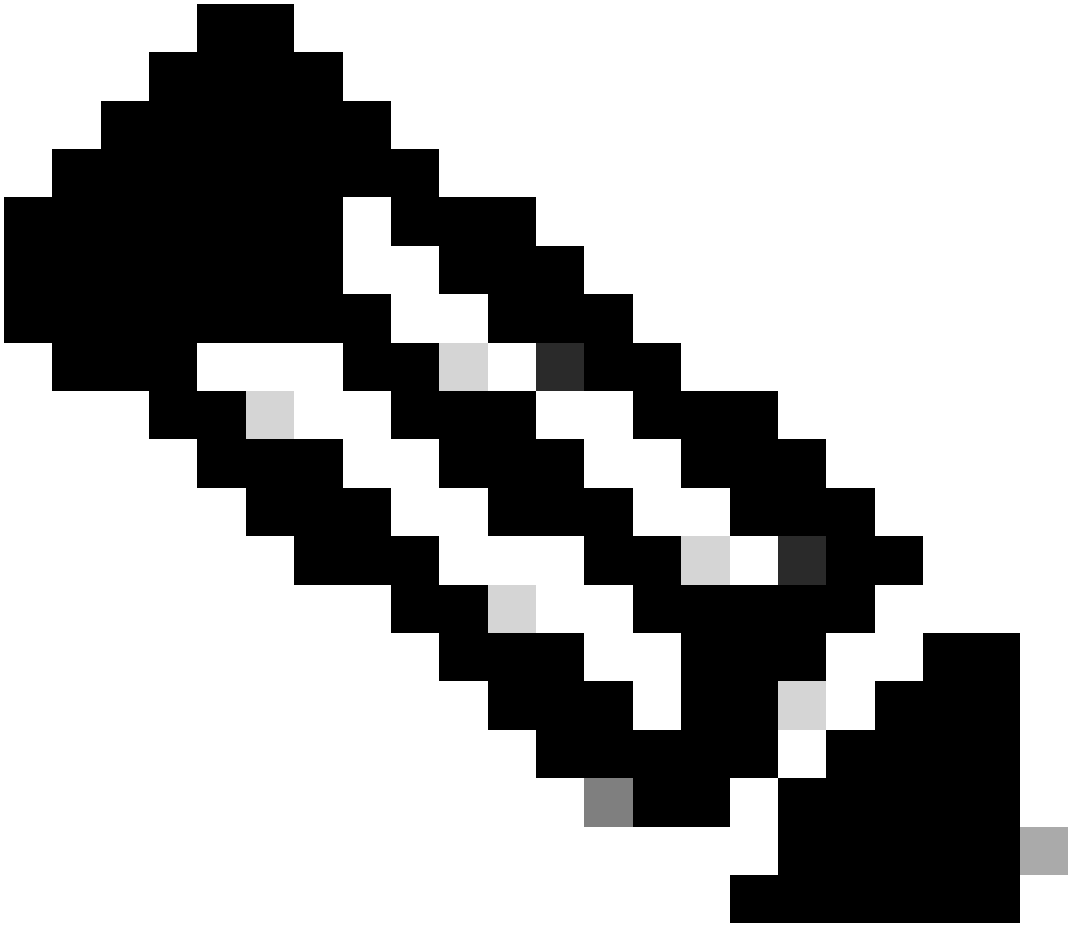
Probleem 19. Fout bij Dap.xml-kopie op ASDM

Het kopiëren van dap.xml naar ASA via het venster Bestandsbeheer in ASDM mislukt met de fout "disk0:/dap.xml is een speciaal systeembestand. Bestand uploaden onder de naam dap.xml in disk0: is niet toegestaan":



Probleemoplossing - Aanbevolen acties

Raadpleeg de software Cisco bug-id CSCvt62162 "Kan dap.xml niet kopiëren met behulp van File Management in ASDM 7.13.1". De tijdelijke oplossing is om het bestand rechtstreeks naar de ASA te kopiëren met behulp van protocollen als FTP of TFTP.



Opmerking: Dit defect is verholpen in recente ASDM-softwarereleases. Controleer de gebreken voor meer informatie.

Probleem 20. Op ASDM zichtbare IKE-beleidslijnen en IPSEC-voorstellen

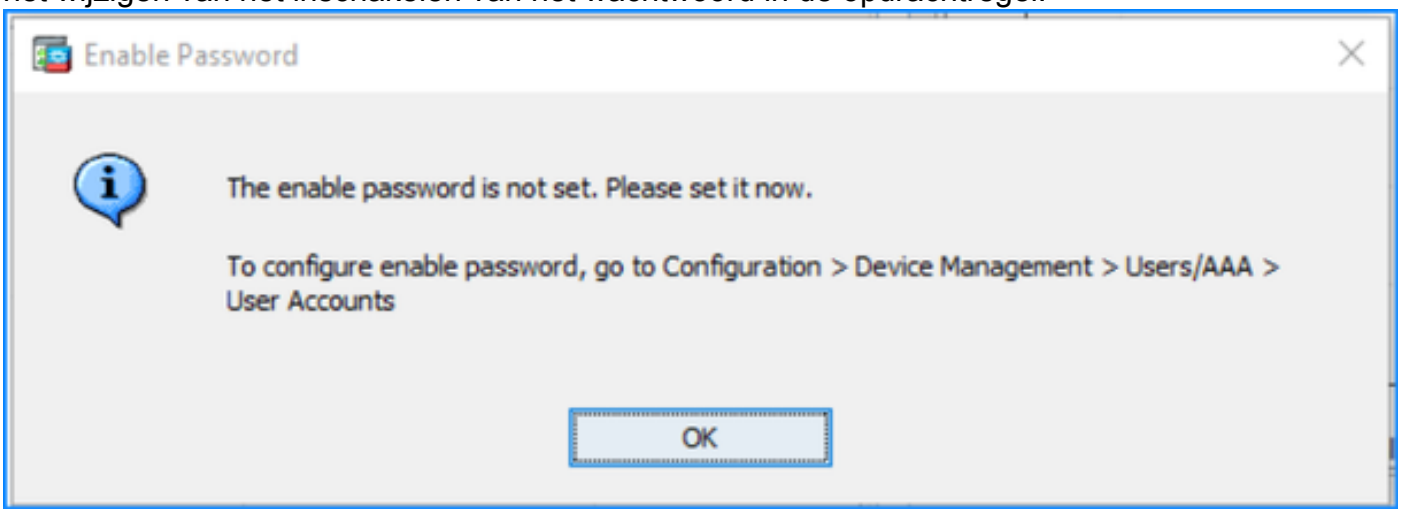
ASDM geeft geen IKE-beleid en IPSEC-voorstellen weer in het venster Configuraties > Site-to-Site VPN.

Probleemoplossing - Aanbevolen acties

Raadpleeg de software-id van Cisco-bug CSCwm42701 "ASDM-displayblanco in het tabblad IKE-beleid en IPSEC-voorstellen".

Probleem 21. ASDM toont het bericht "Het wachtwoord voor inschakelen is niet ingesteld. Stel het nu in."

ASDM toont het bericht "Het wachtwoord voor het inschakelen is niet ingesteld. Stel het nu in." na het wijzigen van het inschakelen van het wachtwoord in de opdrachtregel:



Probleemoplossing - Aanbevolen acties

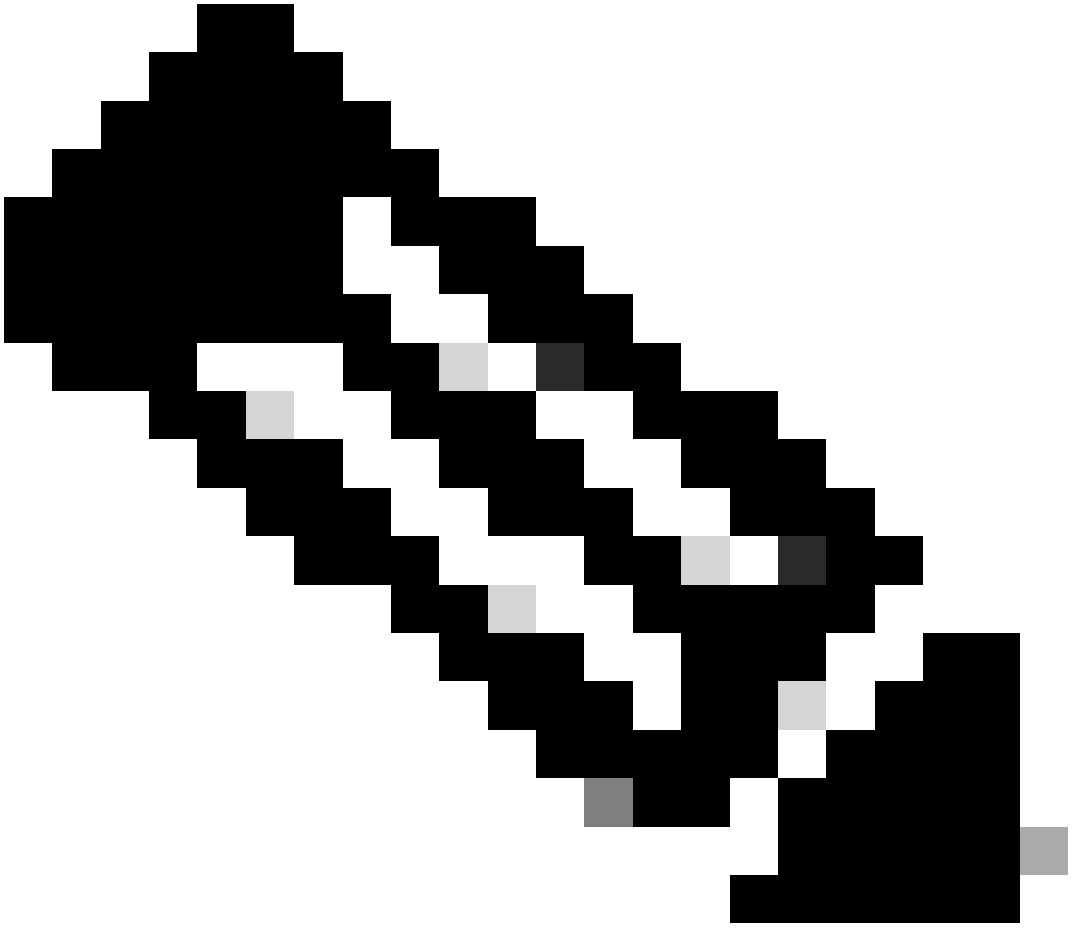
Raadpleeg de software-id van Cisco bug-id CSCvq42317 "ASDM vraagt om wachtwoord in te schakelen nadat het op CLI is ingesteld".

Probleem 22. ASDN-object verdwijnt na het vernieuwen van de ASDM UI

Wanneer een objectgroep en een objecthost aan een bestaande objectgroep worden toegevoegd en na het verfrissen van de ASDM verdwijnt de objectgroep uit de ASDM-lijst. De objectnamen moeten beginnen met getallen voor dit defect.

Probleemoplossing - Aanbevolen acties

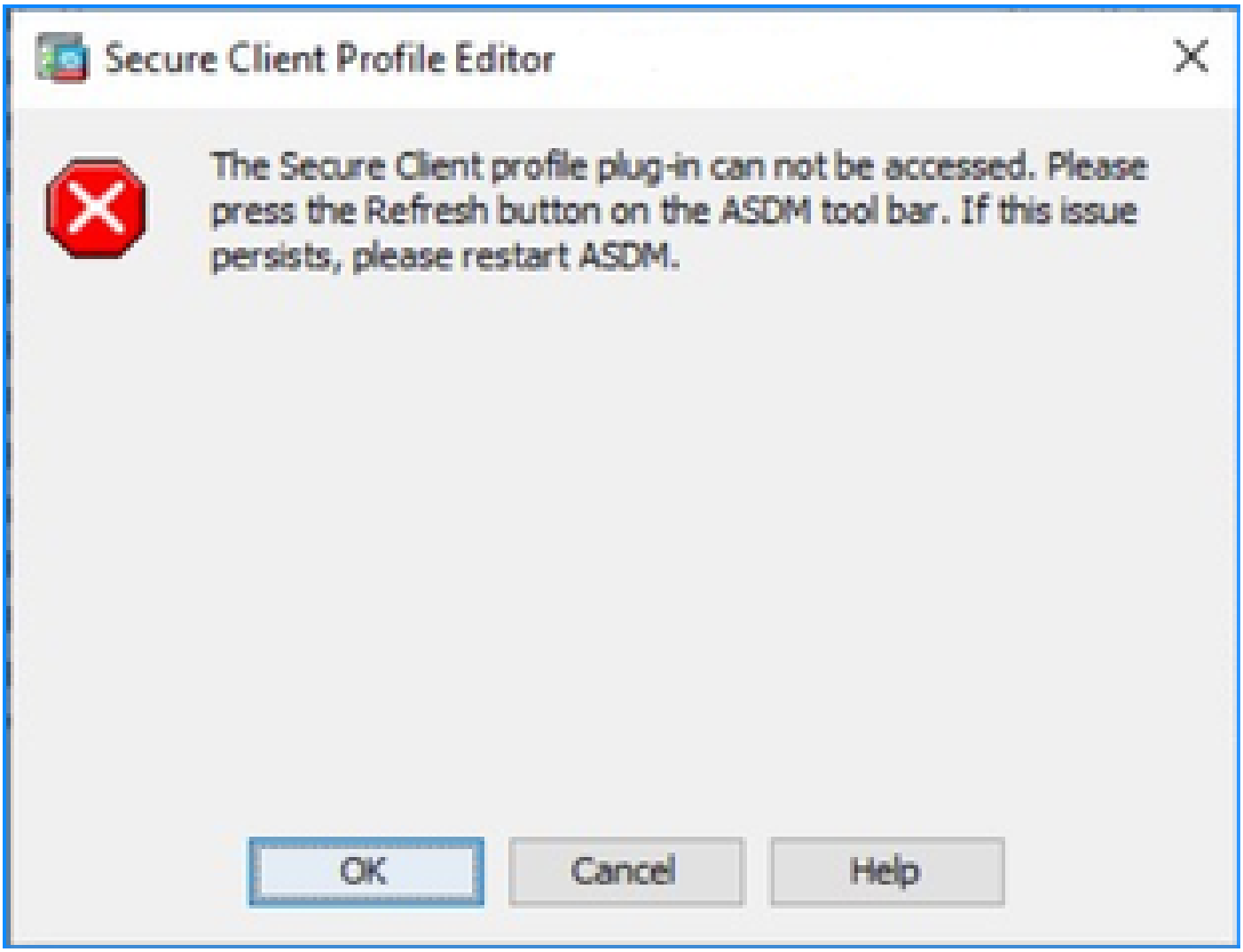
Raadpleeg de software Cisco bug ID CSCwf71723 "ASDM verliest geconfigureerde objecten/objectgroepen".



Opmerking: Dit defect is verholpen in recente ASDM-softwarereleases. Controleer de gebreken voor meer informatie.

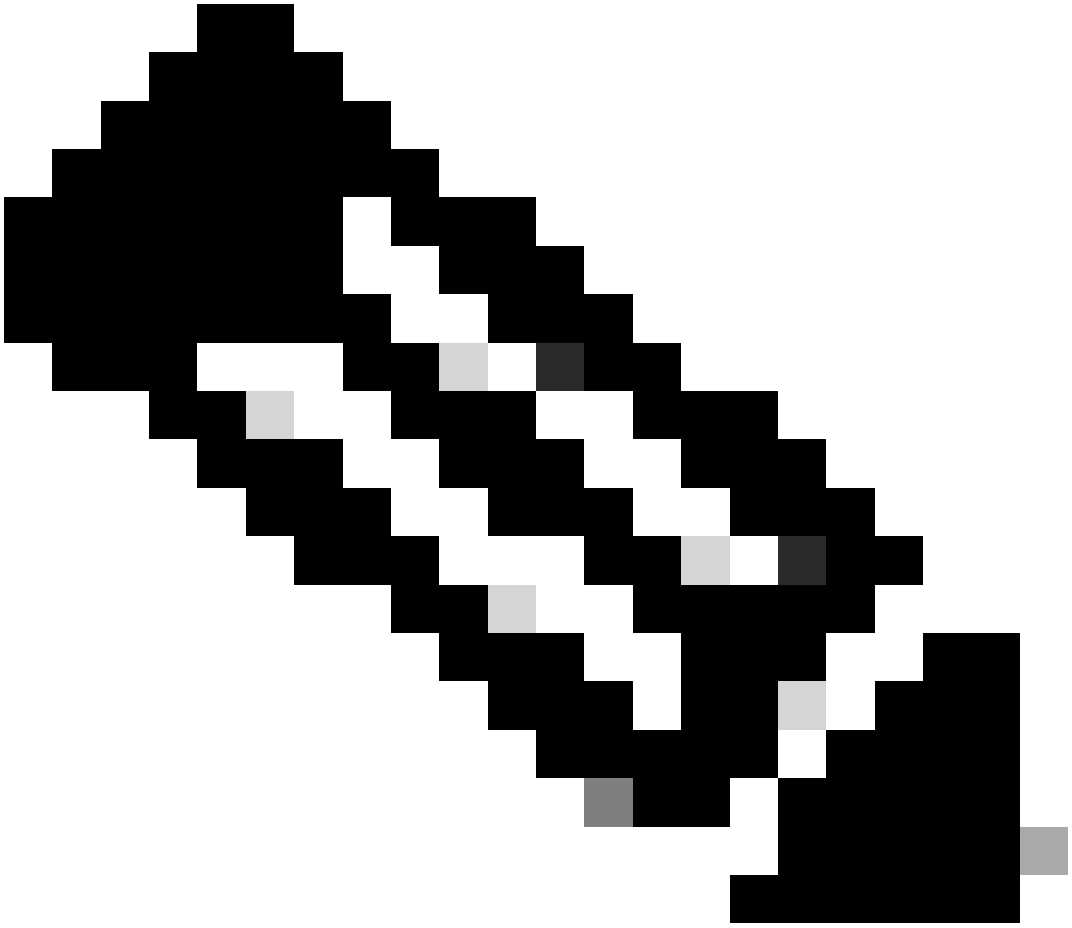
Probleem 23. Kan clientprofielen voor AnyConnect niet bewerken voor versies eerder dan 4.5

De clientprofielen voor AnyConnect kunnen niet eerder worden bewerkt voor AnyConnect Profile dan versie 4.5. De foutmelding "De plug-in voor het beveiligde clientprofiel kan niet worden geopend. Druk op de knop Vernieuwen op de ASDM-werkbalk. Start ASDM opnieuw op als dit probleem blijft optreden.":



Probleemoplossing - Aanbevolen acties

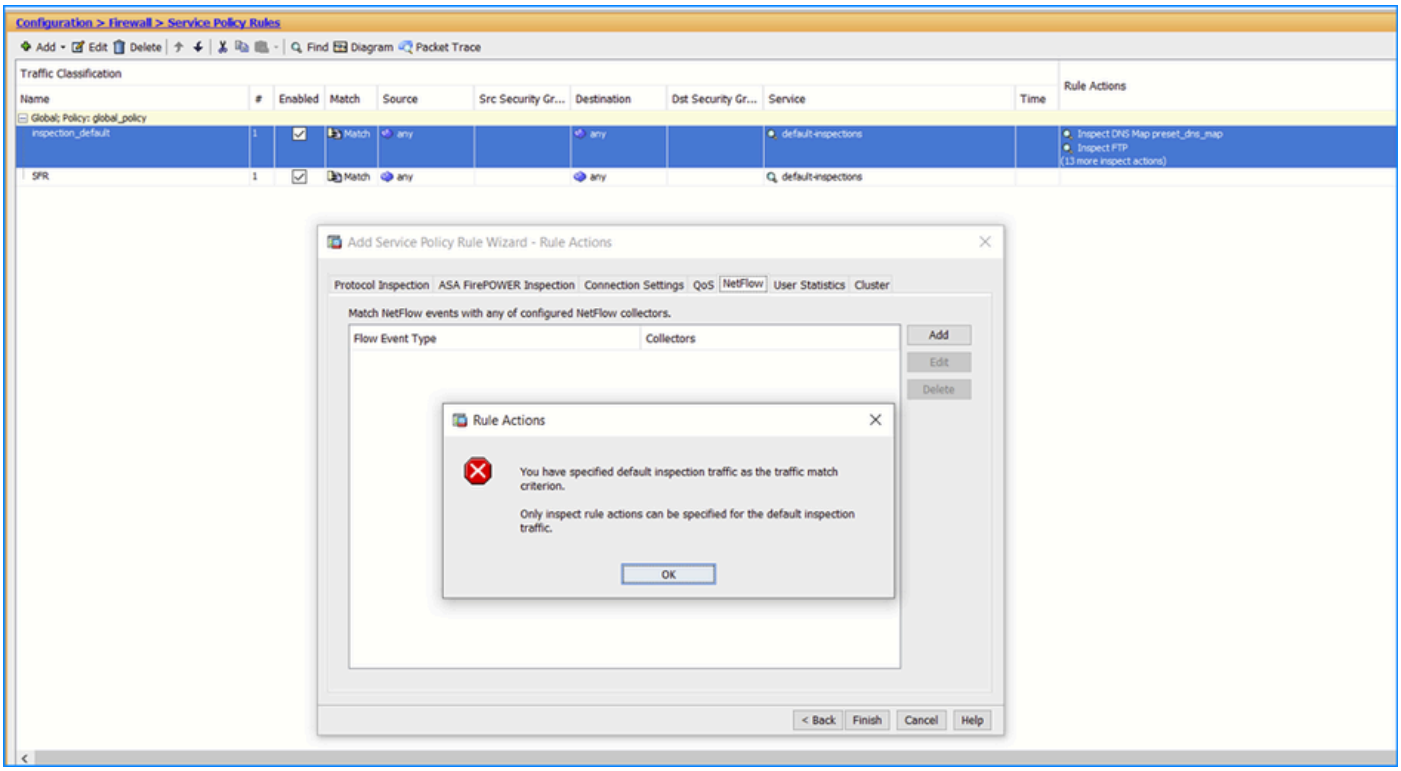
Raadpleeg de software-id van Cisco bug CSCwf16947 "ASDM - Kan de AnyConnect Profile Editor niet laden".



Opmerking: Dit defect is verholpen in recente ASDM-softwarereleases. Controleer de gebreken voor meer informatie.

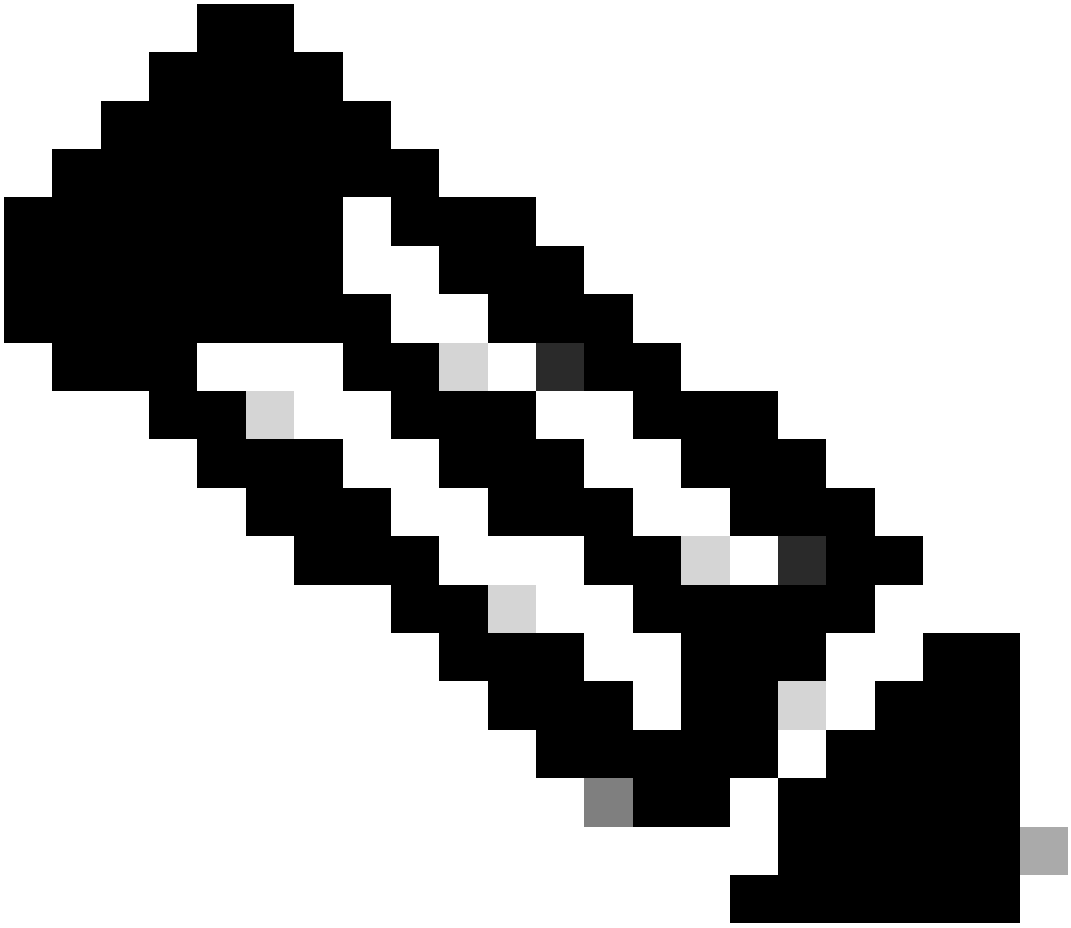
Probleem 24. Kan niet naar het tabblad Servicebeleid bewerken > Handelingen regels > ASA FirePOWER Inspection navigeren

In ASDM-versie 7.8.2 kunnen gebruikers niet navigeren naar het tabblad Servicebeleid bewerken > Handelingen regels > ASA FirePOWER Inspection en wordt de fout weergegeven: "U hebt standaard inspectieverkeer opgegeven als het traffic matchcriterium. U kunt alleen regelacties voor inspectie opgeven voor standaardinspectieverkeer." Dit gebeurt zelfs als een ACL is geselecteerd voor omleiding:



Probleemoplossing - Aanbevolen acties

Raadpleeg de software Cisco bug-id CSCvg15782 "ASDM - Kan wijziging van SFR-verkeer niet bekijken na upgrade naar versie 7.8(2)". De tijdelijke oplossing is om de CLI te gebruiken om de policy-map configuratie te bewerken.



Opmerking: Dit defect is verholpen in recente ASDM-softwarereleases. Controleer de gebreken voor meer informatie.

Probleem 25. AnyConnect Image versie 5.1 en AnyConnect-profieleditor op ASDM

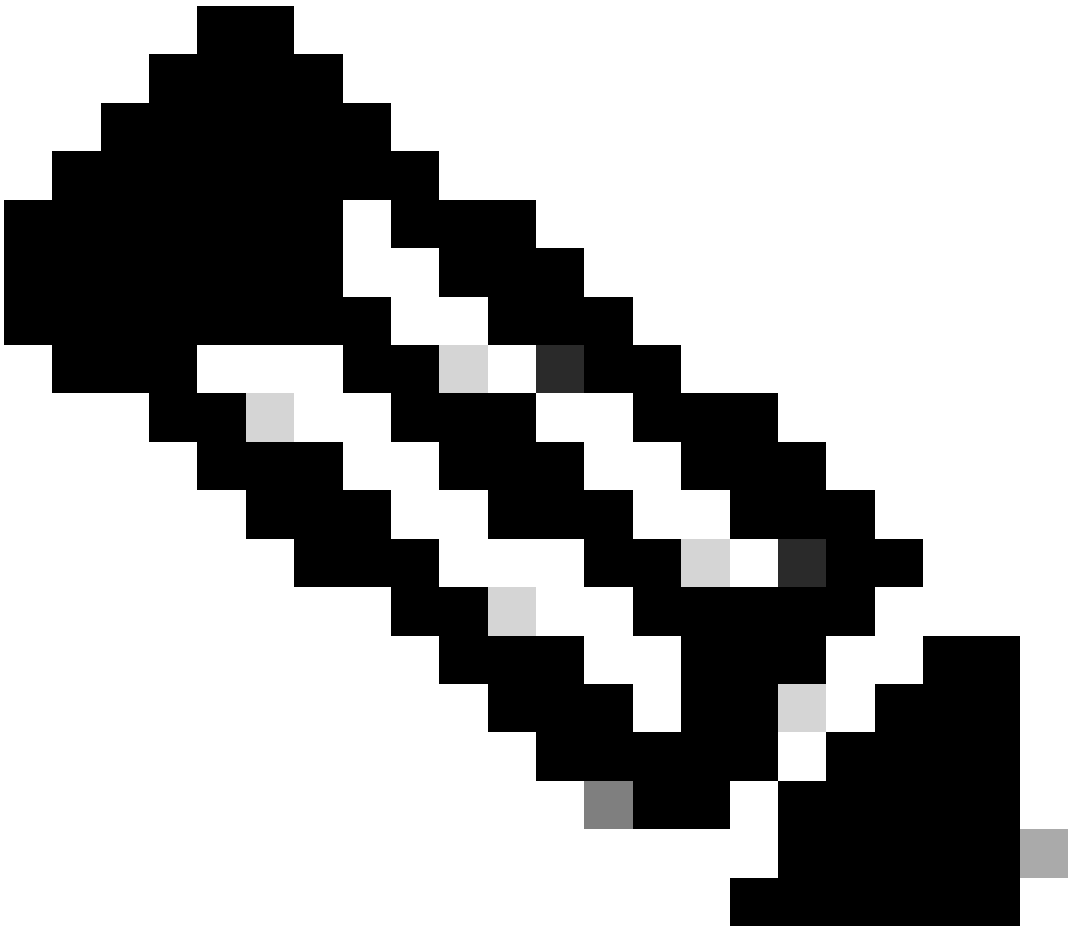
Deze symptomen worden geobserveerd voor Secure Client-softwareversie 5.1:

1. De namen van de groepsbeleidsmodule worden niet vermeld bij het laden van de Win/Mac/Linux-pakketten
2. ASDM kan AnyConnect Profile Editor niet openen.

Probleemoplossing - Aanbevolen acties

Raadpleeg de software met Cisco bug-id CSCwh7417 "ASDM: Profieleditor en groepsbeleid voor AnyConnect kunnen niet worden geladen wanneer u CSC Image 5.1" gebruikt. De tijdelijke

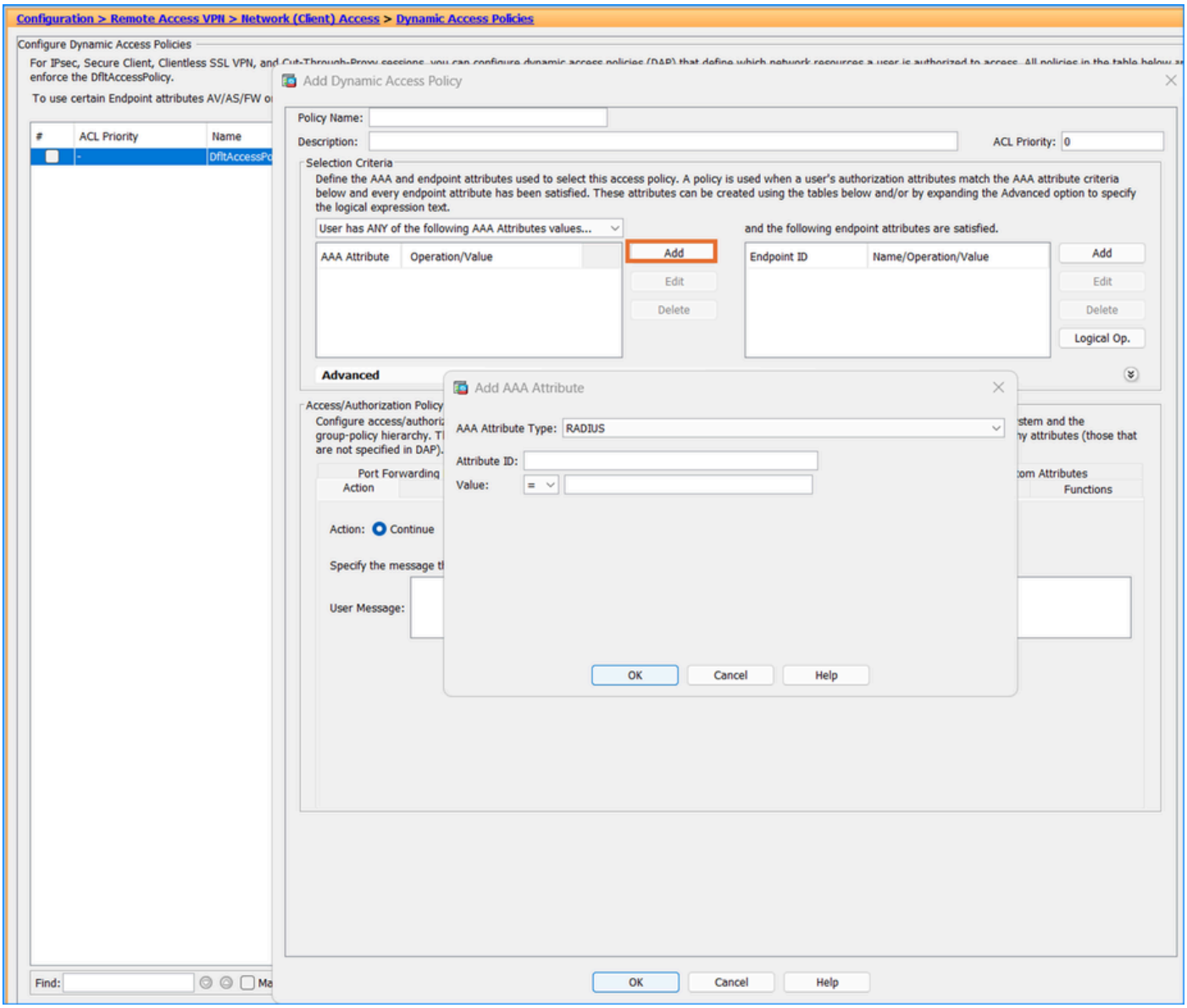
oplossing is om lagere versies van de beveiligde client te gebruiken.



Opmerking: Dit defect is verholpen in recente ASDM-softwarereleases. Controleer de gebreken voor meer informatie.

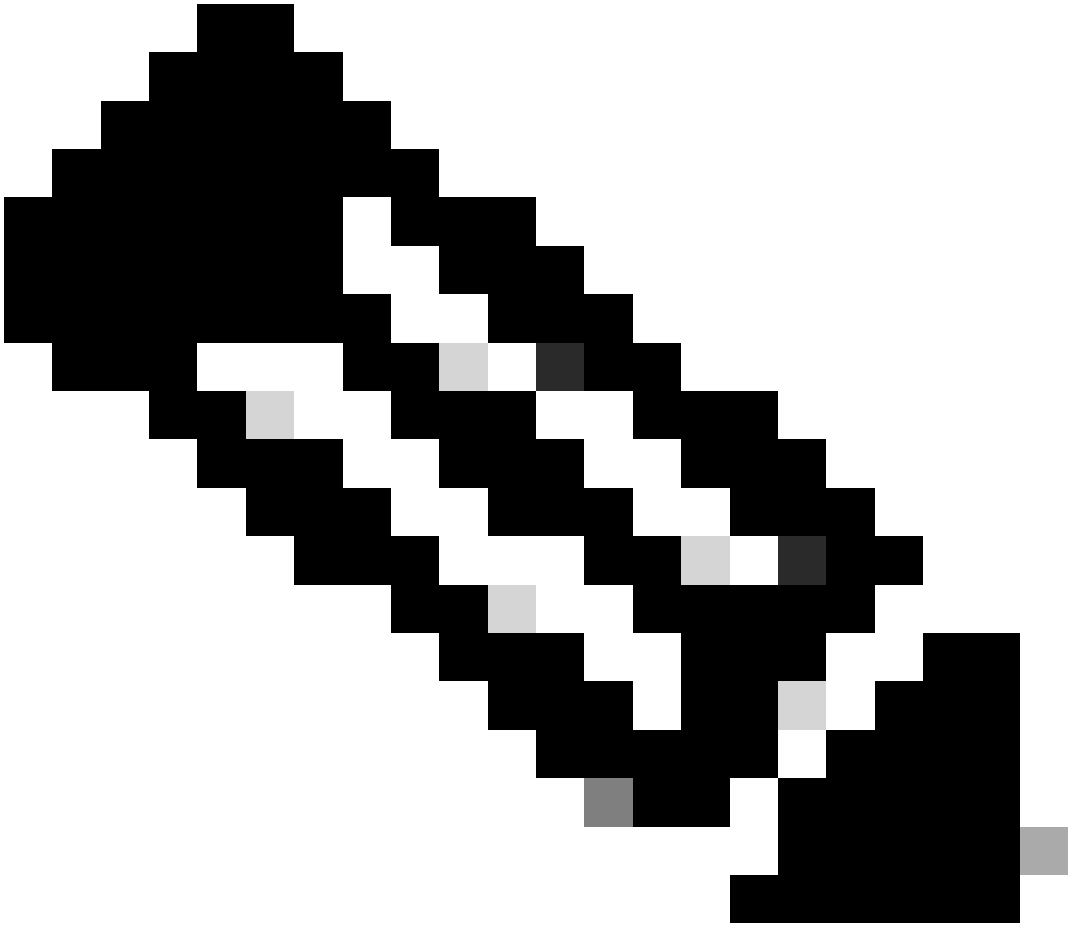
Probleem 26. Het type AAA-kenmerken (Radius/LDAP) is niet zichtbaar in ASDM

Het type AAA-kenmerken (Radius/LDAP) is niet zichtbaar in ASDM > Configuration > Remote Access VPN >Network (Client) Access > Dynamic Access Policies > Add > On AAA attribuut field > Add > Select Radius of LDAP:



Probleemoplossing - Aanbevolen acties

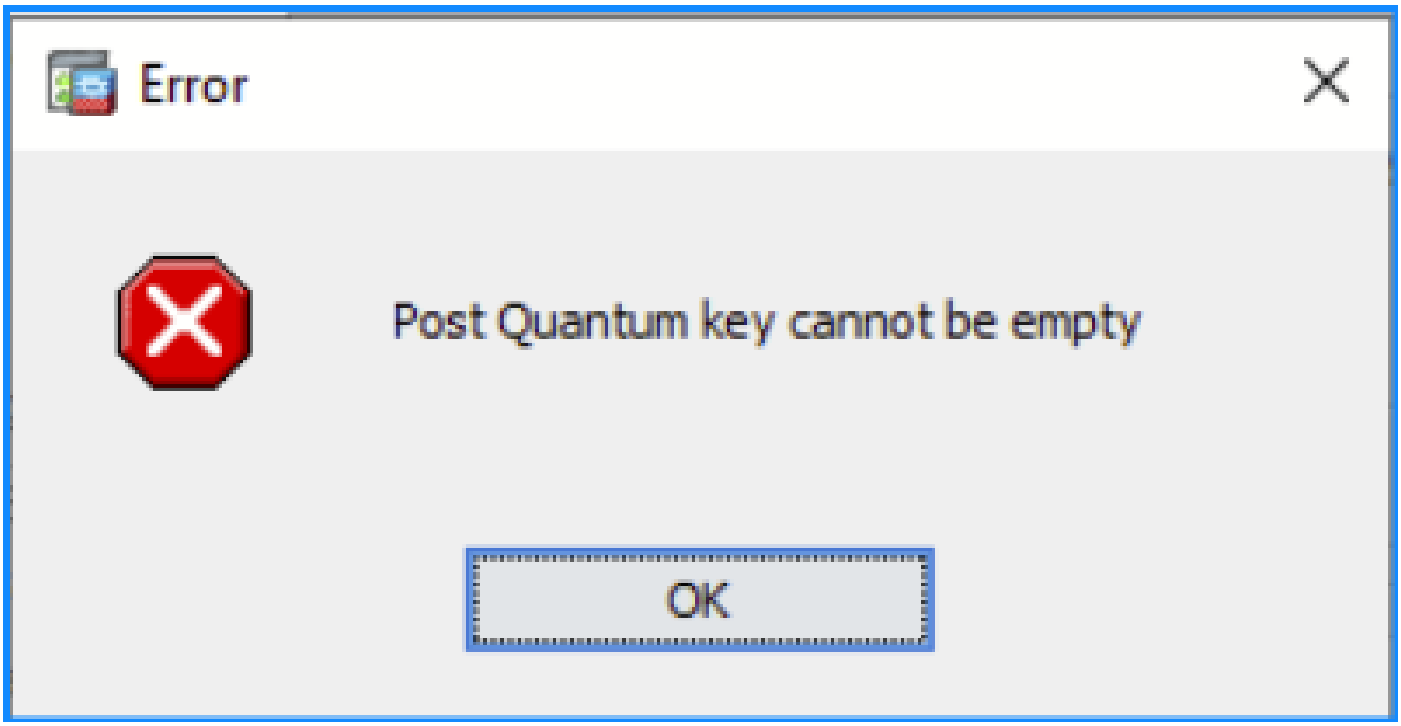
Raadpleeg de software-id van Cisco bug-id CSC9370 "ASDM: ASDM:DAP configuratie ontbrekende AAA Attributes type (Radius/LDAP)" en Cisco bug ID CSCwd16386 "ASDM:DAP configuratie ontbrekende AAA Attributes type (Radius/LDAP)".



Opmerking: Deze tekortkomingen zijn verholpen in recente ASDM-softwarereleases. Controleer de gebreken voor meer informatie.

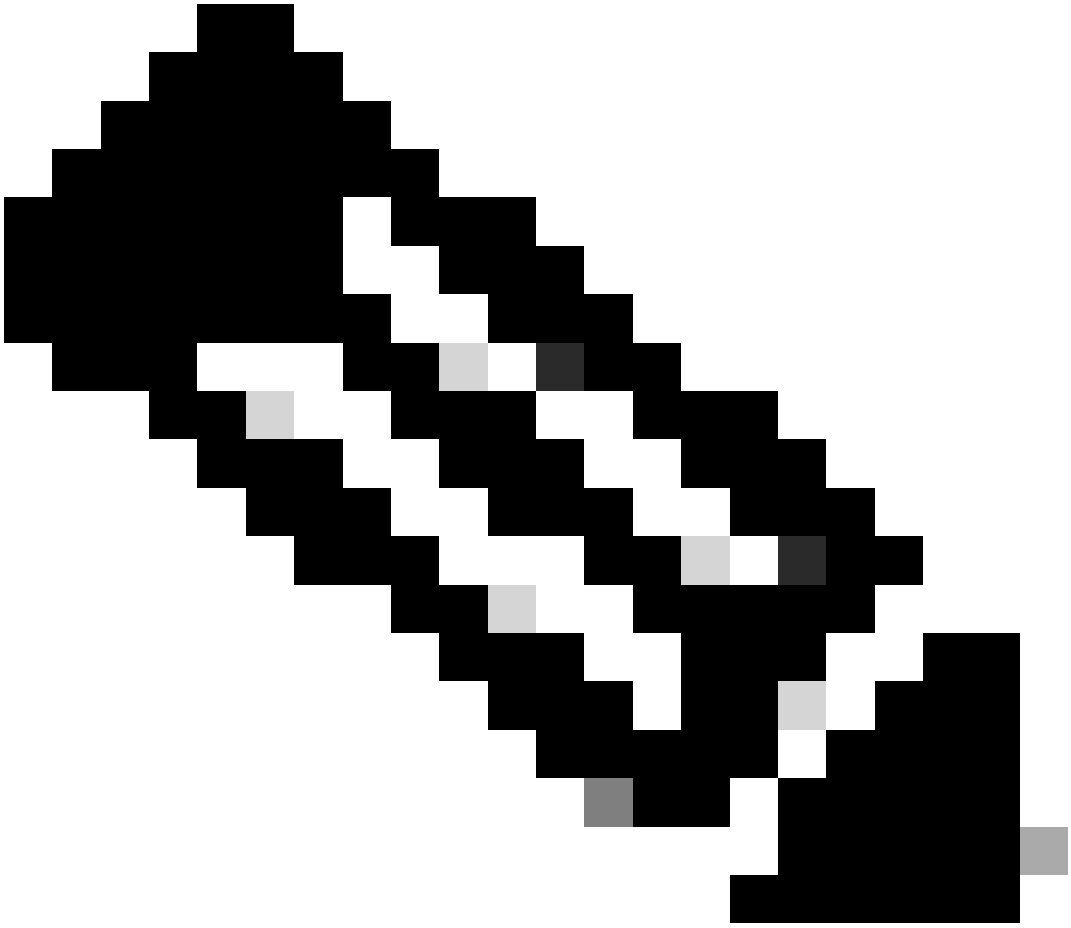
Probleem 27. De fout 'Post Quantum key can be leeg' wordt weergegeven op ASDM

De fout 'De Post Quantum-toets mag niet leeg zijn' wordt weergegeven bij het bewerken van de sectie Advanced in ASDM > Configuration > Remote Access VPN > Network (Client) Access > IPsec (IKEv2) verbindingsprofielen:



Probleemoplossing - Aanbevolen acties

Raadpleeg de software Cisco bug ID CSCwe58266 "ASDM IKEev2 configuratie - Post Quantum Key kan geen lege foutmelding zijn".



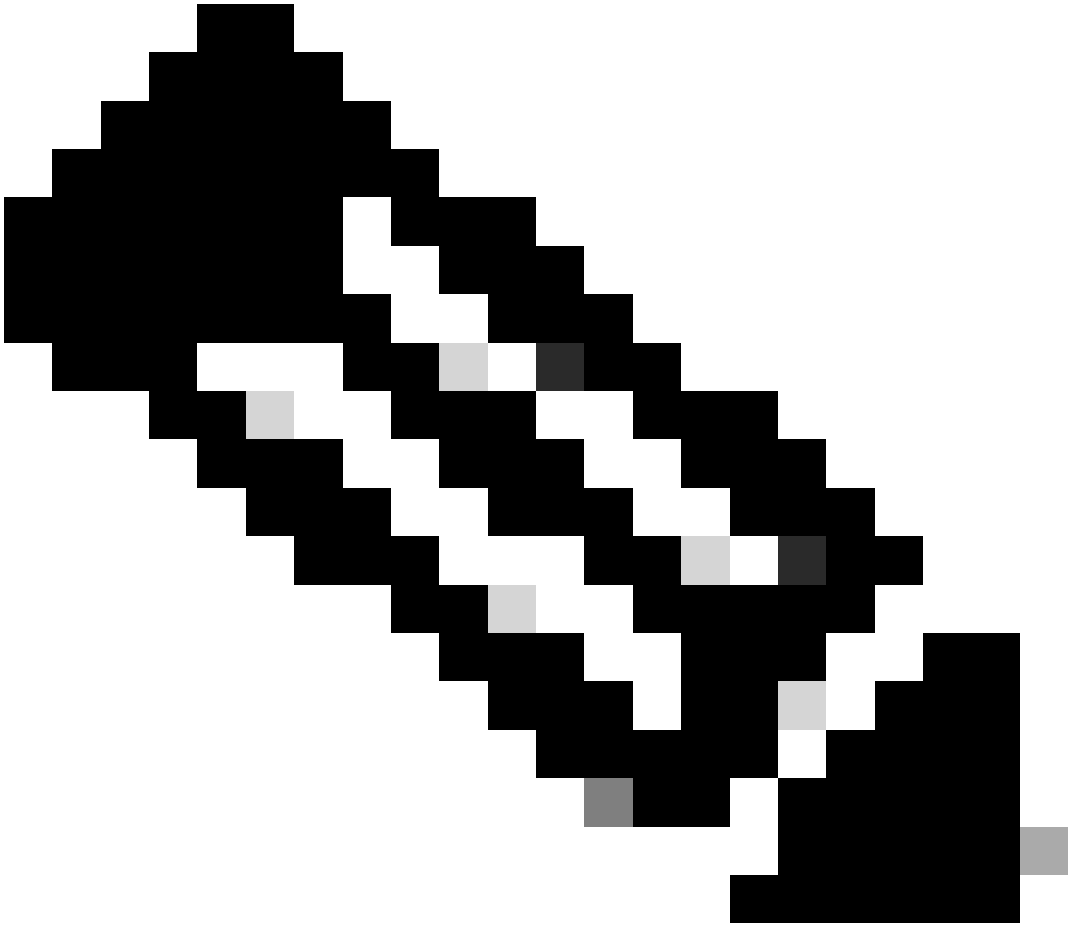
Opmerking: Dit defect is verholpen in recente ASDM-softwarereleases. Controleer de gebreken voor meer informatie.

Probleem 28. ASDM geeft geen resultaten weer bij gebruik van de optie "Waar gebruikt"

ASDM geeft geen resultaten weer bij gebruik van de optie "Waar gebruikt", door te navigeren naar Configuration > Firewall > Objecten > Netwerkobjecten/Groepen en met de rechtermuisknop te klikken op een object.

Probleemoplossing - Aanbevolen acties

Raadpleeg de optie Cisco bug-ID CSCwd98702 "Waar gebruikt" in ASDM werkt niet."



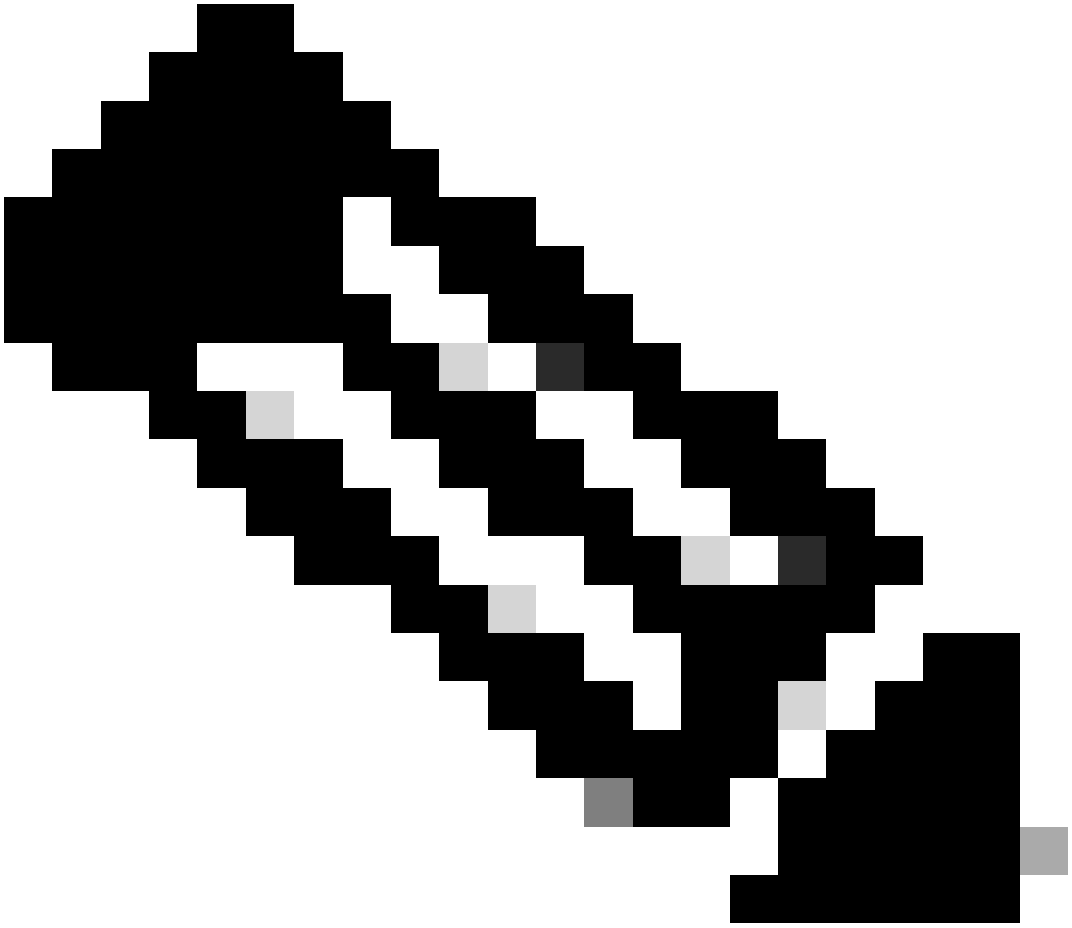
Opmerking: Dit defect is verholpen in recente ASDM-softwarereleases. Controleer de gebreken voor meer informatie.

Probleem 29. Waarschuwingsbericht "[Network Object] kan niet worden verwijderd omdat het in het volgende" wordt gebruikt bij het verwijderen van een netwerkobject

ASDM geeft het waarschuwingsbericht "[Network Object] kan niet worden verwijderd omdat het in het volgende" wordt gebruikt bij het verwijderen van een netwerkobject waarnaar wordt verwezen in een netwerkgroep in Configuration > Firewall > Objects > Network Objects/Groups.

Probleemoplossing - Aanbevolen acties

Raadpleeg de software-id van Cisco bug-id CSCwe67056 "[Network Object] kan niet worden verwijderd omdat het wordt gebruikt bij de volgende" waarschuwing die niet verschijnt".



Opmerking: Dit defect is verholpen in recente ASDM-softwarereleases. Controleer de gebreken voor meer informatie.

Probleem 30. Bruikbaarheidsproblemen met het tabblad Network Objects/Group in ASDM

Een of meer van deze symptomen worden waargenomen:

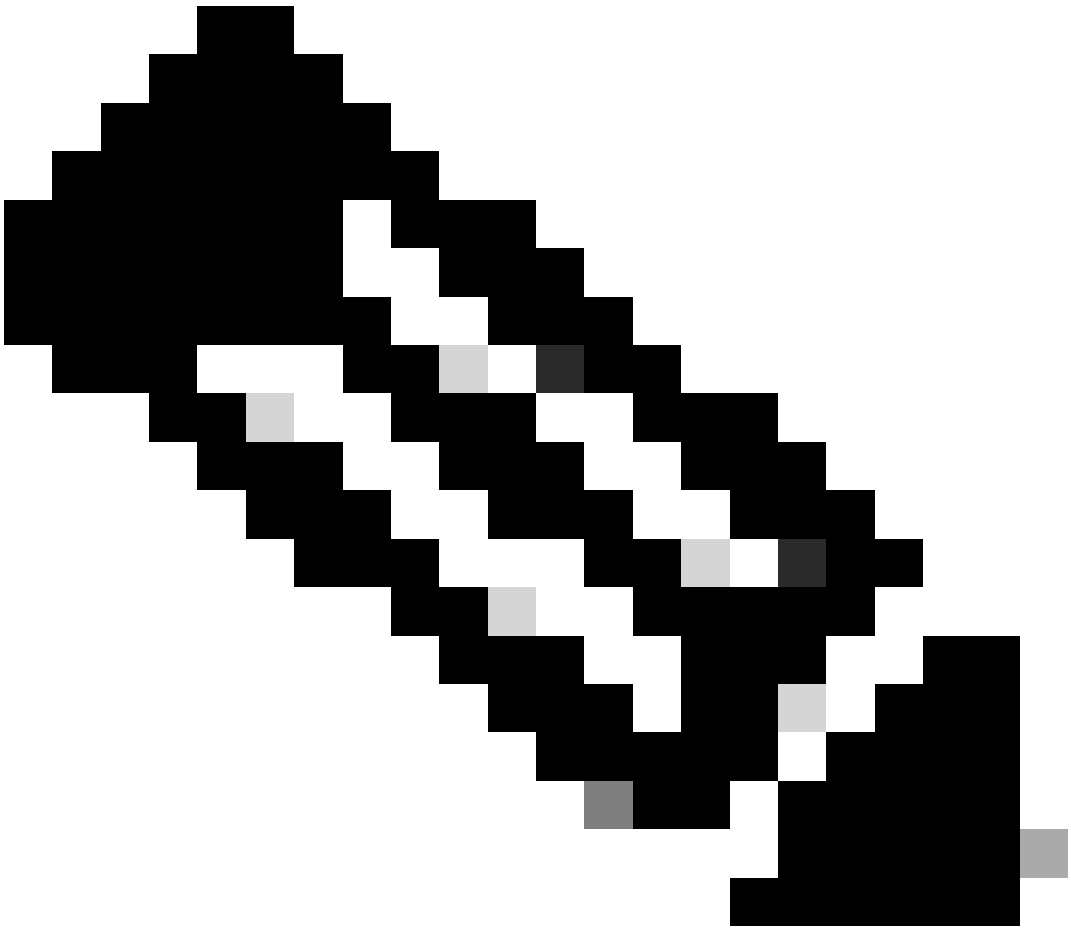
- De tekstinvoer "Naam" in de sectie "Nieuw objectlid maken" van de "Add/Edit Objectgroep Windows" wordt gemarkeerd als "optioneel". De knop "Toevoegen>" om het object te maken en toe te voegen is echter uitgeschakeld, tenzij er een naam wordt ingevoerd.
- Het tabblad "Gebruik" wordt geopend wanneer een gebruiker op de "Waar gebruikt..." klikt In het contextmenu worden alleen entiteiten (ACL's, routekaarten, objectgroepen) vermeld die rechtstreeks naar het object verwijzen. Het moet ook recursief tweede, derde, enzovoorts opsommen. Orderreferenties (dat is een ACL die een objectgroep gebruikt die een object bevat, moet ook worden vermeld als "gebruik" van het object).

- De functie "Verwijderen" in het contextmenu geeft dit gedrag ook weer. Het verwijdert automatisch elke entiteit die direct verwijst naar het object (als de entiteit leeg zou worden wanneer het object wordt verwijderd). Het werkt niet op deze manier als een tweede, derde, enzovoorts. De verwijzing van de orde zou leeg worden wegens het schrappen van het voorwerp en de eerste ordeverwijzing.

De gebruiker kan ervan worden overtuigd dat ASDM entiteiten voorkomt die leeg zouden worden door het wissen van objecten uit de resterende instellingen. Dit is echter niet per se het geval.

Probleemoplossing - Aanbevolen acties

Raadpleeg de software-id van Cisco bug CSCwe86257 "Usability of Network Objects/Group Tab in ASDM".

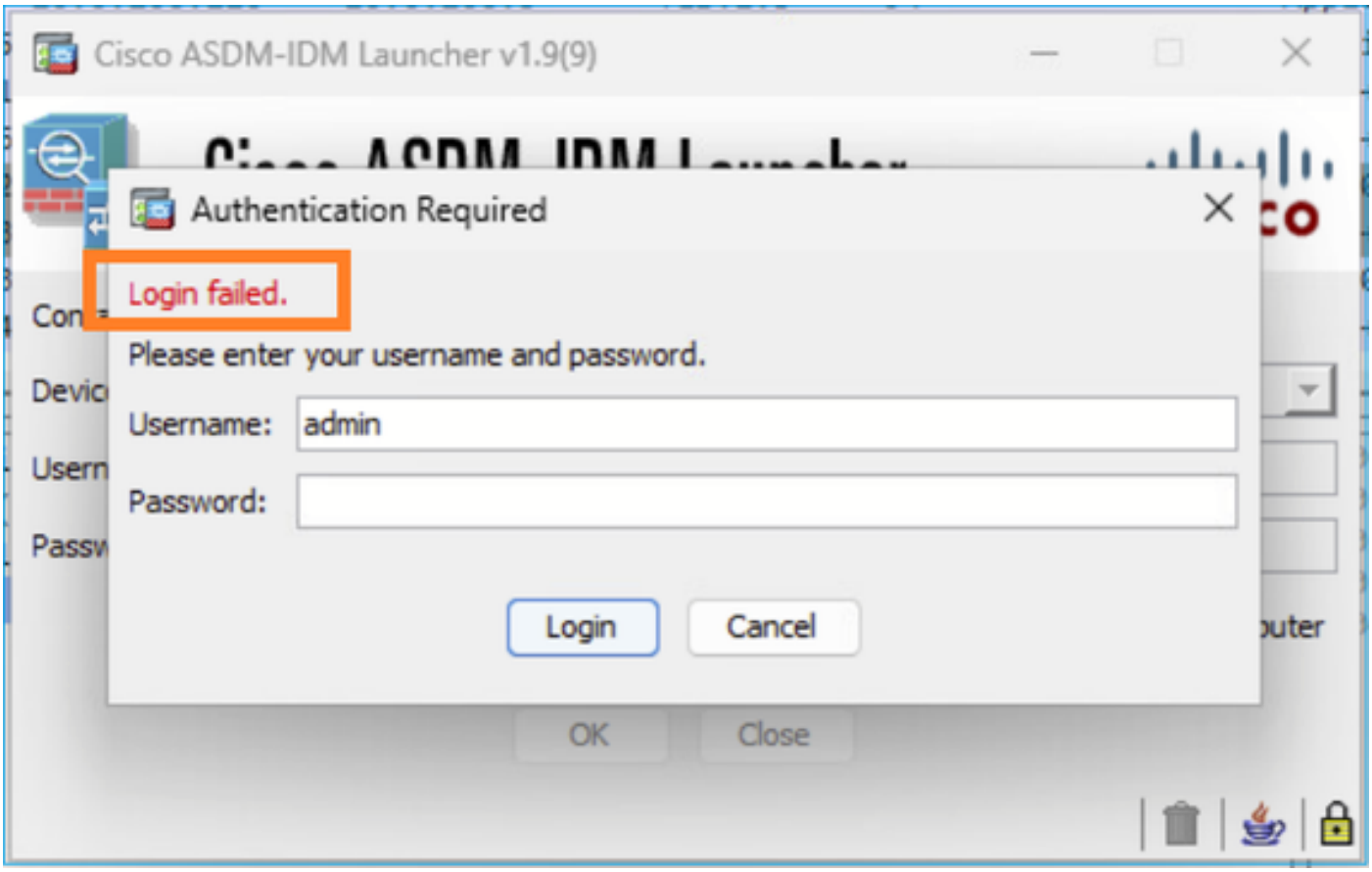


Opmerking: Dit defect is verholpen in recente ASDM-softwarereleases. Controleer de gebreken voor meer informatie.

Problemen met ASDM-verificatie oplossen

Probleem 1. Aanmelden bij ASDM mislukt

De fout die wordt weergegeven op de ASDM UI is:



Probleemoplossing - Aanbevolen acties

Deze fout kan worden waargenomen wanneer zowel HTTP als WebVPN Cisco Secure Client (AnyConnect) op dezelfde interface is ingeschakeld. Aan alle voorwaarden moet dus worden voldaan:

1. AnyConnect/Cisco Secure-client is ingeschakeld op een interface
2. HTTP-server is ingeschakeld op dezelfde interface en dezelfde poort als AnyConnect/Cisco Secure-client

Voorbeeld:

<#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
```

Tip voor probleemoplossing: Schakel 'debug http 255' in en u ziet het conflict tussen ASDM en 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
```

Als zijaantekening, ondanks de inlogfout, tonen de ASA-syslogs aan dat de verificatie succesvol is:

```
<#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

Voorwendselen

Omgeving 1

Verander de TCP-poort voor de ASA HTTP-server, bijvoorbeeld:

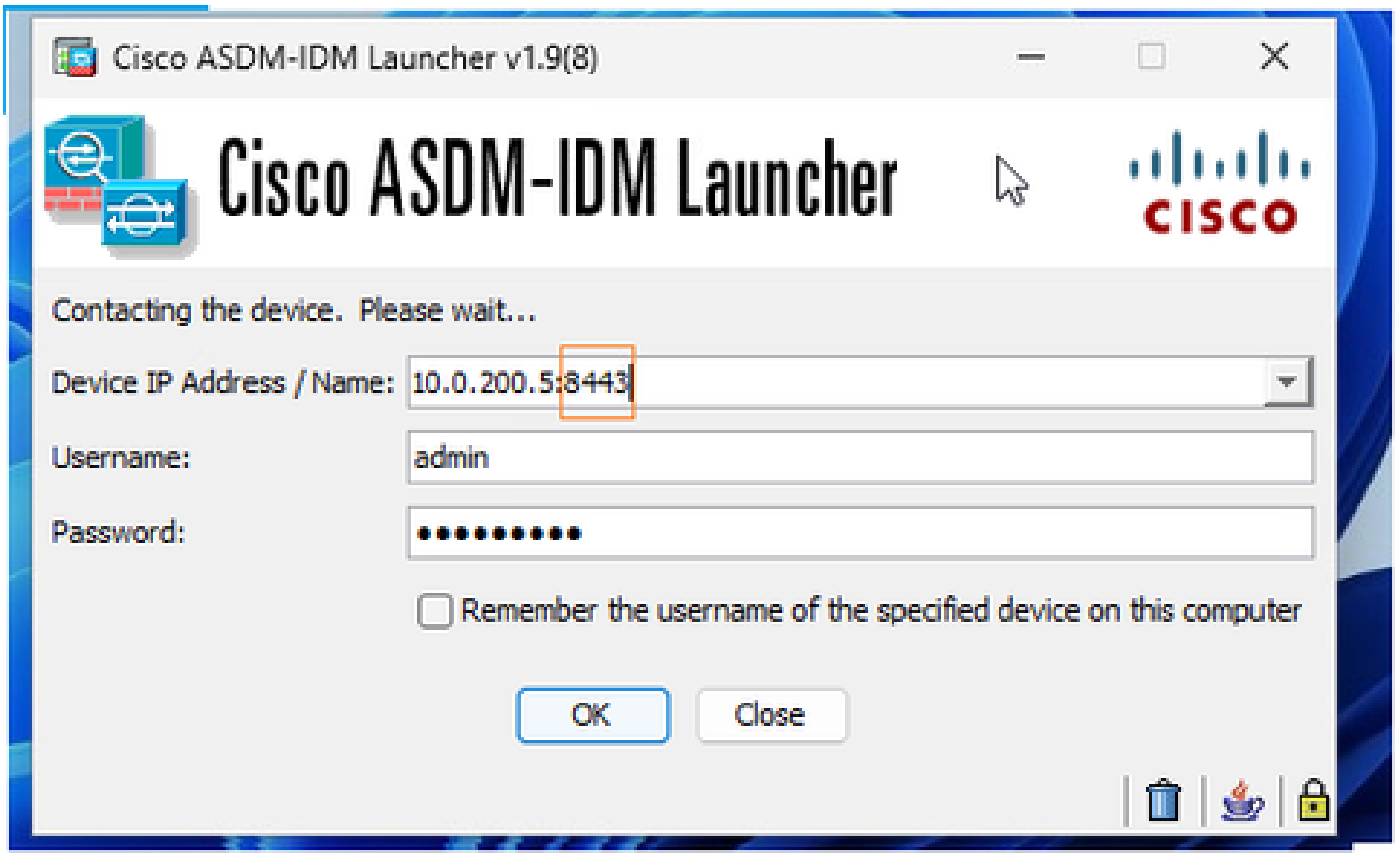
<#root>

```
ciscoasa#
```

configure terminal

```
ciscoasa(config)#
```

http server enable 8443



Oplossing 2

Verander de TCP-poort voor de AnyConnect/Cisco Secure-client, bijvoorbeeld:

<#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
```

Workaround 3

Een andere tijdelijke oplossing is om de configuratie van de "aaa-verificatie http console" te

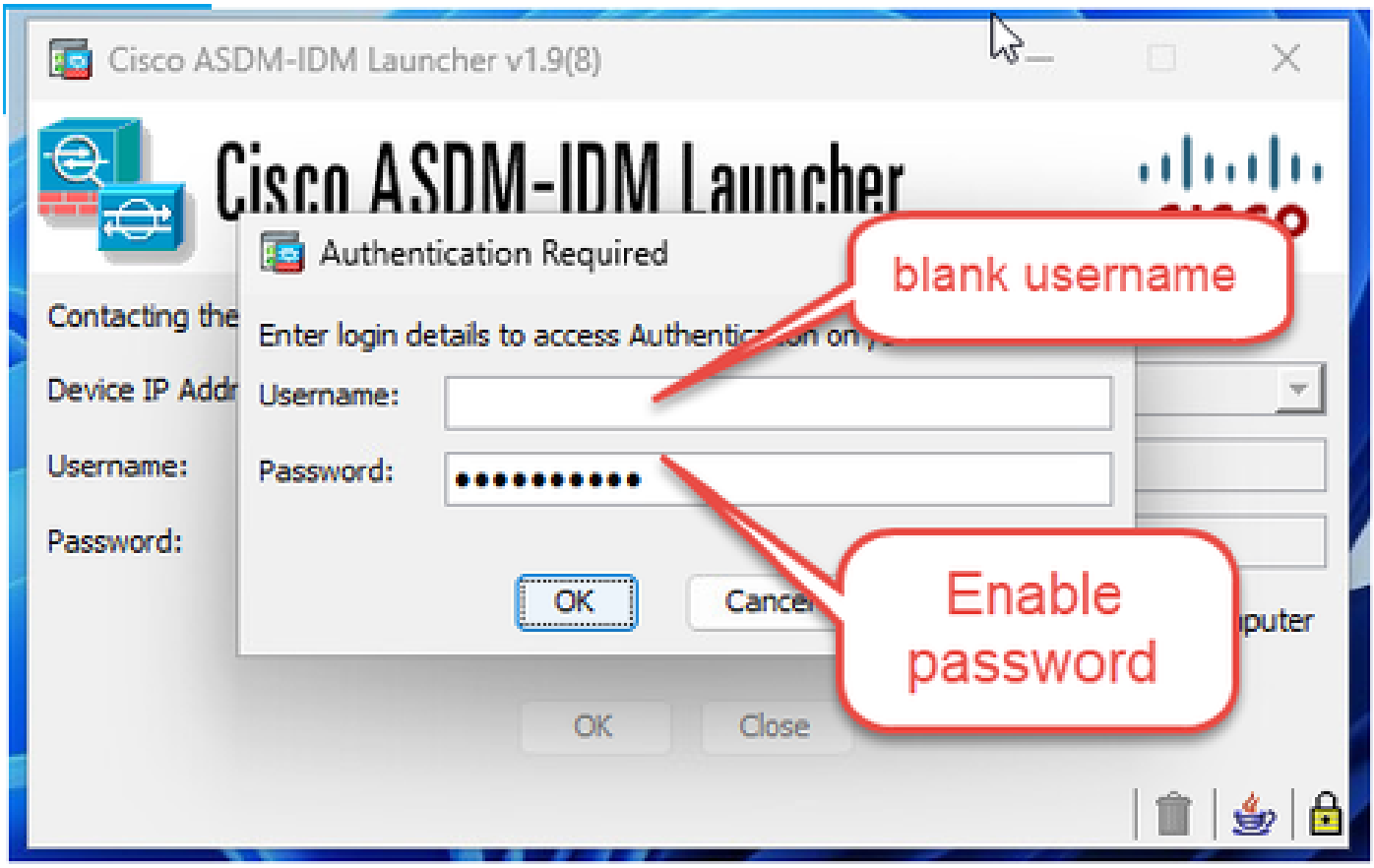
verwijderen:

<#root>

```
ciscoasa(config)#
```

```
no aaa authentication http console LOCAL
```

In dit geval kunt u zich aanmelden bij ASDM met de optie Wachtwoord inschakelen:



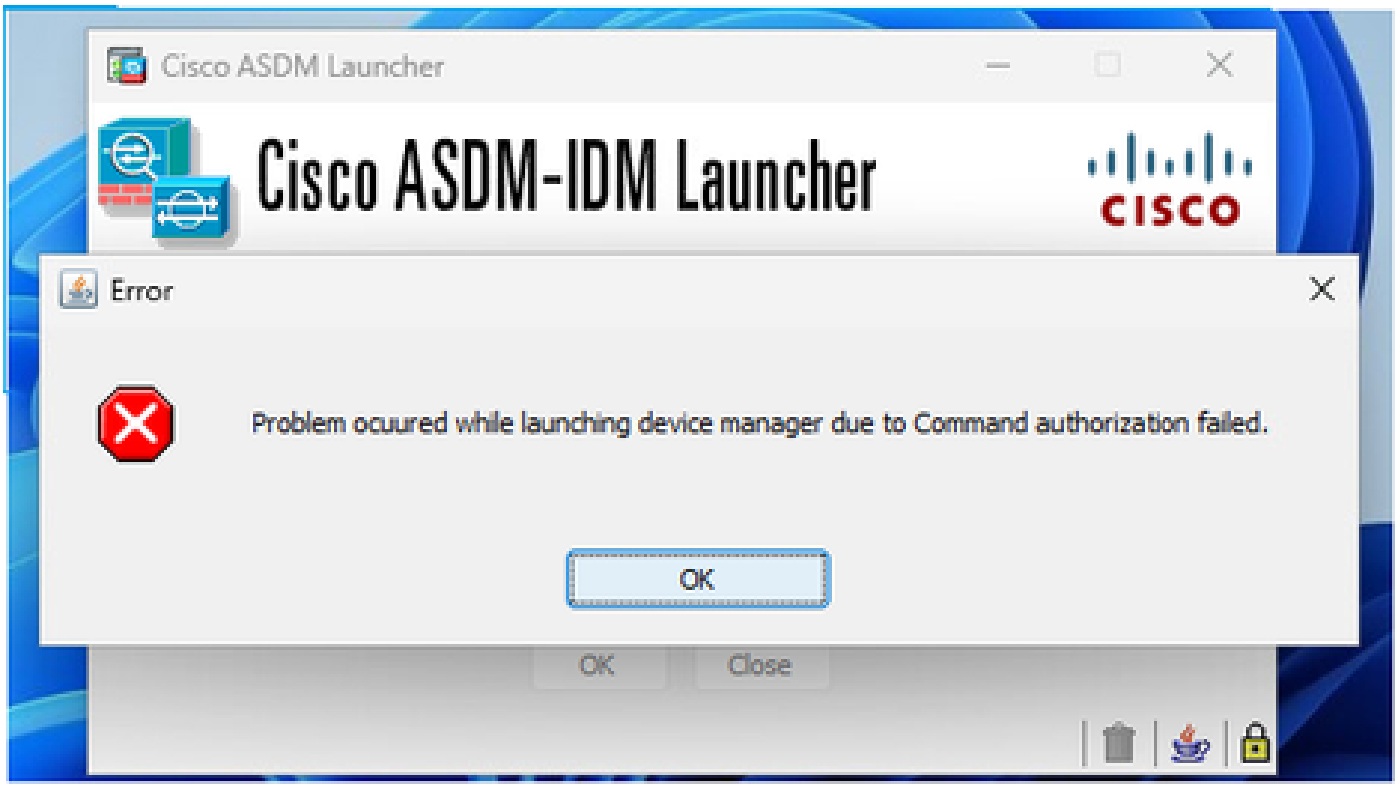
Verwante defecten

Cisco fout-id CSCwb67583

Waarschuwing toevoegen wanneer webVPN en ASDM op dezelfde interface zijn ingeschakeld

Probleem 2. Opdrachtautorisatie ASDM is mislukt

De fout die wordt weergegeven op de ASDM UI is:



Probleemoplossing - Aanbevolen stappen

Controleer uw AAA-configuratie op ASA en zorg ervoor dat:

- U hebt ook AAA-verificatie geconfigureerd.
- Als u een externe verificatieserver gebruikt, is deze bereikbaar en worden de opdrachten geautoriseerd.

Referentie

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

Probleem 3. Configureer ASDM alleen-lezen toegang

Soms wilt u alleen-lezen toegang bieden aan ASDM-gebruikers.

Probleemoplossing - Aanbevolen stappen

Maak een nieuwe gebruiker met een aangepast voorrecht niveau (5), bijvoorbeeld:

<#root>

```
asa(config)#
```

username [username] password [password] privilege 5

Met deze opdracht maakt u een gebruiker met een prioriteitsniveau van 5, het "alleen-controleren"-niveau. Vervang "[gebruikersnaam]" en "[wachtwoord]" door de gewenste gebruikersnaam en het gewenste wachtwoord.

Details

Met lokale opdrachtautorisatie kunt u opdrachten toewijzen aan een van de 16 prioriteitsniveaus (0 tot 15). Standaard wordt elke opdracht toegewezen aan prioriteitsniveau 0 of 15. U kunt bepalen dat elke gebruiker op een specifiek prioriteitsniveau moet staan, en elke gebruiker kan elke opdracht invoeren op het toegewezen prioriteitsniveau of minder. ASA ondersteunt gebruikersrechten die zijn gedefinieerd in de lokale database, een RADIUS-server of een LDAP-server (als u LDAP-kenmerken aan RADIUS-kenmerken toekent).

Procedure

Stap 1	Kies Configuratie > Apparaatbeheer > Gebruikers/AAA > AAA-toegang > Autorisatie.
Stap 2	Schakel het aankruisvakje Activeer autorisatie voor ASA opdrachttoegang > Inschakelen in.
Stap 3	Kies LOCAL in de vervolgkeuzelijst Servergroep.
Stap 4	Wanneer u lokale opdrachtautorisatie inschakelt, hebt u de mogelijkheid om handmatig voorrangsniveaus toe te wijzen aan afzonderlijke opdrachten of groepen opdrachten of om de vooraf gedefinieerde gebruikersaccountrechten in te schakelen. · Klik op ASDM Defined User Roles instellen om vooraf gedefinieerde gebruikersaccountrechten te gebruiken. Het dialoogvenster Instellen ASDM-gedefinieerde gebruikersrollen wordt weergegeven. Klik op Ja om de voorgedefinieerde gebruikersaccountrechten te gebruiken: Beheerder (voorrangsniveau 15) met volledige toegang tot alle CLI-opdrachten; Alleen lezen (voorrangsniveau 5 met alleen-lezen toegang); en alleen monitor (voorrangsniveau 3, met alleen toegang tot de sectie Monitoring). · Klik op Opdrachtrechten configureren om opdrachtniveaus handmatig te configureren. Het dialoogvenster Opdrachtrechten instellen verschijnt. U kunt alle opdrachten weergeven door Alle modi te kiezen uit de vervolgkeuzelijst Opdrachtmodus of u kunt een configuratiemodus kiezen om de opdrachten die in die modus beschikbaar zijn, te bekijken. Als u bijvoorbeeld context kiest, kunt u alle opdrachten in contextconfiguratiemodus weergeven. Als een opdracht kan worden ingevoerd in de gebruikers-EXEC- of geprivilegieerde EXEC-modus en in de configuratiemodus, en de opdracht verschillende acties uitvoert in elke modus, kunt u het voorrangsniveau voor

	deze modi afzonderlijk instellen. De Variant kolom displays tonen, duidelijk, of cmd. U kunt het voorrecht slechts voor de show plaatsen, ontruimen, of vorm van het bevel vormen. De configuratie vorm van het bevel is typisch de vorm die een configuratieverandering veroorzaakt, of als ongewijzigd bevel (zonder de show of duidelijke prefix) of als de nrvorm. Als u het niveau van een opdracht wilt wijzigen, dubbelklikt u op de opdracht of klikt u op Bewerken. U kunt het niveau tussen 0 en 15 instellen. U kunt alleen het voorrangsniveau van de hoofdopdracht configureren. U kunt bijvoorbeeld het niveau van alle aaa-opdrachten configureren, maar niet het niveau van de opdracht aaa-verificatie en de opdracht aaa-autorisatie afzonderlijk. Als u het niveau wilt wijzigen van alle opdrachten die worden weergegeven, klikt u op Alles selecteren en vervolgens op Bewerken. Klik op OK om de wijzigingen te aanvaarden.
Stap 5	Klik op Apply (Toepassen). De autorisatie-instellingen worden toegewezen en de wijzigingen worden opgeslagen in de actieve configuratie.

Referentie

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

Probleem 4. ASDM Multi-Factor Authenticatie (MFA)

Probleemoplossing - Aanbevolen stappen

Op het moment van schrijven ondersteunt ASDM MFA (of 2FA) niet. Deze beperking omvat MFA met oplossingen zoals PingID, etc.

Referentie

Cisco Bug-id CSCvs85995

NIEUW: ASDM-toegang met tweevoudige verificatie of MFA

Probleem 5. ASDM-configuratie voor externe verificatie

Probleemoplossing - Aanbevolen stappen

U kunt LDAP, RADIUS, RSA SecurityID of TACACS+ gebruiken om externe verificatie op ASDM te configureren.

Referenties

- 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

Probleem 6. ASDM LOKALE verificatie mislukt

Probleemoplossing - Aanbevolen stappen

Als u externe verificatie en LOKALE verificatie als een reserve gebruikt, werkt de lokale verificatie alleen als uw externe server niet werkt of niet werkt. Alleen in dit scenario neemt de LOKALE verificatie over en kunt u verbinding maken met de LOKALE gebruikers.

Dit komt doordat externe verificatie voorrang heeft op LOKALE verificatie.

Voorbeeld:

<#root>

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

Referentie

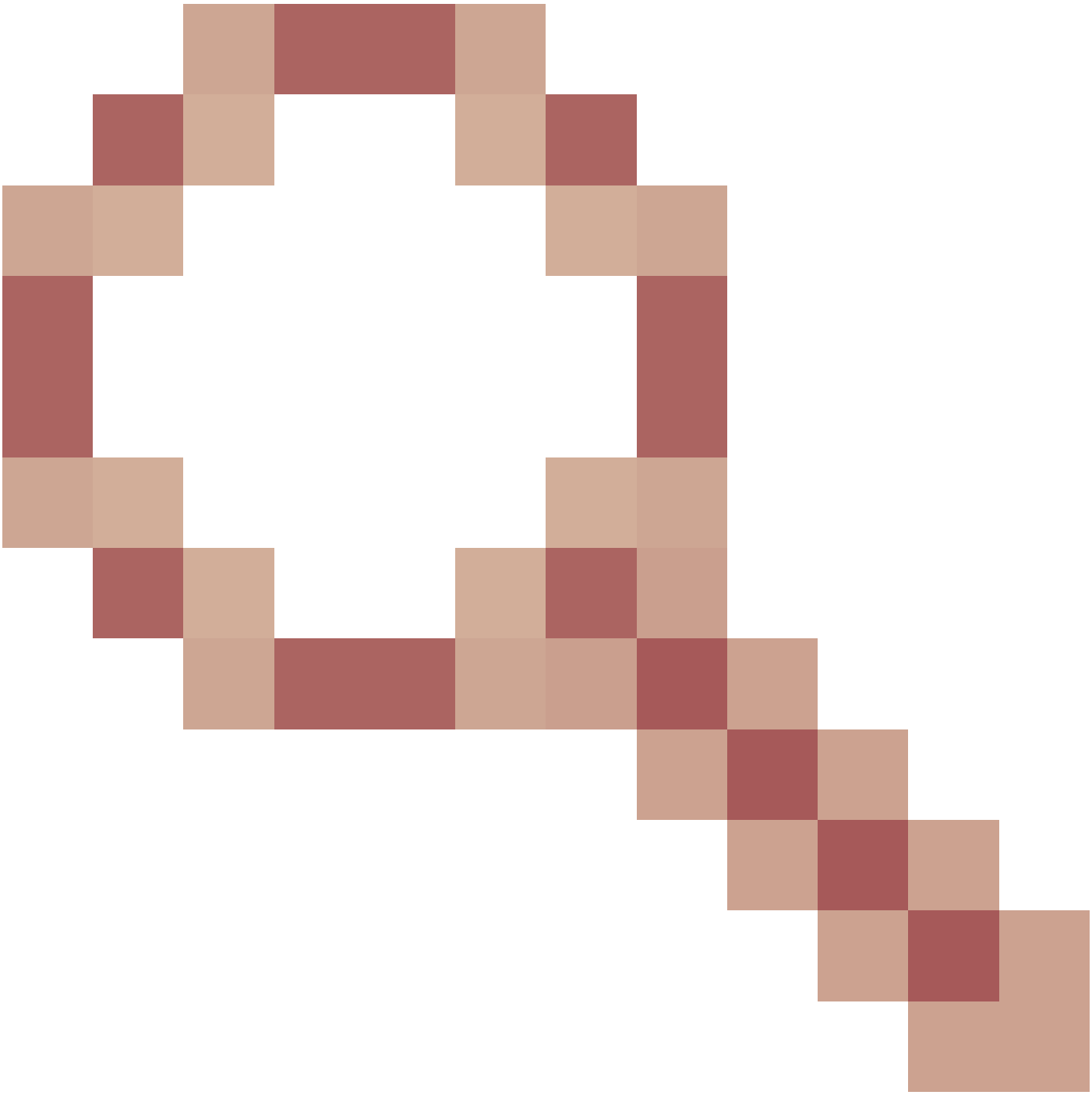
- https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/A-H/asa-command-ref-A-H/aa-ac-commands.html#wp6184732320

Probleem 7. ASDM eenmalig wachtwoord

Probleemoplossing - Aanbevolen stappen

- Ondersteuning van ASDM OTP-verificatie (eenmalig wachtwoord) is toegevoegd in ASA versie 8.x - 9.x en alleen in single-routed-mode.
- ASDM OTP-verificatie voor ASA Firewall transparante mode en/of multi-context mode valt niet in deze categorie.

Raadpleeg de Cisco Bug-id CSCtf23419



NIEUW: Ondersteuning van ASDM OTP-verificatie in multi-context en transparante modi

Probleem 8. Verbindingsprofiel toont niet alle methoden

Het probleem in dit geval is een discrepantie tussen de ASA CLI-configuratie en de ASDM UI.

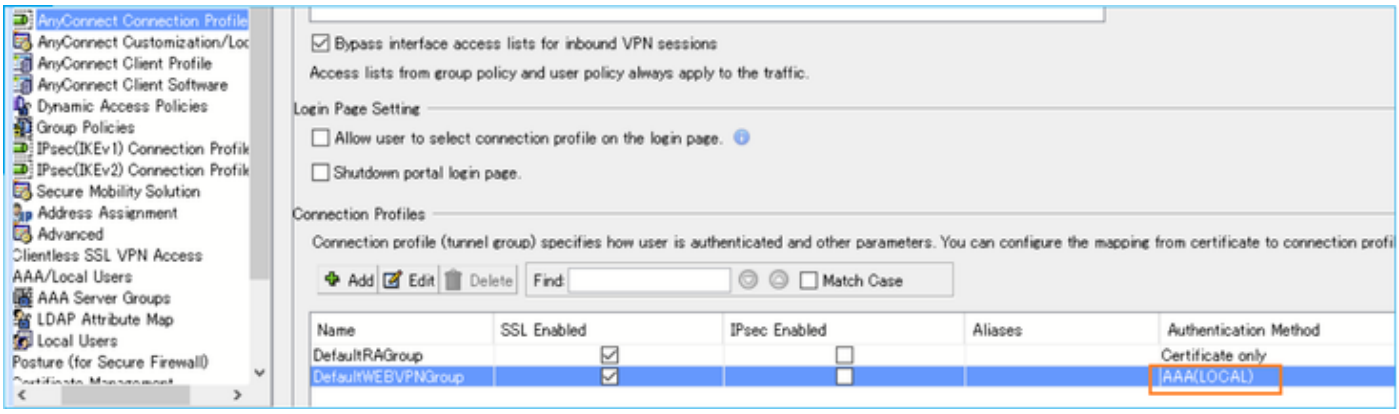
De CLI heeft in het bijzonder:

<#root>

```
tunnel-group DefaultWEBVPNGroup webvpn-attributes
```

authentication aaa certificate

Terwijl de ASDM UI de certificaatmethode niet vermeldt:



Probleemoplossing - Aanbevolen stappen

Dit is een cosmetische kwestie. De methode verschijnt niet in ASDM, maar de certificaathandleiding wordt gebruikt.

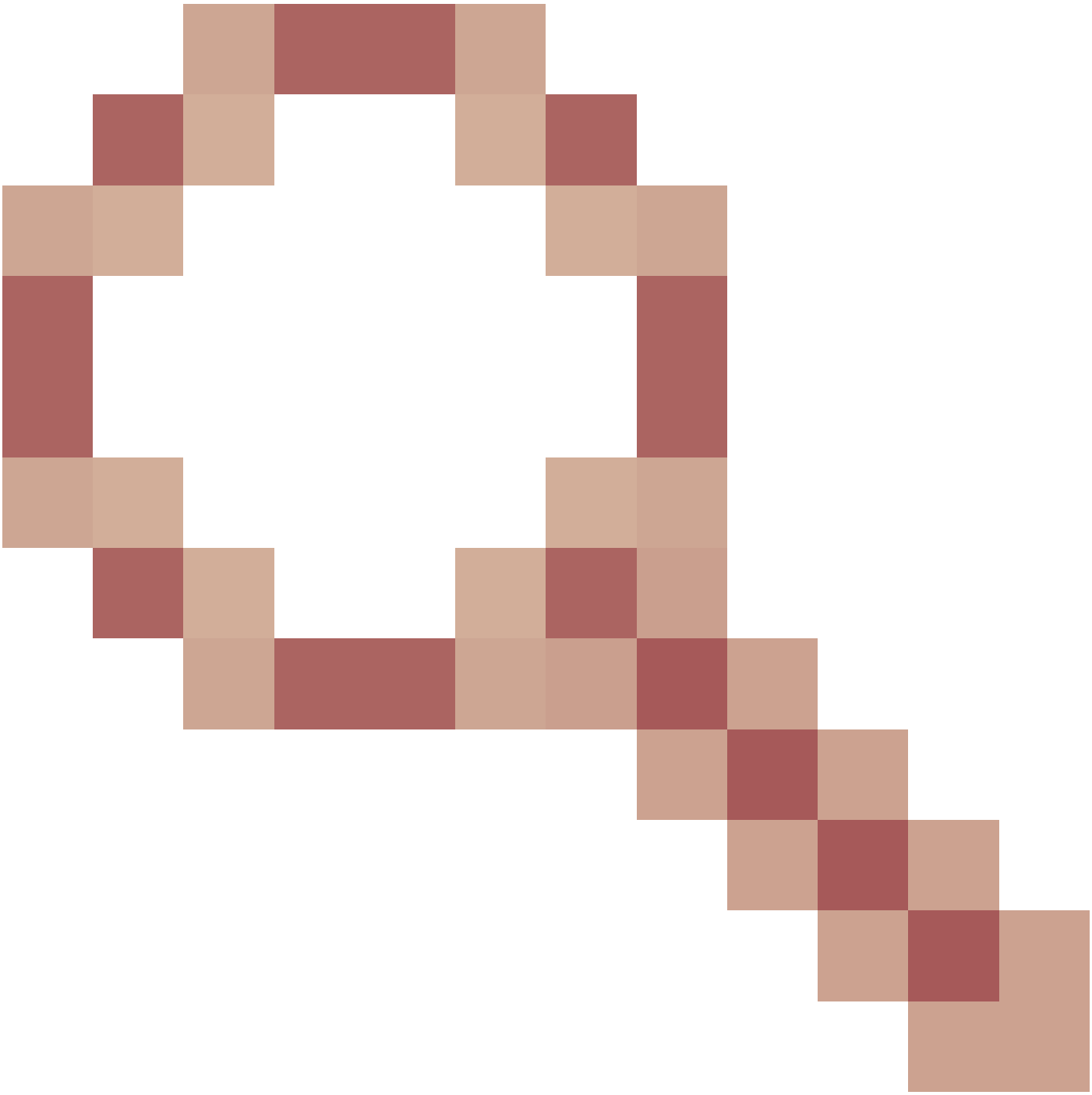
Probleem 9. ASDM-sessie leidt niet tot time-out

Het symptoom is dat de onderbreking van de ASDM GUI zitting niet in overweging wordt genomen.

Probleemoplossing - Aanbevolen stappen

Dit gebeurt wanneer de opdracht "aaa authenticatie http console LOCAL" niet is ingesteld op de beheerde ASA.

Raadpleeg de Cisco Bug-id CSCwj70826



NIEUW: een waarschuwing toevoegen: voor het instellen van de sessie-timeout, is "aaa authenticatie http console LOCAL" vereist

Tijdelijke oplossing

Configureer de opdracht ""aaa authenticatie http console LOCAL" op de beheerde ASA.

Probleem 10. ASDM LDAP-verificatie mislukt

Probleemoplossing - Aanbevolen stappen

Stap 1

Zorg ervoor dat de configuratie is geïnstalleerd, bijvoorbeeld:

<#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

Stap 2

Controleer de LDAP-serverstatus:

<#root>

```
asa#
```

show aaa-server

Goed scenario:

<#root>

```
Server status:
```

ACTIVE

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

Slecht scenario:

<#root>

```
Server status:
```

FAILED

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

Stap 3

Controleer of de LOKALE verificatie correct werkt door de LDAP-verificatie tijdelijk uit te

schakelen.

Stap 4

Op ASA open LDAP debugs en probeer de gebruiker te authenticeren:

<#root>

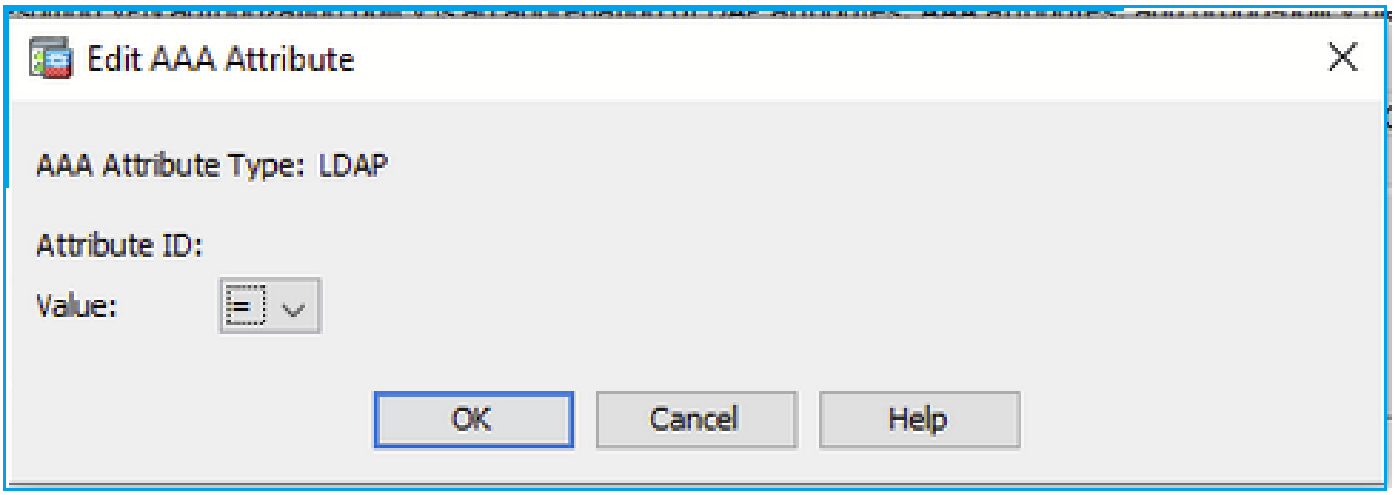
#

debug ldap 255

In de debugs zoek naar lijnen die hints bevatten zoals "Mislukt".

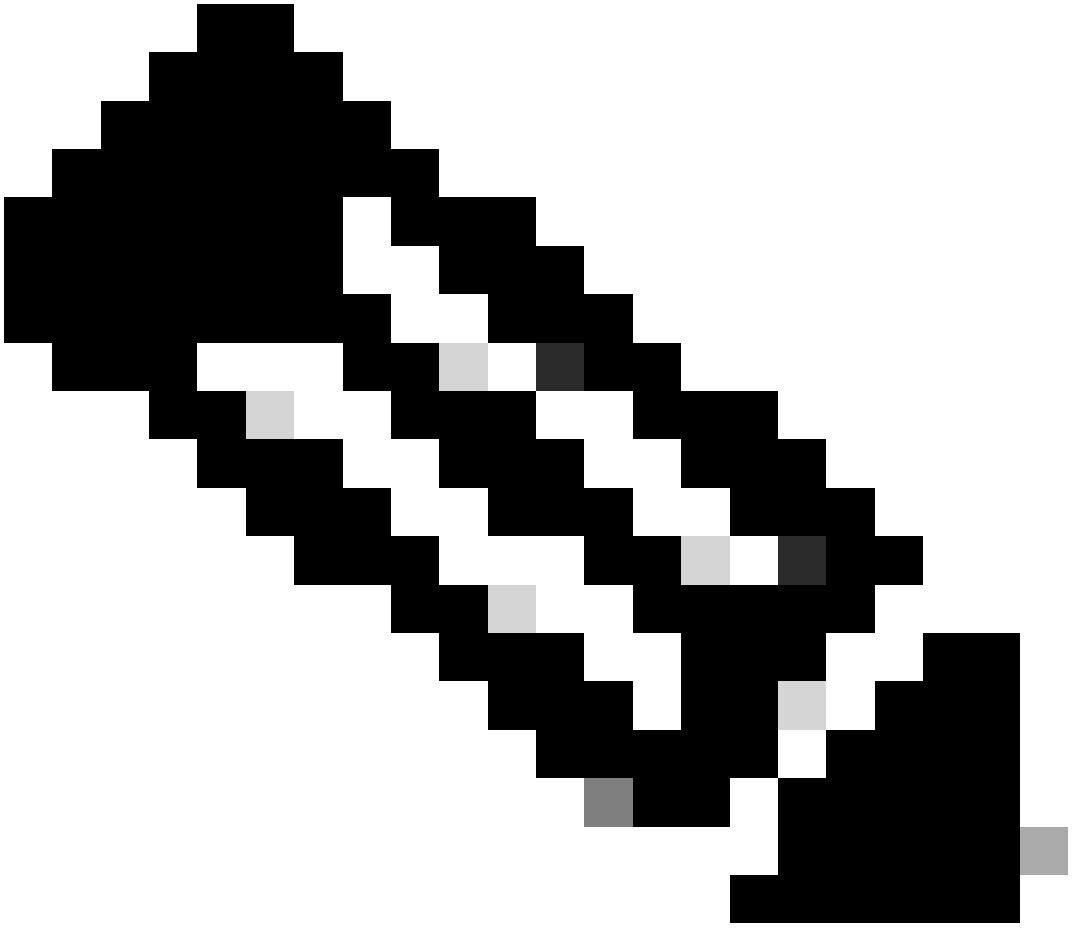
Probleem 11. ASDM WebVPN DAP-configuratie ontbreekt

Onder DAP configuratie op ASDM AAA Attributes type (Radius/LDAP) zijn niet alleen zichtbaar zien = en != op dropdown:



Probleemoplossing - Aanbevolen stappen

Dit is een softwaredefect dat door Cisco Bug-id CSCwa wordt getraceerd99370 ASDM:DAP-configuratie voor ontbrekende AAA-kenmerken (Radius/LDAP)

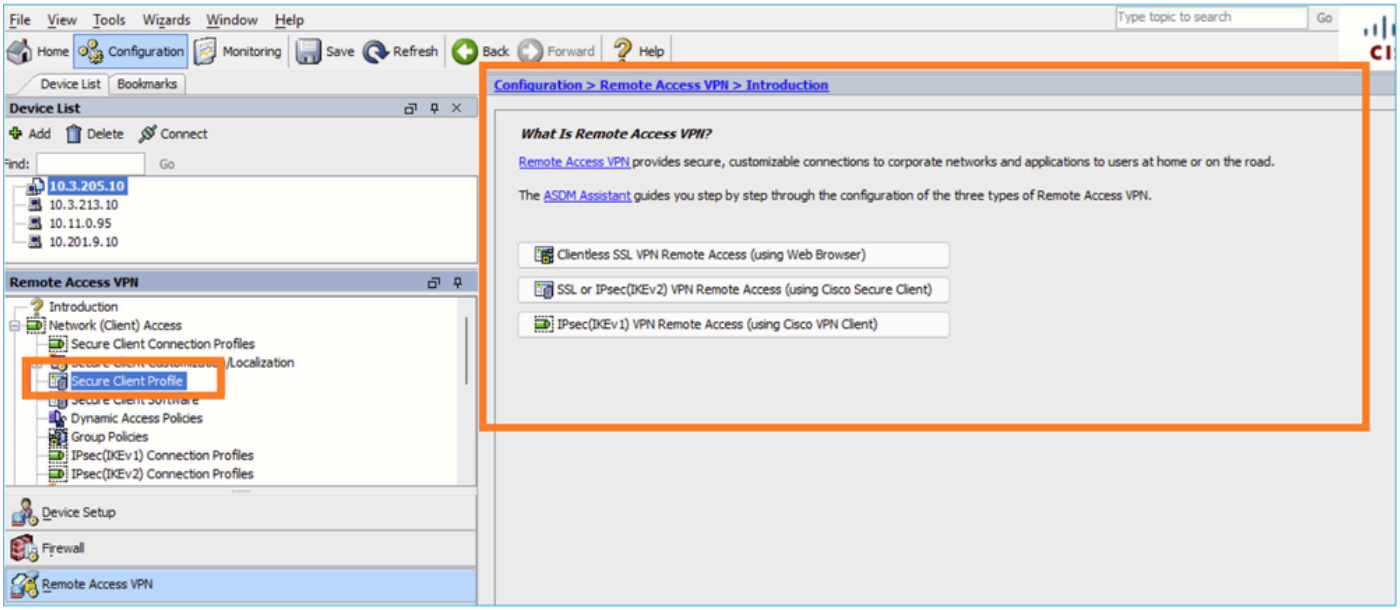


Opmerking: Dit defect is verholpen in recente ASDM-softwarereleases. Controleer de gebreken voor meer informatie.

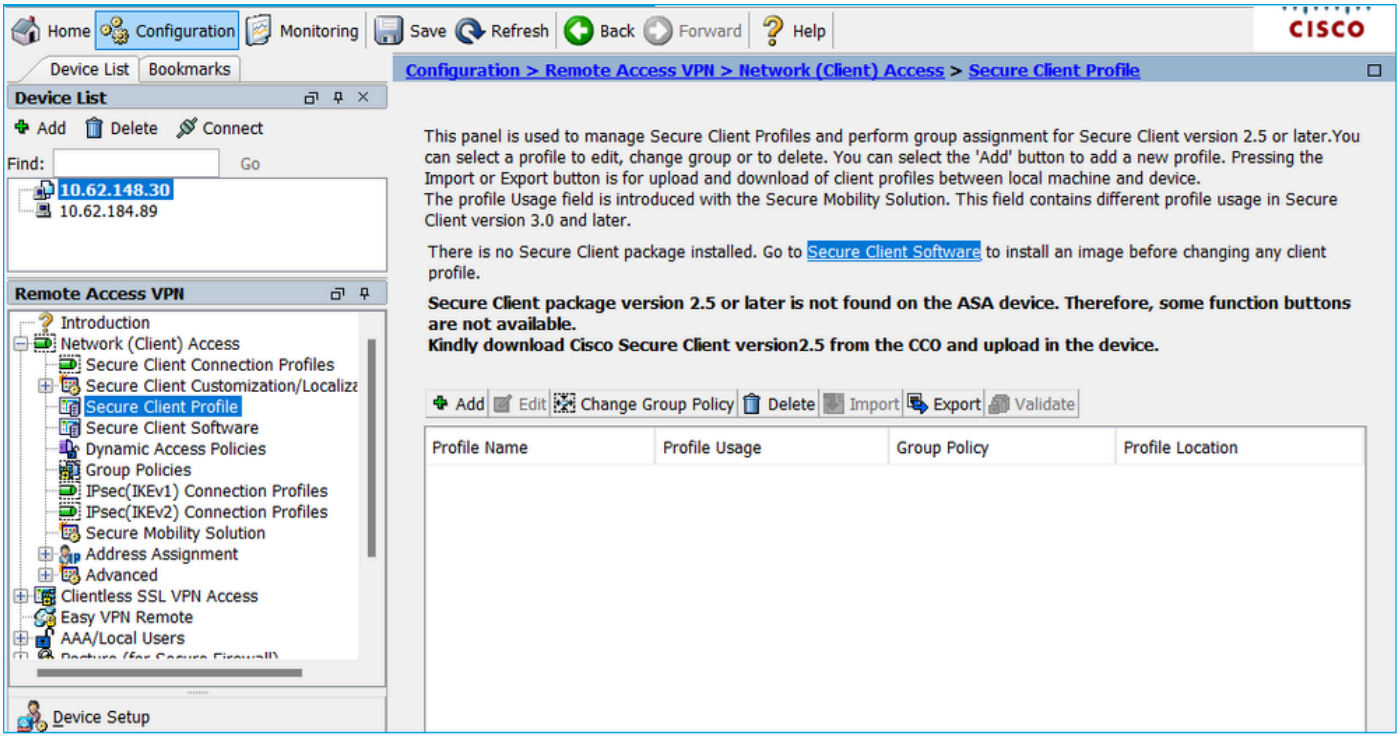
Probleemoplossing voor ASDM Andere problemen

Probleem 1. Kan geen toegang krijgen tot beveiligd clientprofiel op ASDM

De ASDM UI laat dit zien:



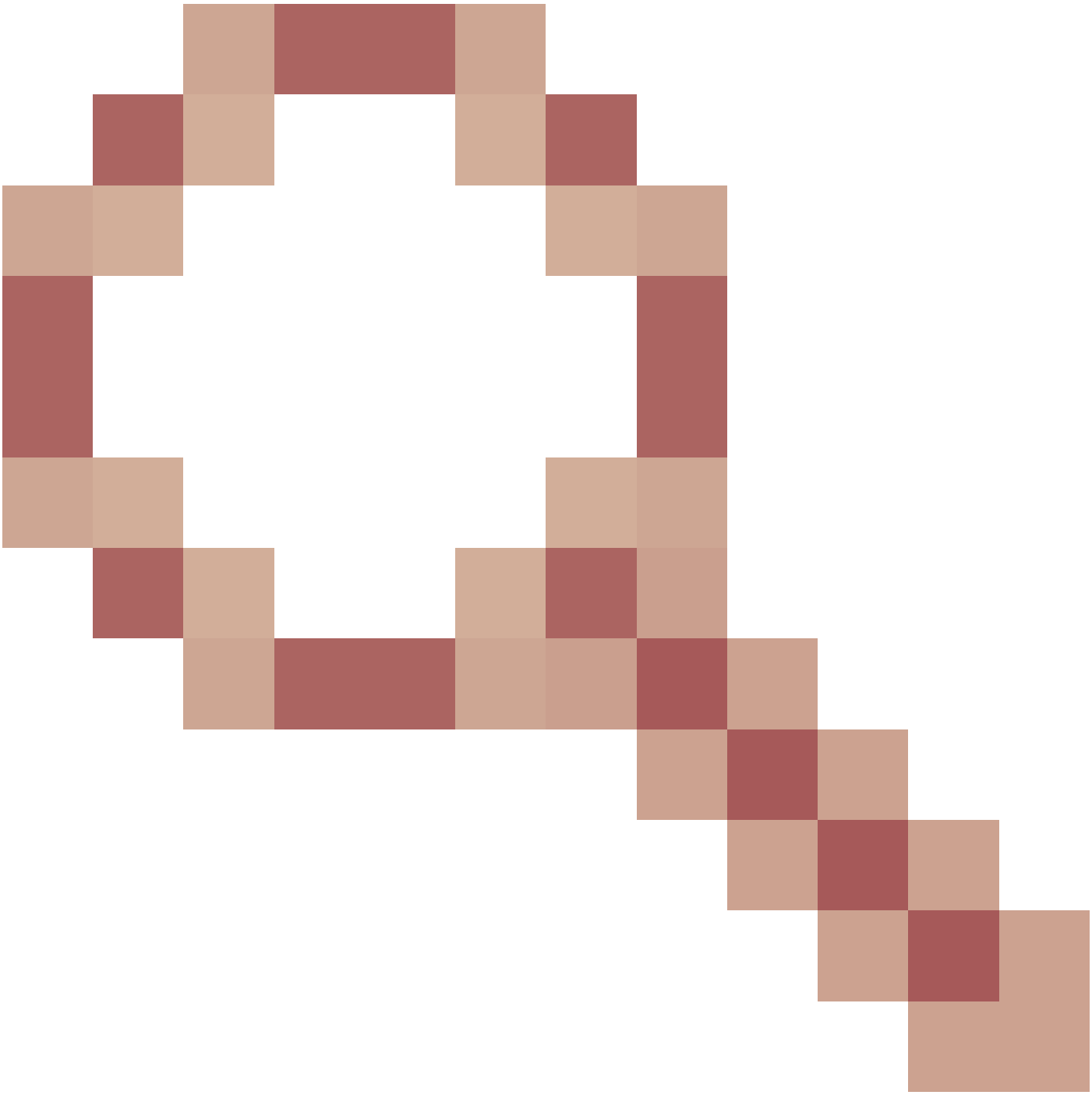
Terwijl de verwachte UI-uitvoer is:



Probleemoplossing - Aanbevolen stappen

Dit is een bekend defect:

Cisco Bug-id CSCwi56155



Kan geen toegang krijgen tot beveiligd clientprofiel op ASDM

Verweringen:

Downgrade AnyConnect

of

Upgrade ASDM naar versie 7.20.2

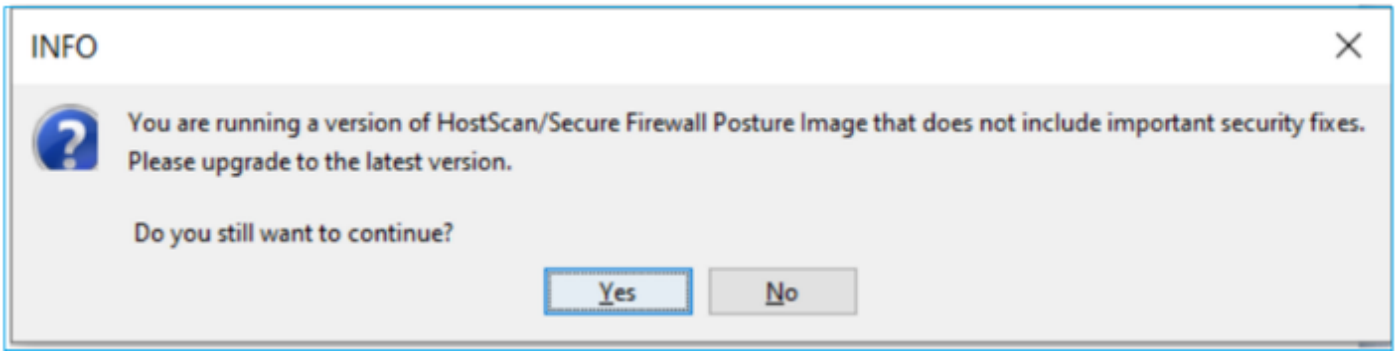
Controleer de tekortkomingen voor meer informatie. Daarnaast kunt u zich abonneren op het defect, zodat u een melding ontvangt over defect updates.

Probleem 2. ASDM toont pop-up voor hostscan - afbeelding bevat geen belangrijke

beveiligingsoplossingen

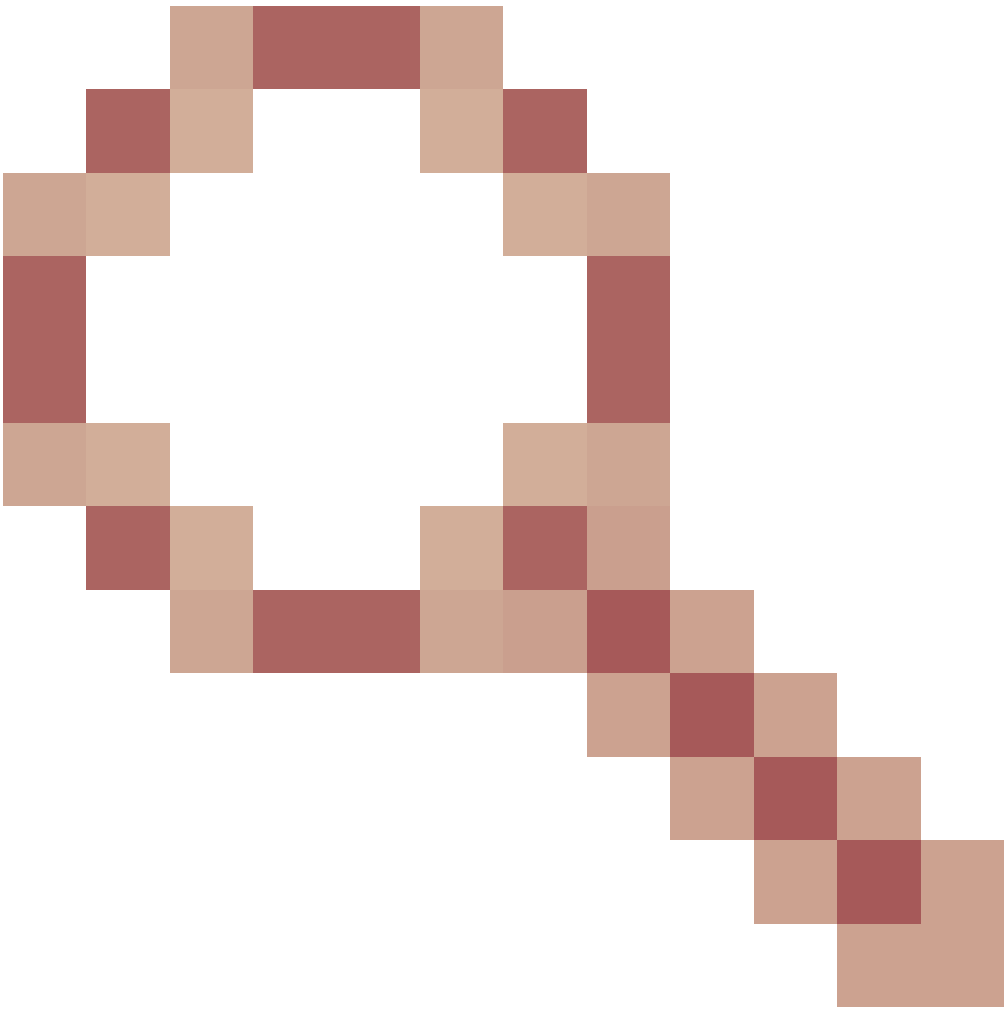
De ASDM UI toont:

"U voert een versie van HostScan/SecureFirewall Posture-afbeelding uit die geen belangrijke beveiligingsoplossingen bevat. Upgrade naar de nieuwste versie. Wilt u nog steeds doorgaan?"

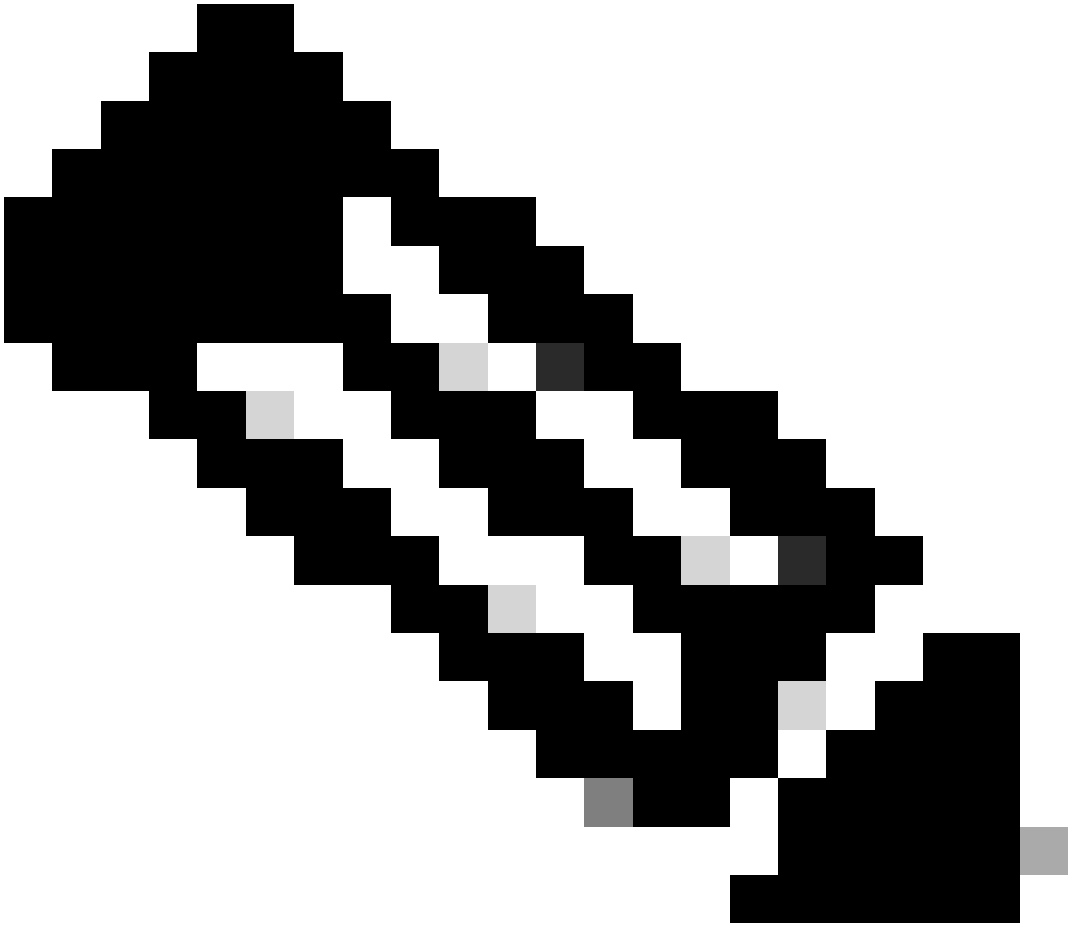


Probleemoplossing - Aanbevolen stappen

Dit is een bekend defect:



Cisco Bug-id CSCwc62461
Bij inloggen op ASDM pop-up voor hostscan - afbeelding bevat geen belangrijke beveiligingsoplossingen



Opmerking: Dit defect is verholpen in recente ASDM-softwarereleases. Controleer de gebreken voor meer informatie.

Tijdelijke oplossing:

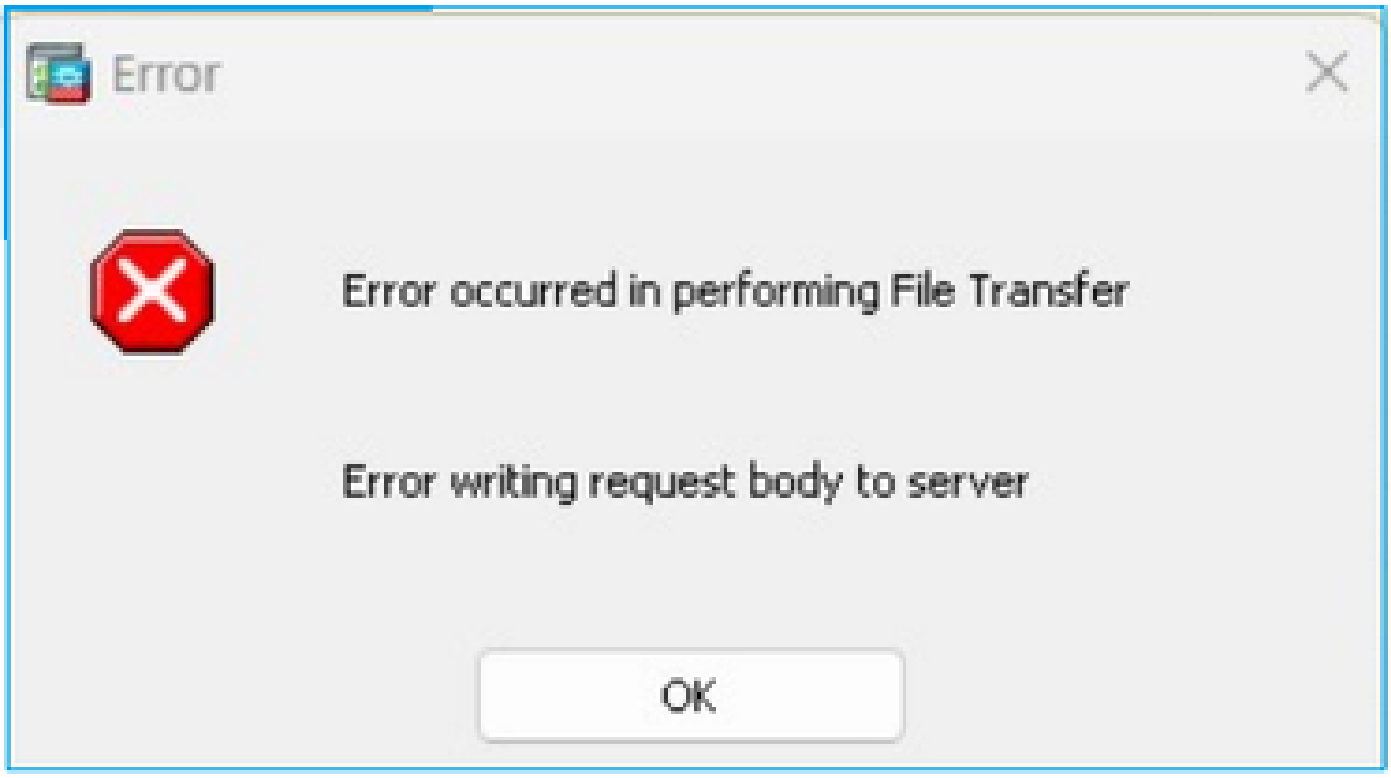
Klik op 'Ja' in het pop-upbericht om door te gaan.

Probleem 3. ASDM "Fout bij schrijven verzoek lichaam naar server" bij het kopiëren van een afbeelding via ASDM

De ASDM UI toont:

Fout bij uitvoeren van bestandsoverdracht

Fout bij schrijven van aanvraagformulier op server



Probleemoplossing - Aanbevolen acties

Dit is een bekend defect dat wordt gevolgd door:

Cisco Bug-id CSCtf74236

ASDM "Fout bij schrijven aanvraagformulier naar server" bij het kopiëren van de afbeelding

Tijdelijke oplossing

Gebruik SCP/TFTP om het bestand over te dragen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.