Dépannage de la configuration, de l'authentification et d'autres problèmes ASDM

Table des matières

Introduction

Ce document décrit la procédure de dépannage pour la configuration, l'authentification et d'autres problèmes de l'ASDM (Adaptive Security Appliance Device Manager).

Fond

Ce document fait partie de la série de dépannages ASDM, avec les documents suivants :

Liaison1<>

Lien2<>

Lien 3<>

Dépannage des problèmes de configuration ASDM

Problème 1. L’ASDM n’affiche aucune liste de contrôle d’accès appliquée à une interface

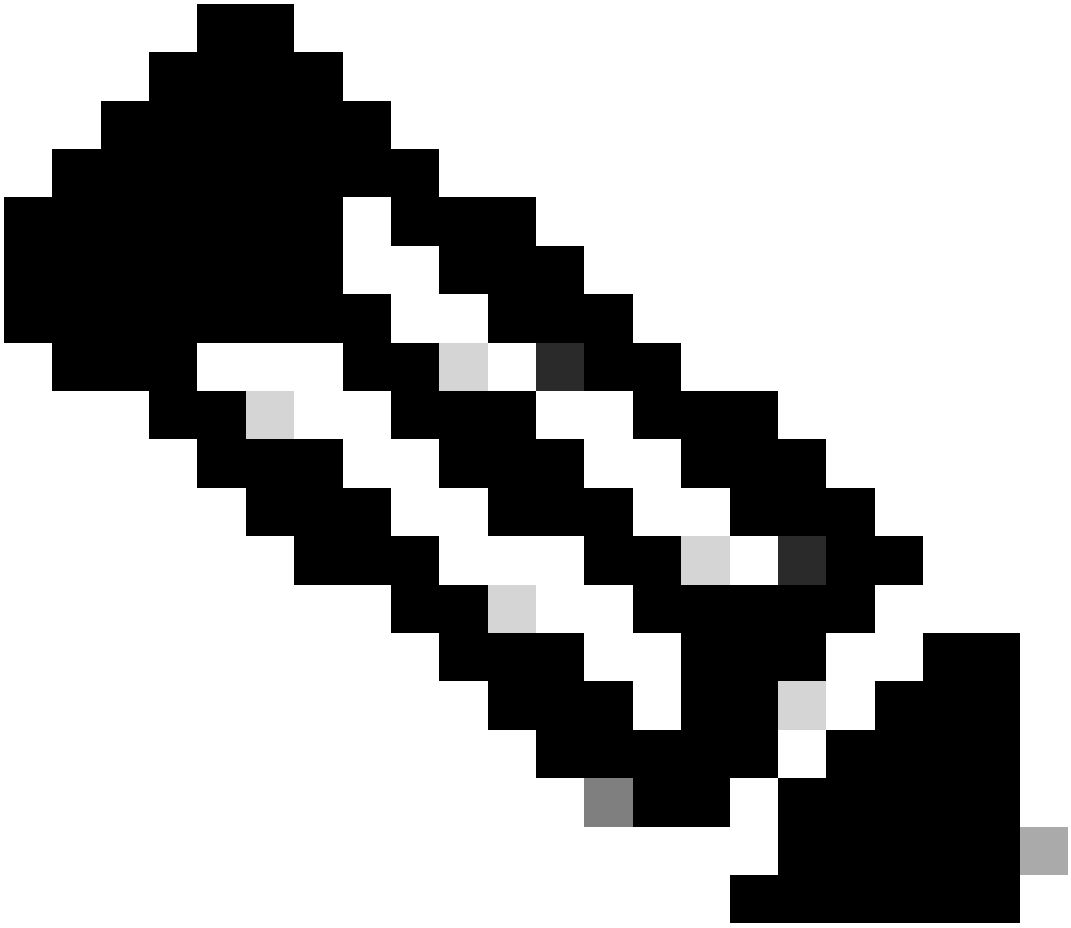
L'ASDM n'affiche aucune liste de contrôle d'accès appliquée à une interface, même si un groupe d'accès valide est appliqué à l'interface en question. Le message indique plutôt « 0 règles entrantes ». Ces symptômes sont observés dans les listes de contrôle d’accès L3 et L2 configurées dans la configuration du groupe d’accès pour une 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
```

Dépannage - Actions recommandées

Référez-vous au bogue logiciel Cisco ID CSCwj14147 « ASDM failed to load access-group config if L2 and L3 acl's are mixed. »



Remarque : Ce défaut a été corrigé dans les versions récentes du logiciel ASDM. Consultez les détails du défaut pour plus d'informations.

Problème 2. Incohérence du nombre d'accès entre l'interface CLI ASA et l'interface utilisateur ASDM

Les entrées de nombre d'accès dans l'ASDM ne sont pas cohérentes avec les nombres d'accès de la liste d'accès tels que rapportés par la commande show access-list sur la sortie du pare-feu.

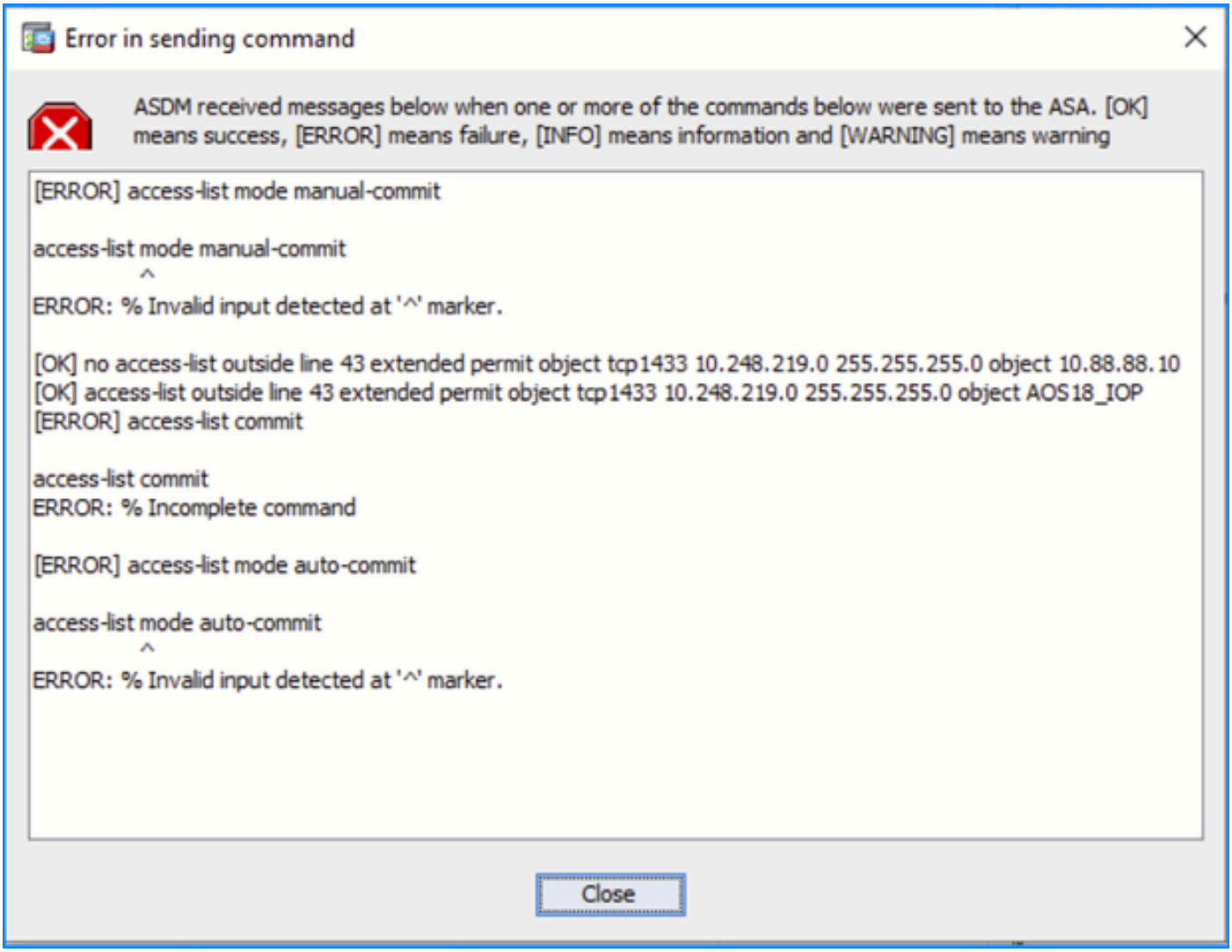
Dépannage - Actions recommandées

Référez-vous au bogue logiciel Cisco ID CSCtq38377 « ENH: L'ASDM doit utiliser le hachage de l'ACL calc'd sur l'ASA et non calc'd localement» et l'ID de bogue Cisco CSCtq38405« ENH : ASA a besoin d'un mécanisme pour fournir des informations de hachage ACL à ASD »

Problème 3. « ERREUR : % Entrée non valide détectée au niveau du marqueur '^'.» message d'erreur lors de la modification d'une ACL dans ASDM

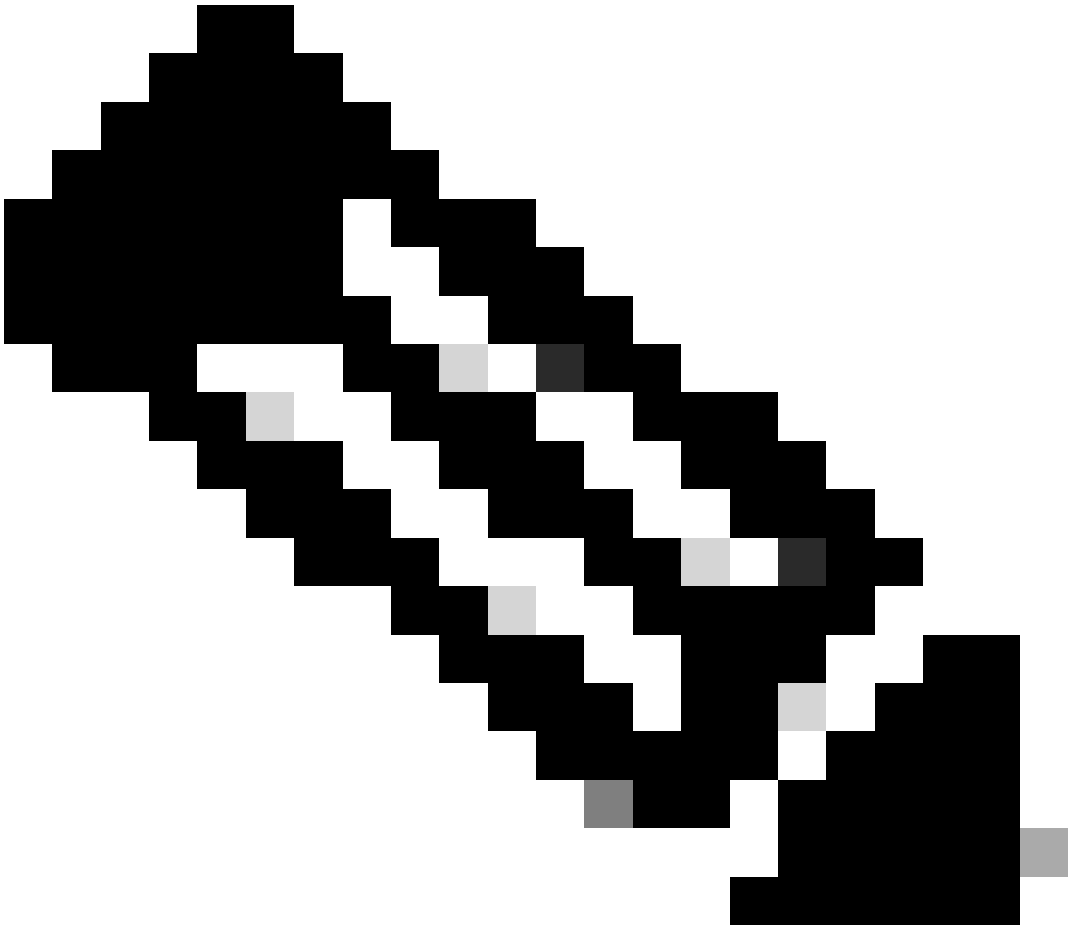
L'ERREUR « ERROR: % Entrée non valide détectée au niveau du marqueur '^'.» Un message d'erreur s'affiche lors de la modification d'une ACL dans ASDM :

```
[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.
```



Dépannage - Actions recommandées

Référez-vous au bogue logiciel Cisco ID CSCvq05064 « Edit an entry (ACL) from ASDM given an error. Lors de l'utilisation d'ASDM avec OpenJRE/Oracle - version 7.12.2 » et l'ID de bogue Cisco CSCvp88926 « Envoi de commandes d'ajout lors de la suppression de la liste d'accès ».



Remarque : Ces défauts ont été corrigés dans les versions récentes du logiciel ASDM. Consultez les détails du défaut pour plus d'informations.

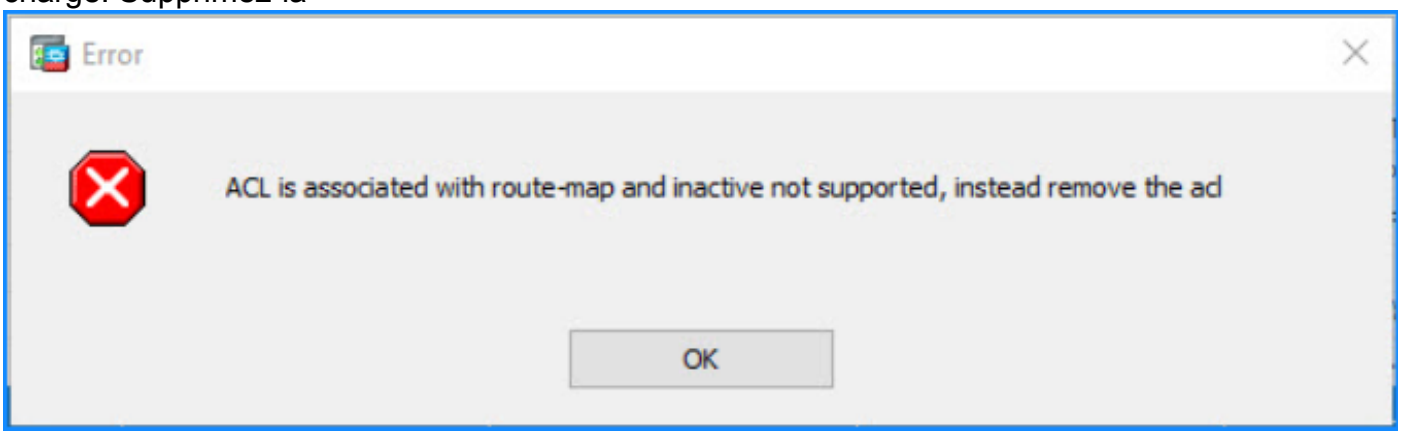
Problème 4. L'ERREUR « ERROR: La liste de contrôle d'accès est associée à route-map et inactive n'est pas prise en charge. Supprimez plutôt le message d'erreur « acl » dans des cas spécifiques

L'ERREUR « ERROR: La liste de contrôle d'accès est associée à la route-map et inactive n'est pas prise en charge. Le message d'erreur « remove the acl » s'affiche dans l'un des cas suivants :

1. Modifier une liste de contrôle d'accès dans ASDM utilisée dans une configuration de routage basée sur des politiques :

firewall (config)# access-list pbr line 1 permit ip any host 192.0.2.1

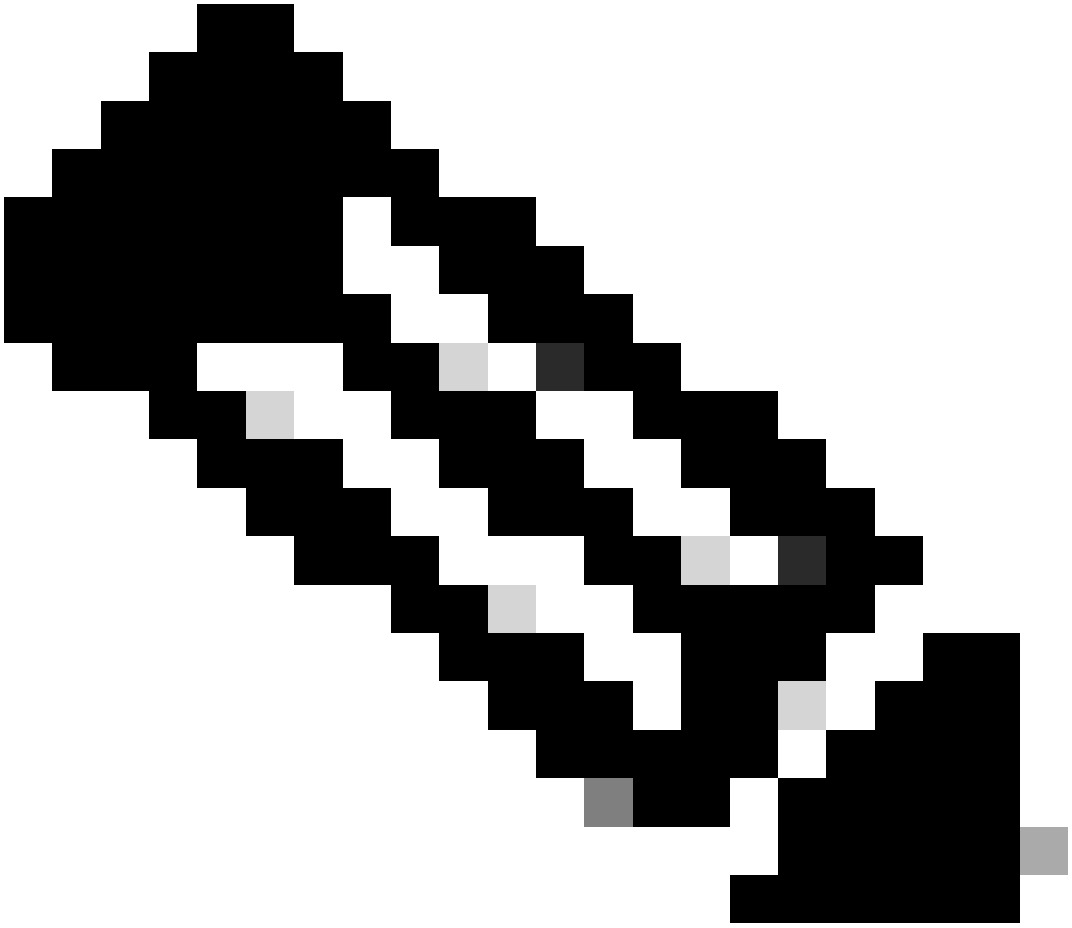
ERREUR : La liste de contrôle d'accès est associée à route-map et inactive n'est pas prise en charge. Supprimez-la



2. Modifier une liste de contrôle d'accès ASDM > Configuration -> Remote Access VPN -> Network (Client) Access > > Dynamic Access policy

Dépannage - Actions recommandées

1. Référez-vous au bogue logiciel Cisco ID CSCwb57615 « Configuring pbr access-list with line number failed ». La solution consiste à exclure le paramètre « line » de la configuration.
2. Référez-vous au bogue logiciel Cisco ID CSCwe34665 « Unable to Edit the ACL objects if it is already in use, get the exception ».



Remarque : Ces défauts ont été corrigés dans les versions récentes du logiciel ASA. Consultez les détails du défaut pour plus d'informations.

Problème 5. Aucune connexion dans ASDM Real-Time Log Viewer pour les connexions implicitement refusées

ASDM Real-Time Log Viewer n'affiche pas les journaux pour les connexions implicitement refusées.

Dépannage - Actions recommandées

Le refus implicite à la fin de la liste de contrôle d’accès ne génère pas de Syslog. Si vous voulez que tout le trafic refusé génère syslog, ajoutez une règle avec le mot clé log à la fin de l'ACL.

Problème 6. L’ASDM se fige lorsqu’il tente de modifier un objet réseau ou un groupe d’objets

L'ASDM se bloque lorsqu'il tente de modifier un objet réseau ou un groupe d'objets à partir de la page Configuration > Firewall > Access Rules sous l'onglet Addresses. L'utilisateur ne peut modifier aucun des paramètres de la fenêtre d'objet réseau lorsque ce problème se produit.

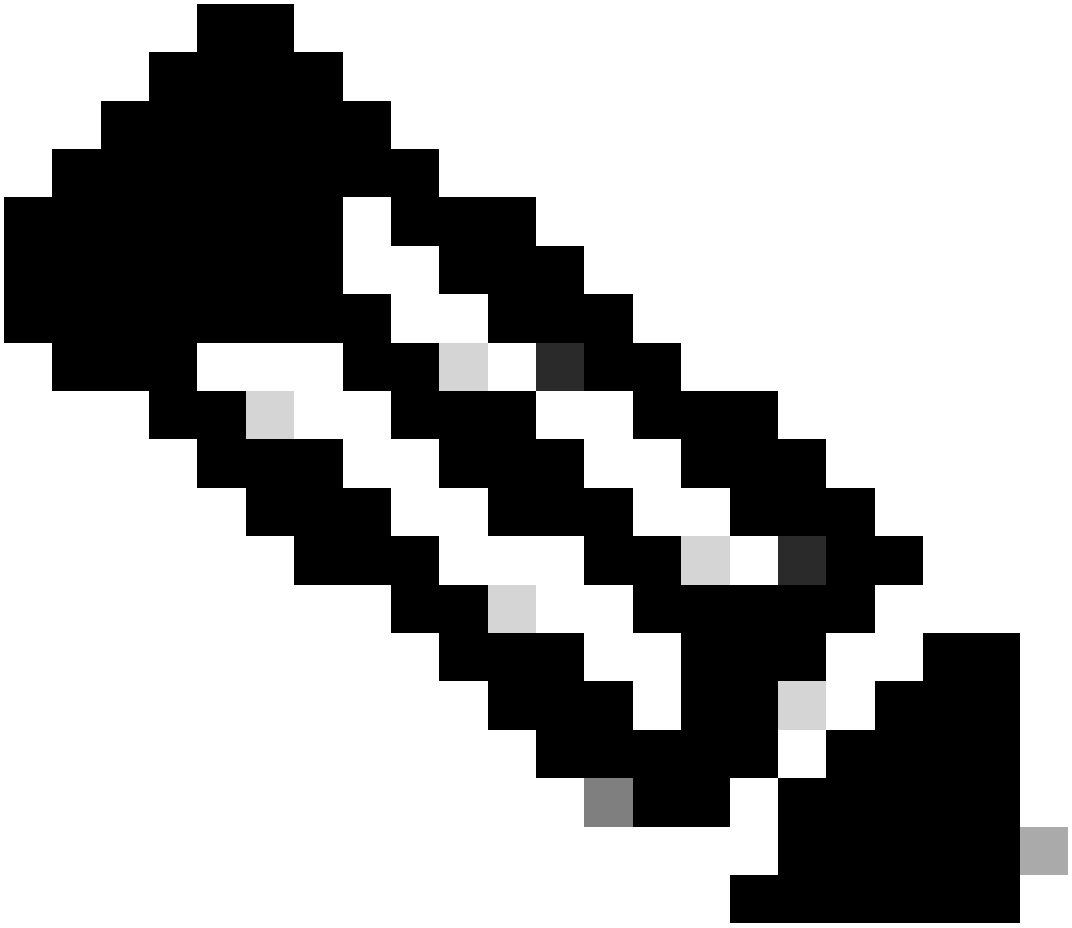
Dépannage - Actions recommandées

Référez-vous au bogue logiciel Cisco ID CSCwj12250 « ASDM se bloque lors de la modification d'objets réseau ou de groupes d'objets réseau ». La solution de contournement consiste à désactiver la collecte de statistiques sur l'hôte topN :

<#root>

```
ASA(config)#
```

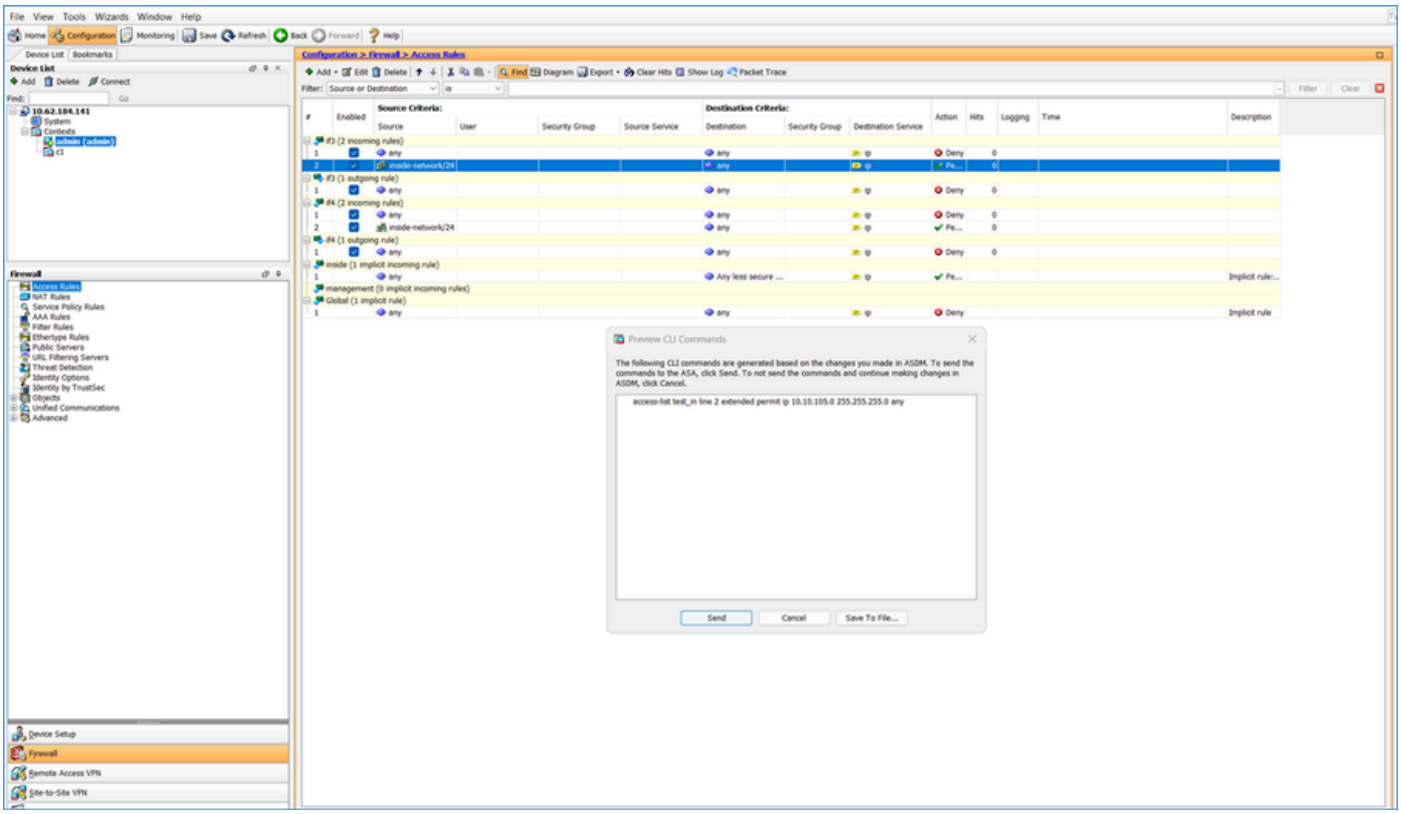
no hpm topN enable



Remarque : Ce défaut a été corrigé dans les versions récentes du logiciel ASDM. Consultez les détails du défaut pour plus d'informations.

Problème 7. ASDM peut afficher des règles de liste de contrôle d’accès supplémentaires pour différentes interfaces

ASDM peut afficher des règles de liste de contrôle d'accès supplémentaires pour différentes interfaces si une liste de contrôle d'accès au niveau de l'interface est modifiée. Dans cet exemple, une règle entrante n° 2 a été ajoutée à l'interface if3 ACL. L'ASDM affiche également #2 pour l'interface if4, alors que cette règle n'a pas été configurée par l'utilisateur. L'aperçu de commande affiche correctement une seule modification en attente. Il s'agit d'un problème d'affichage de l'interface utilisateur.



Dépannage - Actions recommandées

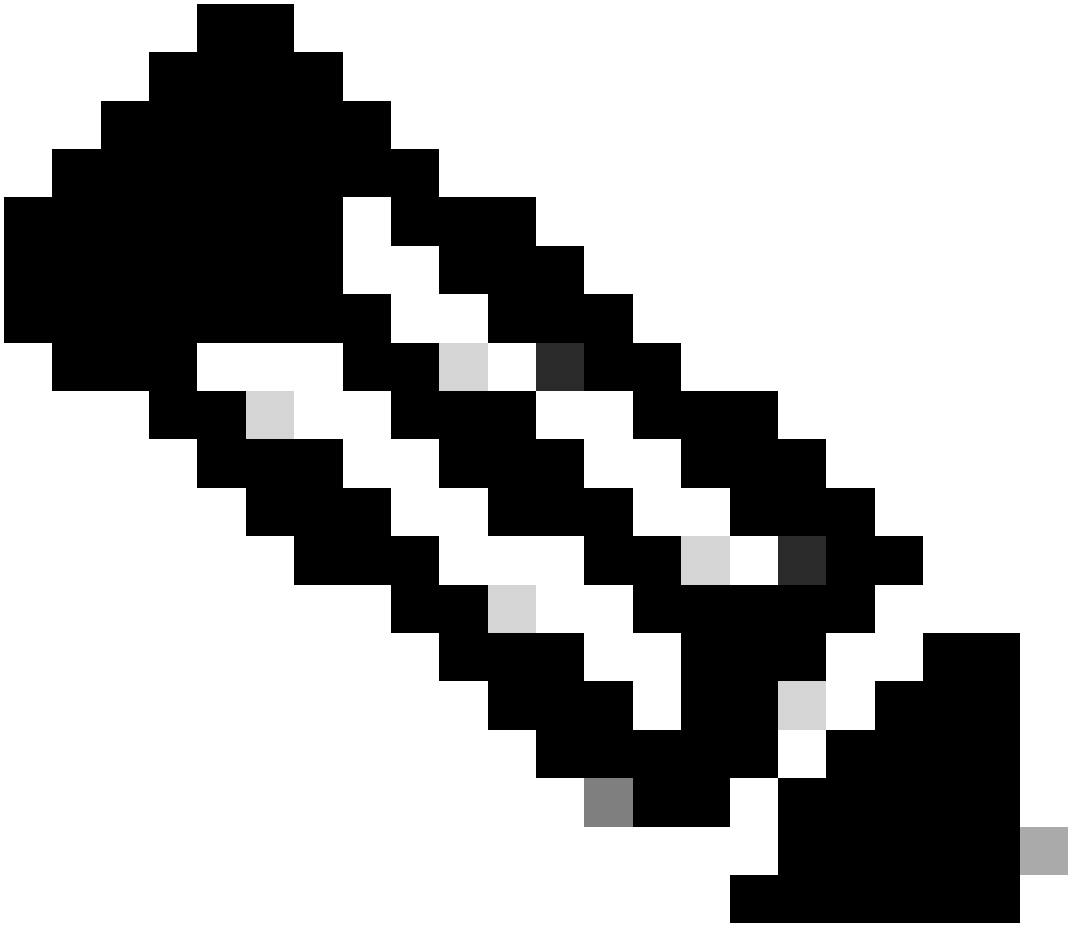
Référez-vous au bogue logiciel Cisco ID CSCwm71434 « ASDM may display duplicate interface access-list entries ».

Problème 8. Les journaux en temps réel ne sont pas disponibles dans la visionneuse de journaux en temps réel

Aucun journal n'est affiché dans la visionneuse de journaux en temps réel

Dépannage - Actions recommandées

1. Assurez-vous que la journalisation est configurée. Reportez-vous au livre 1 ASDM : Guide de configuration de l'ASDM pour les opérations générales de la gamme Cisco ASA, 7.22, chapitre : Journalisation.
2. Référez-vous au bogue logiciel Cisco ID CSCvf82966 « ASDM - Logging : Impossible d'afficher les journaux en temps réel ».

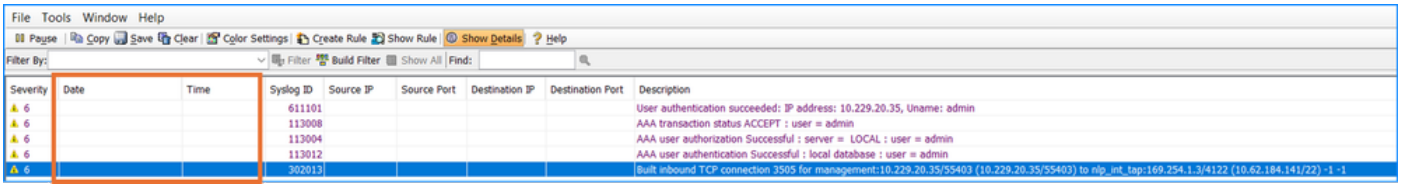


Remarque : Ce défaut a été corrigé dans les versions récentes du logiciel ASDM. Consultez les détails du défaut pour plus d'informations.

Références

- Livre 1 ASDM : Guide de configuration de l'ASDM pour les opérations générales de la gamme Cisco ASA, 7.22, chapitre : Journalisation.

Problème 9. Les colonnes Date et Heure sont vides dans la visionneuse du journal en temps réel



Dépannage - Actions recommandées

1. Vérifiez si le format d'horodatage de journalisation RFC5424 est utilisé :

<#root>

#

show run logging

logging enable

logging timestamp rfc5424

2. Si le format d'horodatage de journalisation RFC5424 est utilisé, référez-vous au bogue logiciel Cisco ID CSCvs52212 « ASDM ENH: fonctionnalité permettant aux Observateurs du journal des événements d'afficher les syslogs ASA avec le format d'horodatage rfc5424 ». La solution de contournement consiste à éviter d'utiliser le format RFC5424 :

<#root>

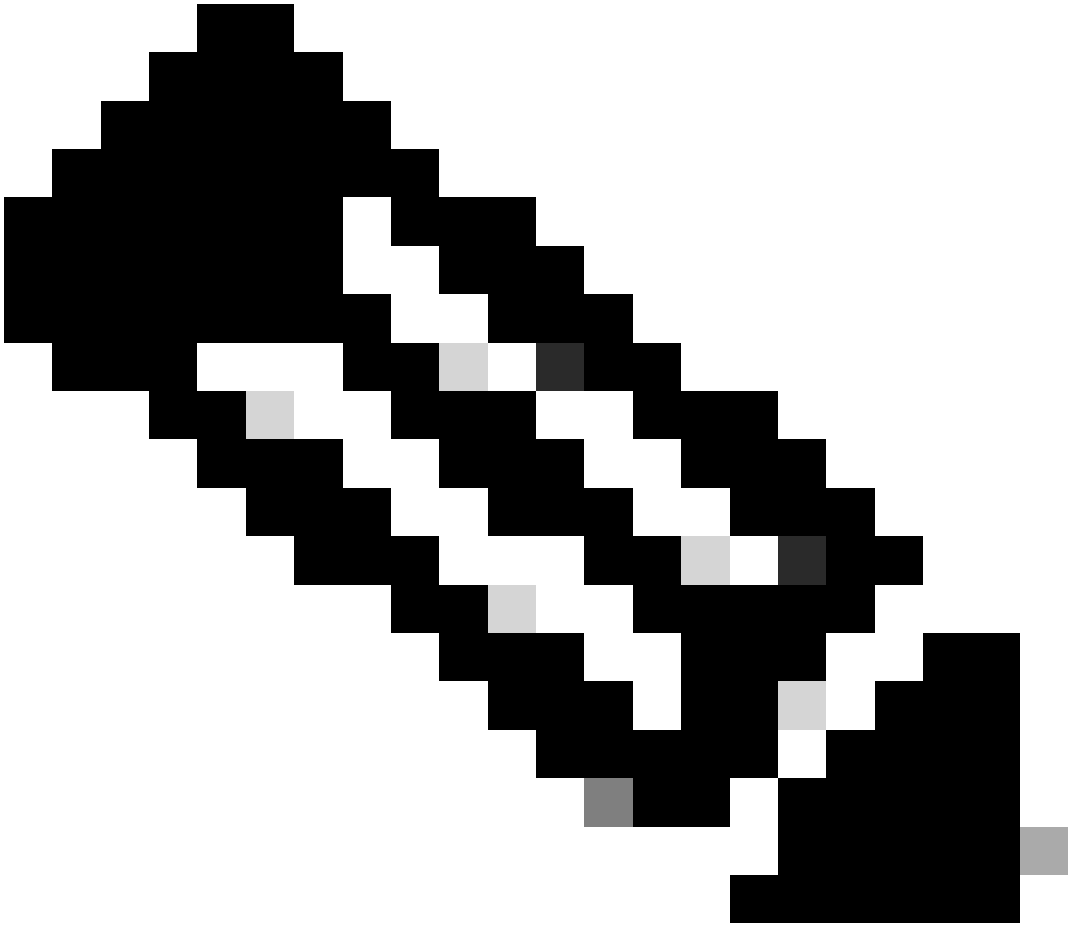
firewall(config)#

no logging timestamp rfc5424

firewall(config)#

logging timestamp

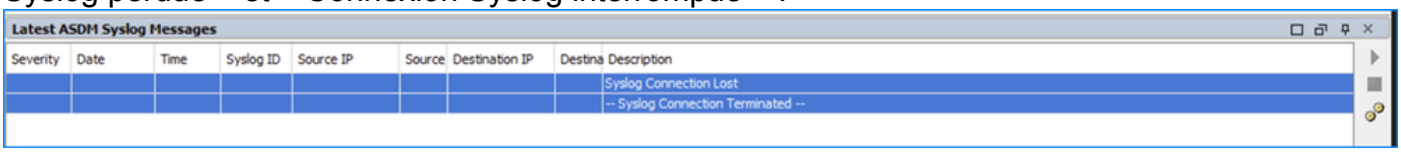
3. En outre, référez-vous à l'ID de bogue Cisco CSCwh70323 de défaut de logiciel « Entrée d'horodatage manquante pour certains messages syslog envoyés au serveur syslog ».



Remarque : Ce défaut a été corrigé dans les versions récentes du logiciel ASDM. Consultez les détails du défaut pour plus d'informations.

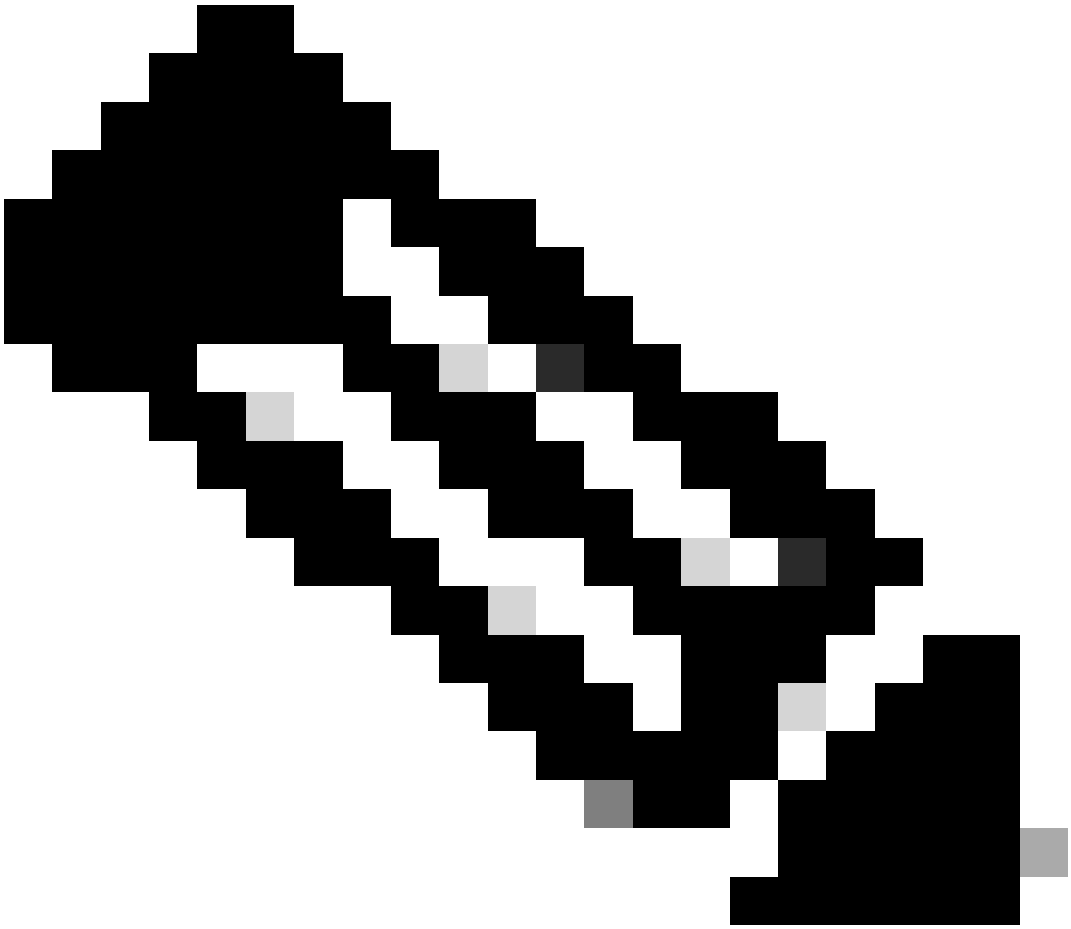
Problème 10. La connexion à ASDM peut échouer après la commutation vers un contexte différent dans un ASA multicontexte

L'onglet Derniers messages Syslog ASDM de la page d'accueil affiche les messages « Connexion Syslog perdue » et « Connexion Syslog interrompue » :



Dépannage - Actions recommandées

Assurez-vous que la journalisation est configurée. Référez-vous au bogue logiciel Cisco ID CSCvz15404 « ASA: Mode contexte multiple : La journalisation ASDM s'arrête, lorsqu'elle est basculée vers un contexte différent. »



Remarque : Ce défaut a été corrigé dans les versions récentes du logiciel ASDM. Consultez les détails du défaut pour plus d'informations.

Problème 11. La session ASDM se termine brusquement lors de la commutation entre différents contextes

La session ASDM s'est interrompue brusquement lors de la commutation entre différents contextes avec le message d'erreur « Le nombre maximal de sessions de gestion pour le protocole http ou l'utilisateur existe déjà. Veuillez réessayer ultérieurement. » Ces journaux sont affichés dans les messages syslog :

```
%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
```

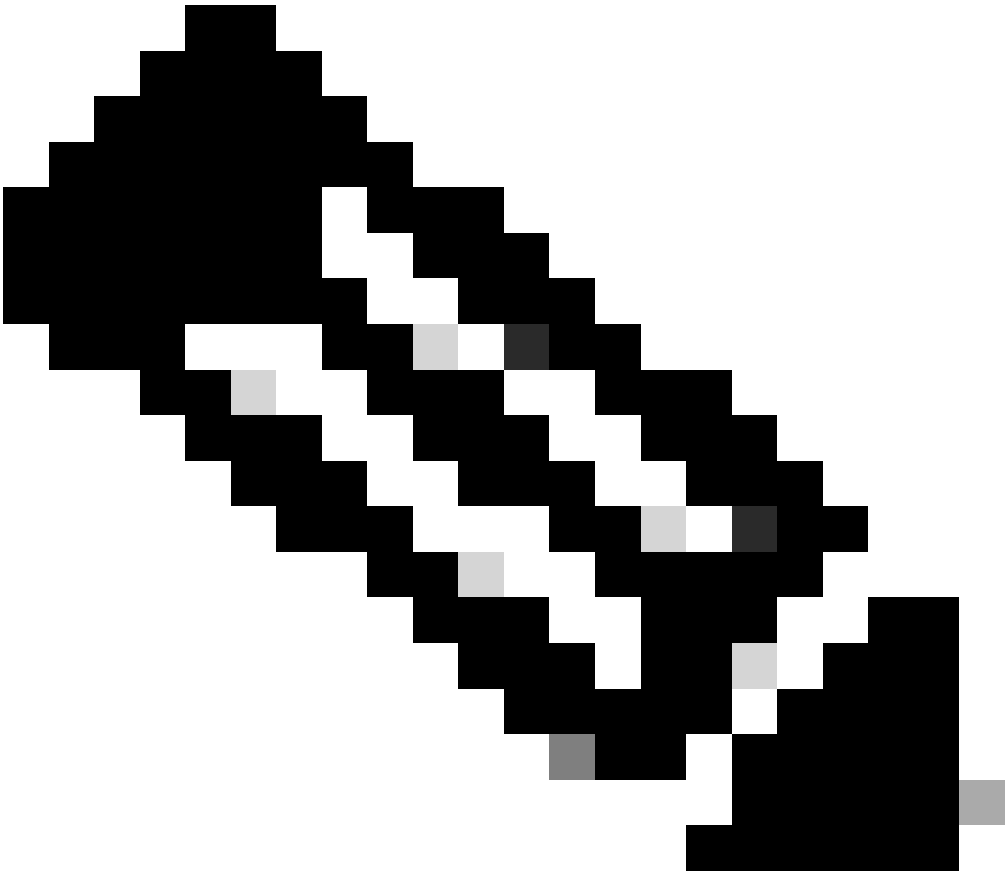
Dépannage - Actions recommandées

1. Vérifiez si l'utilisation actuelle des ressources ASDM a atteint la limite. Dans ce cas, le compteur Refusé augmente :

<#root>

```
firewall #

show resource usage resource ASDM


Resource                Current        Peak      Limit        Denied Context
ASDM

5

           5

5


10

 admin
```

2. Référez-vous à l'ID de bogue Cisco CSCvs72378 du logiciel « Session ASDM interrompue brusquement lors de la commutation entre différents contextes ».



Remarque : Ce défaut a été corrigé dans les versions récentes du logiciel ASA. Consultez les détails du défaut pour plus d'informations.

3. Si la version du logiciel a le correctif pour l'ID de bogue Cisco CSCvs72378, et que la ressource actuelle a atteint la limite, déconnectez certaines des sessions ASDM existantes. Vous pouvez fermer l'ASDM ou supprimer les connexions HTTPS pour l'adresse IP de l'hôte exécutant l'ASDM. Dans cet exemple, nous supposons que le serveur HTTP sur ASDM s'exécute sur le port HTTPS par défaut 443 :

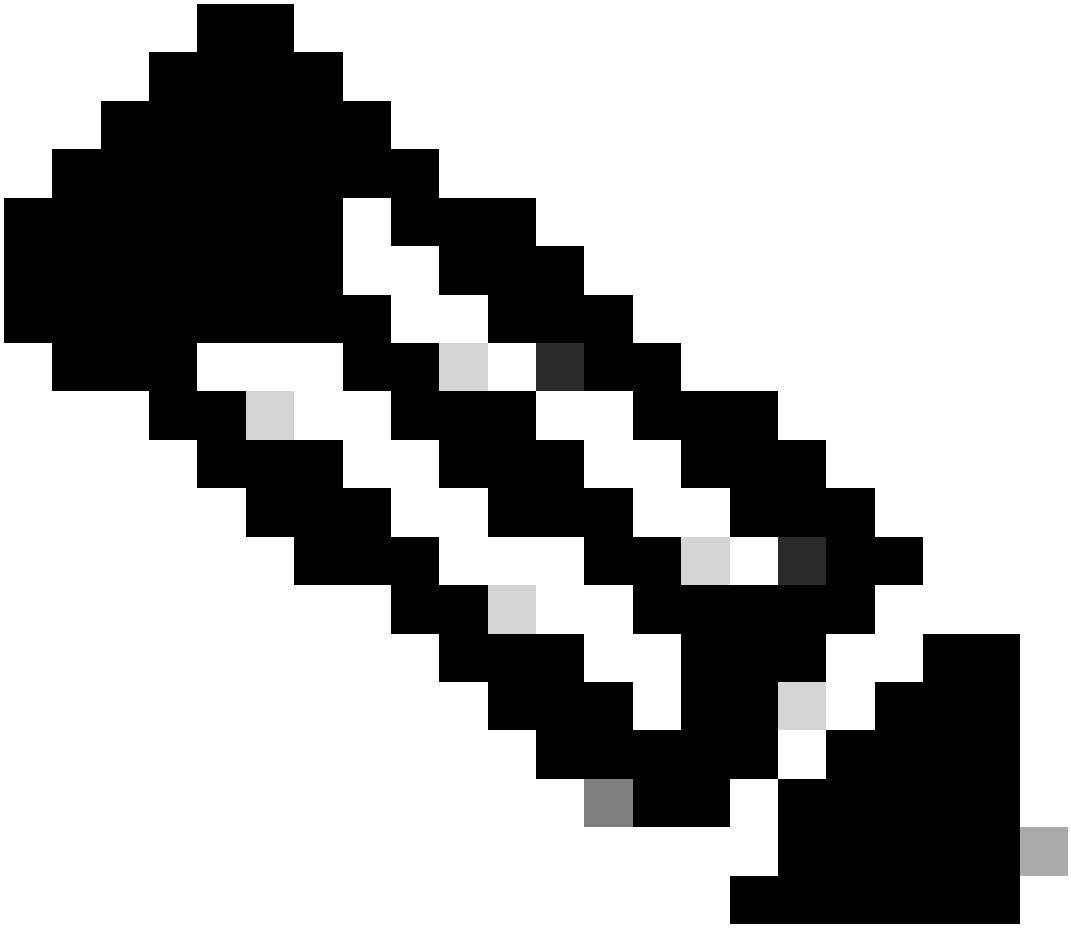
```
<#root>

#

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
```

Problème 12. ASDM se ferme/se termine de manière aléatoire avec le message « ASDM a reçu un message du périphérique ASA pour se déconnecter. L'ASDM va maintenant se fermer. »

Sur l'ASA multicontexte, l'ASDM se ferme/se termine de manière aléatoire avec le message « ASDM a reçu un message du périphérique ASA pour se déconnecter. L'ASDM va maintenant se fermer. ».

Dépannage - Actions recommandées

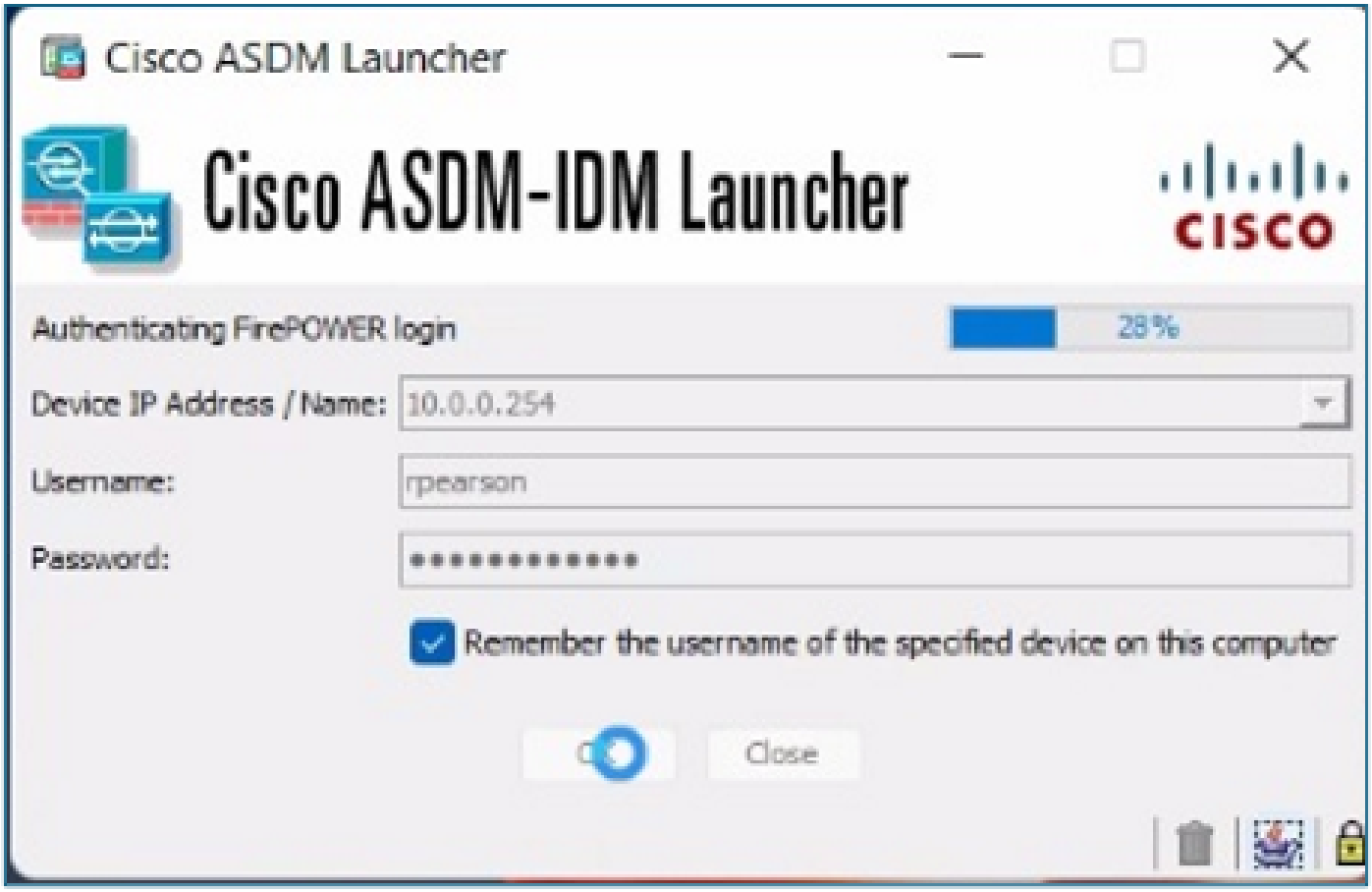
Référez-vous à l'ID de bogue Cisco CSCwh04395 défaut du logiciel « L'application ASDM se ferme/se termine de manière aléatoire avec un message d'alerte sur la configuration multicontexte ».



> Remarque : Ce défaut a été corrigé dans les versions récentes du logiciel ASA. Consultez les détails du défaut pour plus d'informations.

Problème 13. La charge ASDM se bloque avec le message « Authentication FirePOWER login »

La charge ASDM se bloque avec le message « Authentication FirePOWER login » :



Les journaux de la console Java affichent le message « Failed to connect to FirePower, persistent without it » :

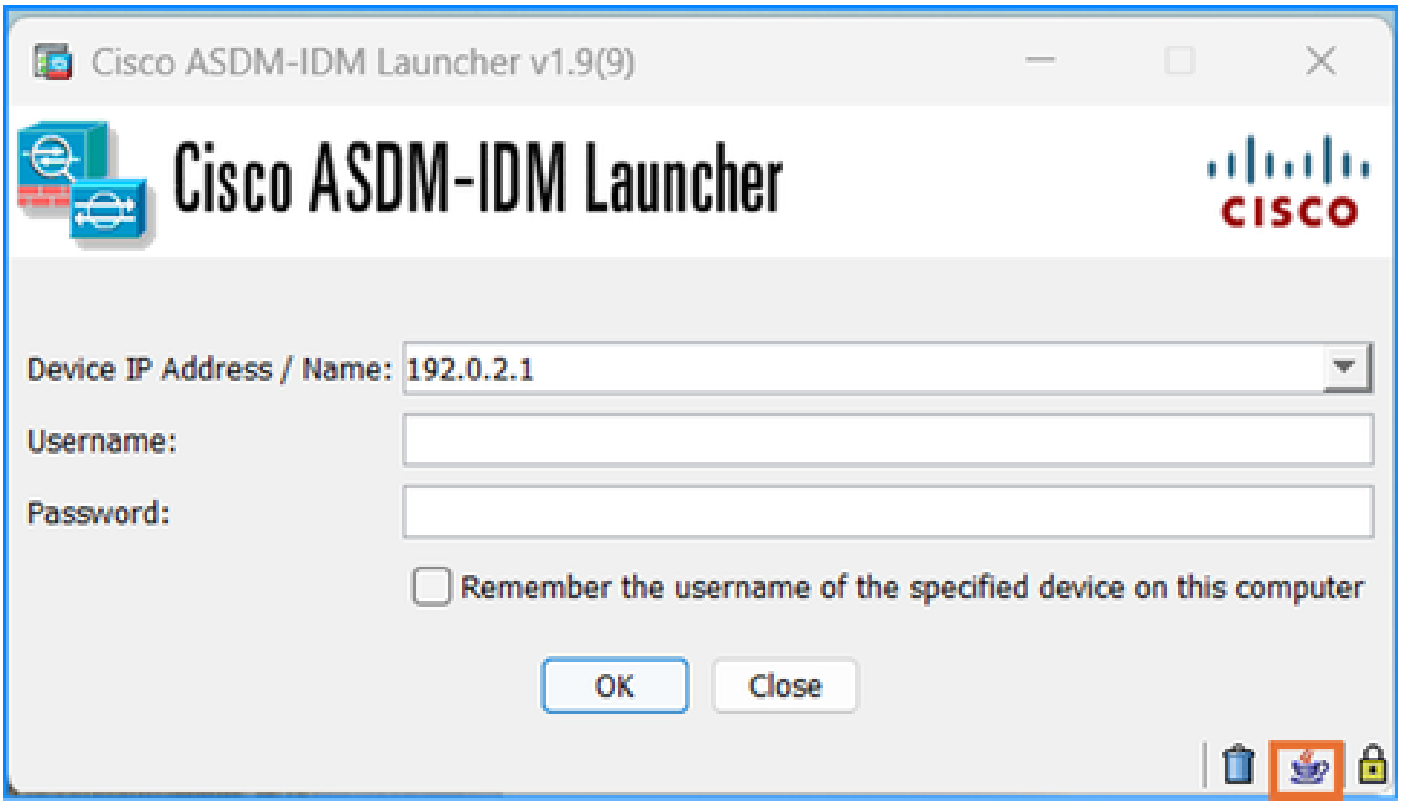
<#root>

```
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)
```

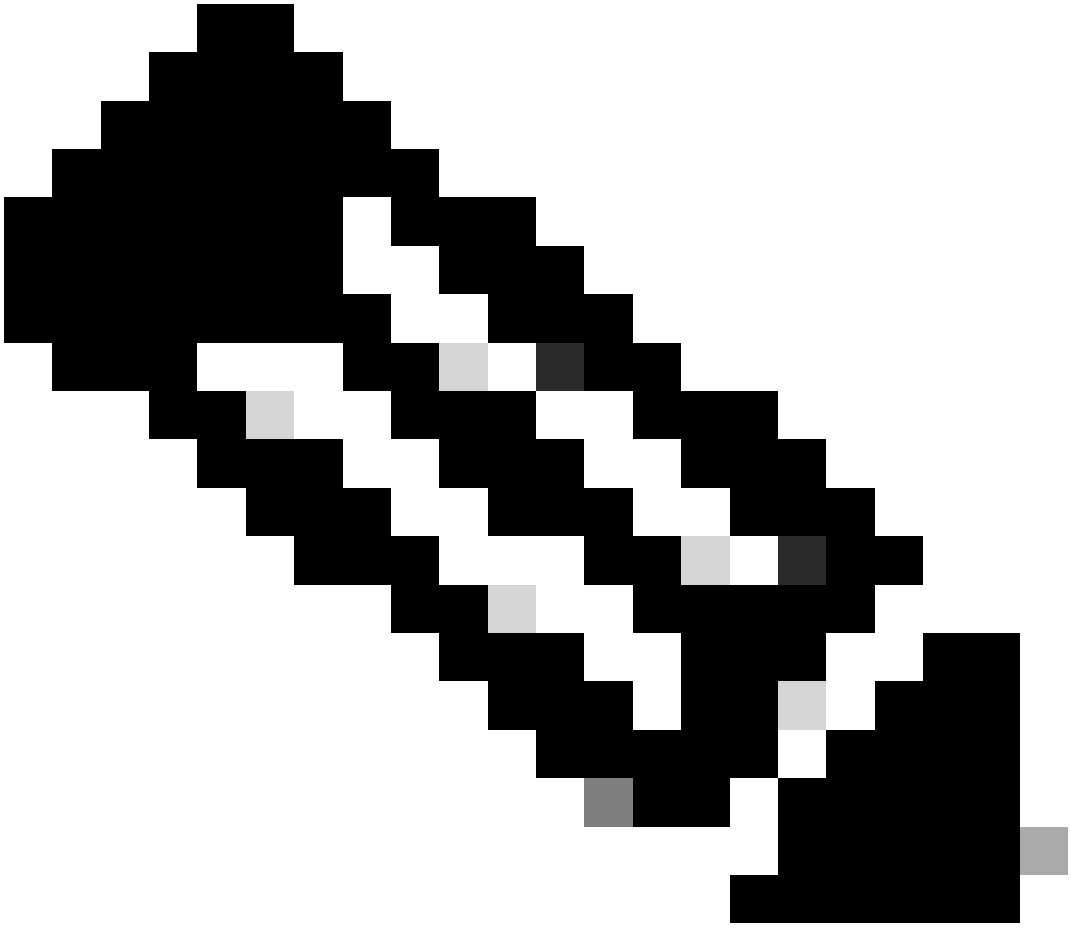
Pour vérifier ce symptôme, activez les journaux de la console Java :



Dépannage - Actions recommandées

Référez-vous au bogue logiciel Cisco ID CSCwe15164 « ASA: L'ASDM ne peut pas afficher les onglets SFR tant qu'il n'est pas « réveillé » via son interface de ligne de commande. Étapes de contournement :

1. Fermez le gestionnaire ASDM.
2. Obtenez un accès SSH au SFR et passez l'utilisateur à root (sudo su).
3. Après avoir effectué les étapes ci-dessus, relancez l'ASDM une fois de plus et il peut être en mesure de charger les onglets Firepower (SFR).



Remarque : Ce défaut a été corrigé dans les versions récentes du logiciel Firepower. Consultez les détails du défaut pour plus d'informations.

Problème 14. ASDM n’affiche pas la gestion/configuration du module Firepower

La configuration du module Firepower n'est pas disponible sur ASDM.

Dépannage - Actions recommandées

1. Assurez-vous que les versions ASA, ASDM, du module Firepower et du système d'exploitation sont compatibles. Reportez-vous aux Notes de version de Cisco Secure Firewall ASA, Notes de version de Cisco Secure Firewall ASDM, Compatibilité Cisco Secure Firewall ASA :

- ASA 9.14/ASDM 7.14/Firepower 6.6 est la version finale du module ASA FirePOWER sur les

modèles ASA 5525-X, 5545-X et 5555-X.
- ASA 9.12/ASDM 7.12/Firepower 6.4.0 est la version finale du module ASA FirePOWER sur les modèles ASA 5515-X et 5585-X.
- ASA 9.9/ASDM 7.9(2)/Firepower 6.2.3 est la version finale du module ASA FirePOWER sur les gammes ASA 5506-X et 5512-X.
- Les versions ASDM sont rétrocompatibles avec toutes les versions ASA précédentes, sauf indication contraire. Par exemple, ASDM 7.13(1) peut gérer un ASA 5516-X sur ASA 9.10(1).
- L'ASDM n'est pas pris en charge pour la gestion des modules FirePOWER avec ASA 9.8(4.45)+, 9.12(4.50)+, 9.14(4.14)+ et 9.16(3.19)+; vous devez utiliser FMC pour gérer le module avec ces versions. Ces versions d'ASA nécessitent ASDM 7.18(1.152) ou une version ultérieure, mais la prise en charge ASDM du module ASA FirePOWER se terminait par 7.16.
- ASDM 7.13(1) et ASDM 7.14(1) ne prenaient pas en charge ASA 5512-X, 5515-X, 5585-X et ASASM ; vous devez effectuer une mise à niveau vers ASDM 7.13(1.101) ou 7.14(1.48) pour restaurer la prise en charge ASDM.

2. Si les versions sont compatibles, vérifiez si le module est opérationnel :

<#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
```

Si le module est en panne, la commande sw-module module reset peut être utilisée pour réinitialiser le module, puis recharger le logiciel du module.

Références

- Notes de version de Cisco Secure Firewall ASA
- Notes de version de Cisco Secure Firewall ASDM
- Compatibilité Cisco Secure Firewall ASA

Problème 15. Les profils clients sécurisés sont inaccessibles sur l'ASDM

Les journaux de la console Java affichent l'exception « java.lang.ArrayIndexOutOfBoundsException : Message d'erreur 3 pouces :

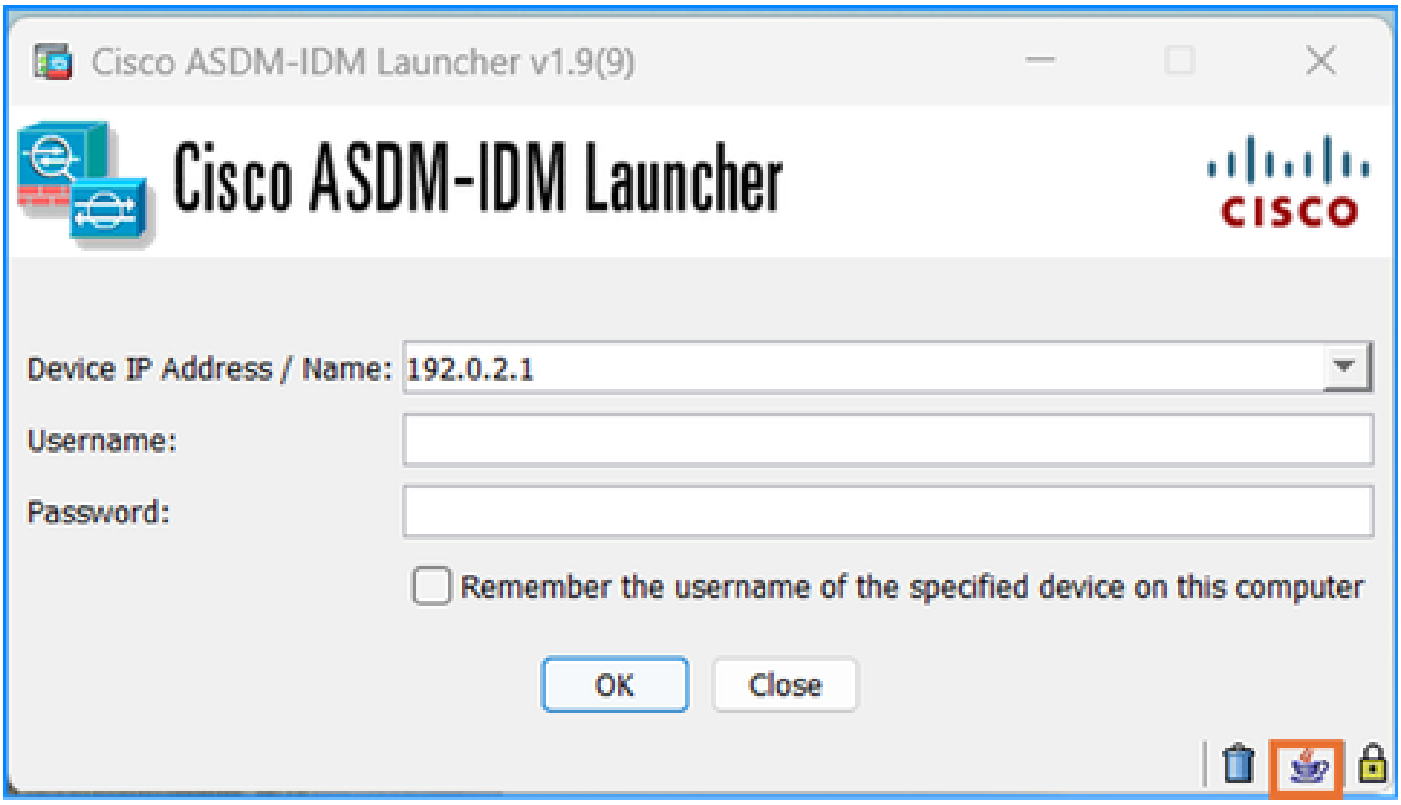
<#root>

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

```
java.lang.ArrayIndexOutOfBoundsException: 3
```

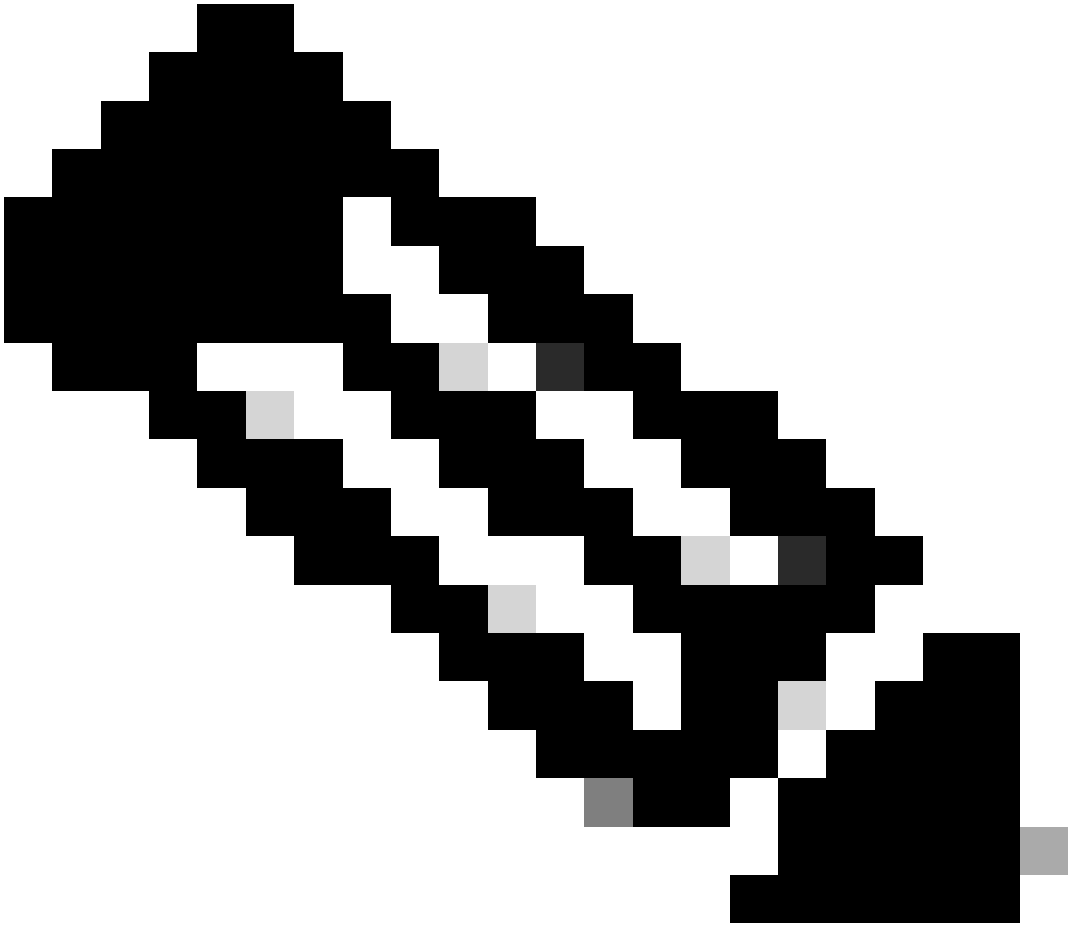
```
   at doz.a(doz.java:1256)
   at doz.a(doz.java:935)
   at doz.l(doz.java:1100)
```

Pour vérifier ce symptôme, activez les journaux de la console Java :



Dépannage - Actions recommandées

Référez-vous à l'ID de bogue Cisco CSCwi56155 du logiciel « Unable to access Secure Client Profile on ASDM ».



Remarque : Ce défaut a été corrigé dans les versions récentes du logiciel ASDM. Consultez les détails du défaut pour plus d'informations.

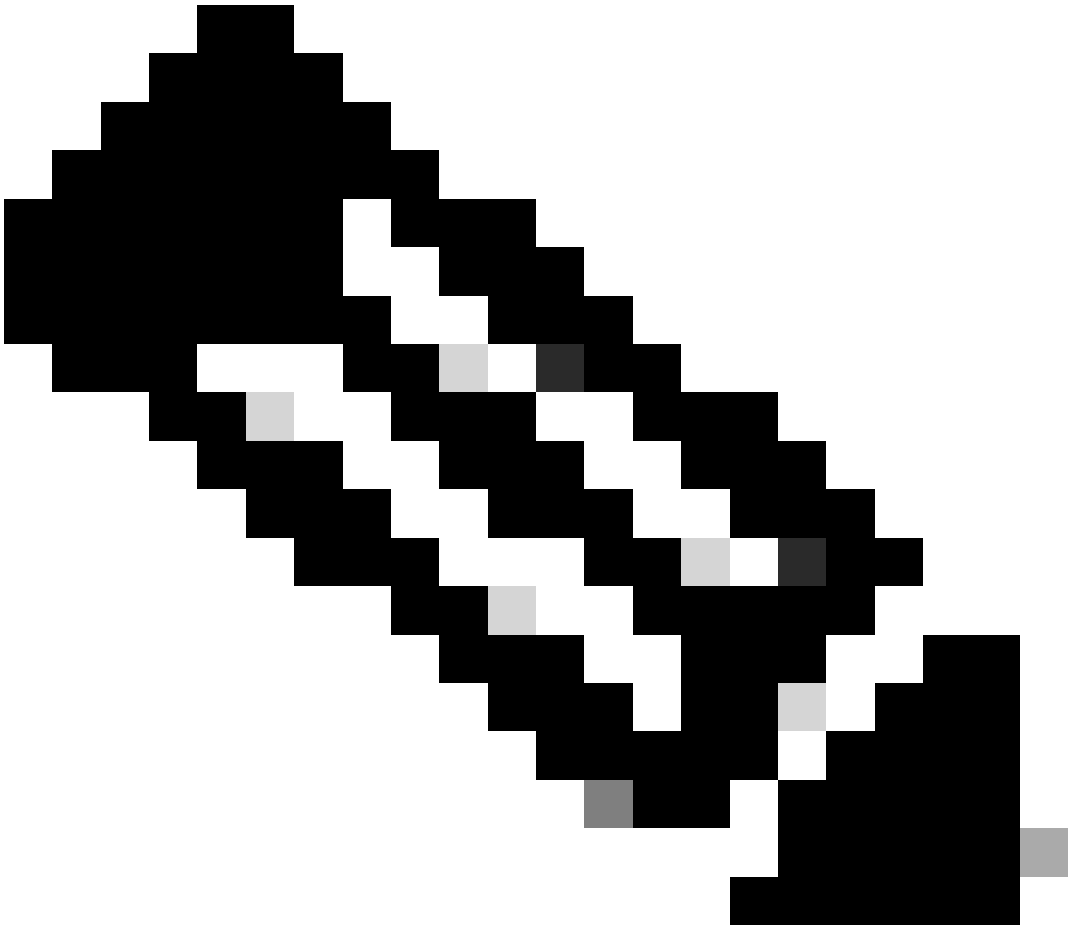
Problème 16. Impossible de modifier les profils XML du profil client sécurisé sur ASDM

Les profils XML Secure Client Profile dans Configuration ASDM > Remote Access VPN > Network (Client) Access ne peuvent pas être modifiés sur un périphérique ASA si une image AnyConnect présente sur le disque est antérieure à la version 4.8.

Le message d'erreur « There is no profile editor plugin in your Secure Client Image on the device. Accédez à Network (Client) Access > Secure Client Software et installez Secure Client Image version 2.5 ou ultérieure, puis réessayez. » s'affiche.

Dépannage - Actions recommandées

Référez-vous au bogue logiciel Cisco ID CSCwk64399 « ASDM- Unable to edit Secure Client Profile ». La solution de contournement consiste à définir une autre image AnyConnect avec une priorité inférieure.



Remarque : Ce défaut a été corrigé dans les versions récentes du logiciel ASDM. Consultez les détails du défaut pour plus d'informations.

Problème 17. Des images du client sécurisé sont manquantes après les modifications de configuration

Après avoir effectué des modifications dans Configuration ASDM > Network (Client) Access > Secure Client Profile, les images dans Configuration > Network (Client) Access > Secure Client Software sont manquantes.

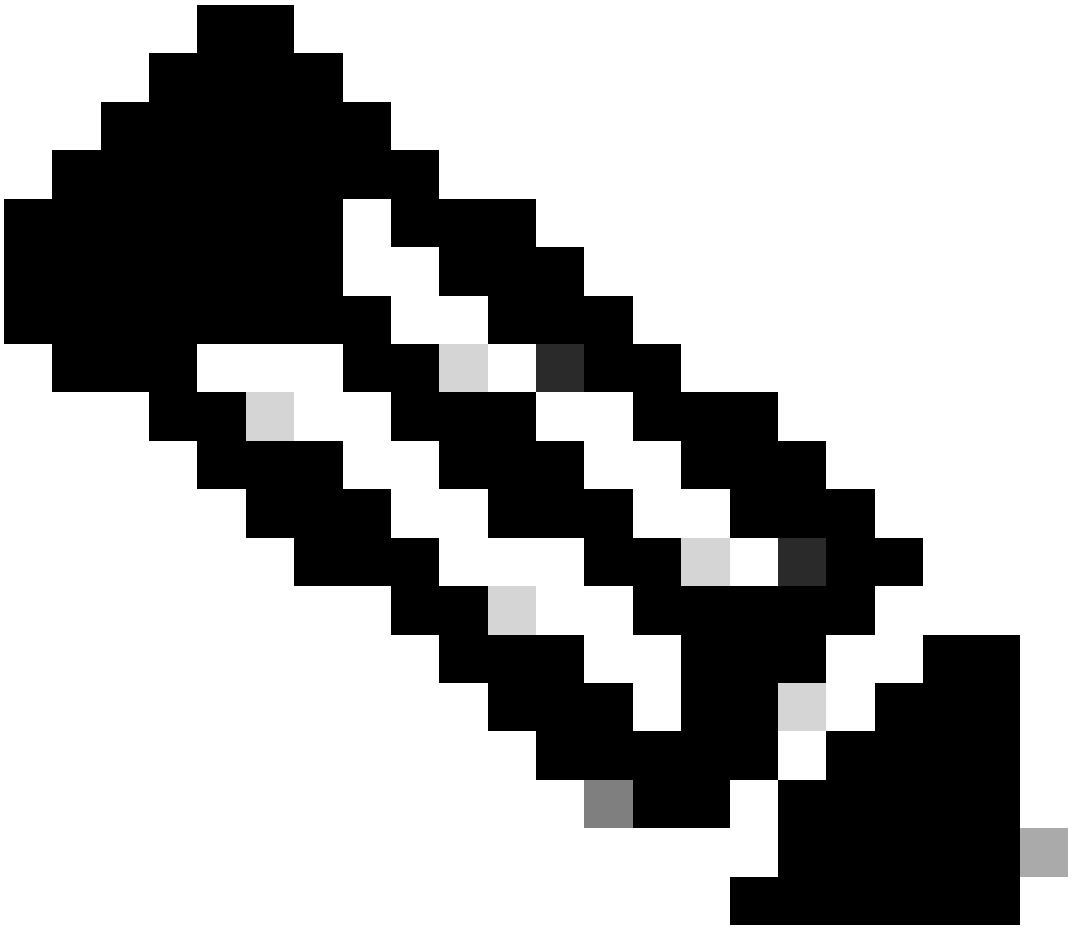
Dépannage - Actions recommandées

Référez-vous au bogue logiciel Cisco ID CSCwf23826 « Le logiciel client sécurisé ne s'affiche pas après la modification de l'Éditeur de profil client sécurisé dans ASDM ». Les options de contournement :

- Cliquez sur l'icône Actualiser dans ASDM

OU

- Fermer et rouvrir ASDM



Remarque : Ce défaut a été corrigé dans les versions récentes du logiciel ASDM. Consultez les détails du défaut pour plus d'informations.

Problème 18. Inefficacité des commandes http server session-timeout et http

server idle-timeout

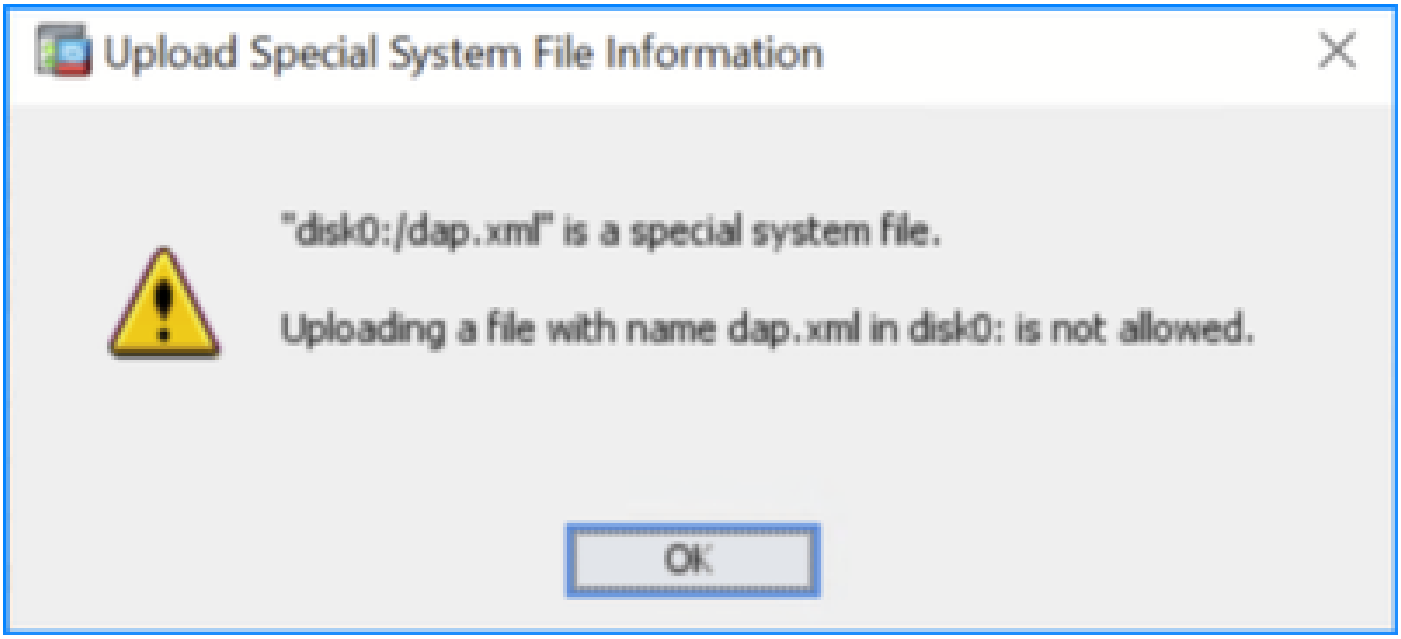
Les commandes http server session-timeout et http server idle-timeout n'ont aucun effet en mode multicontexte ASA.

Dépannage - Actions recommandées

Référez-vous au bogue logiciel Cisco ID CSCtx41707 « Support for http server timeout command in multi-context mode ». Les commandes sont configurables, mais les valeurs n'ont aucun effet.

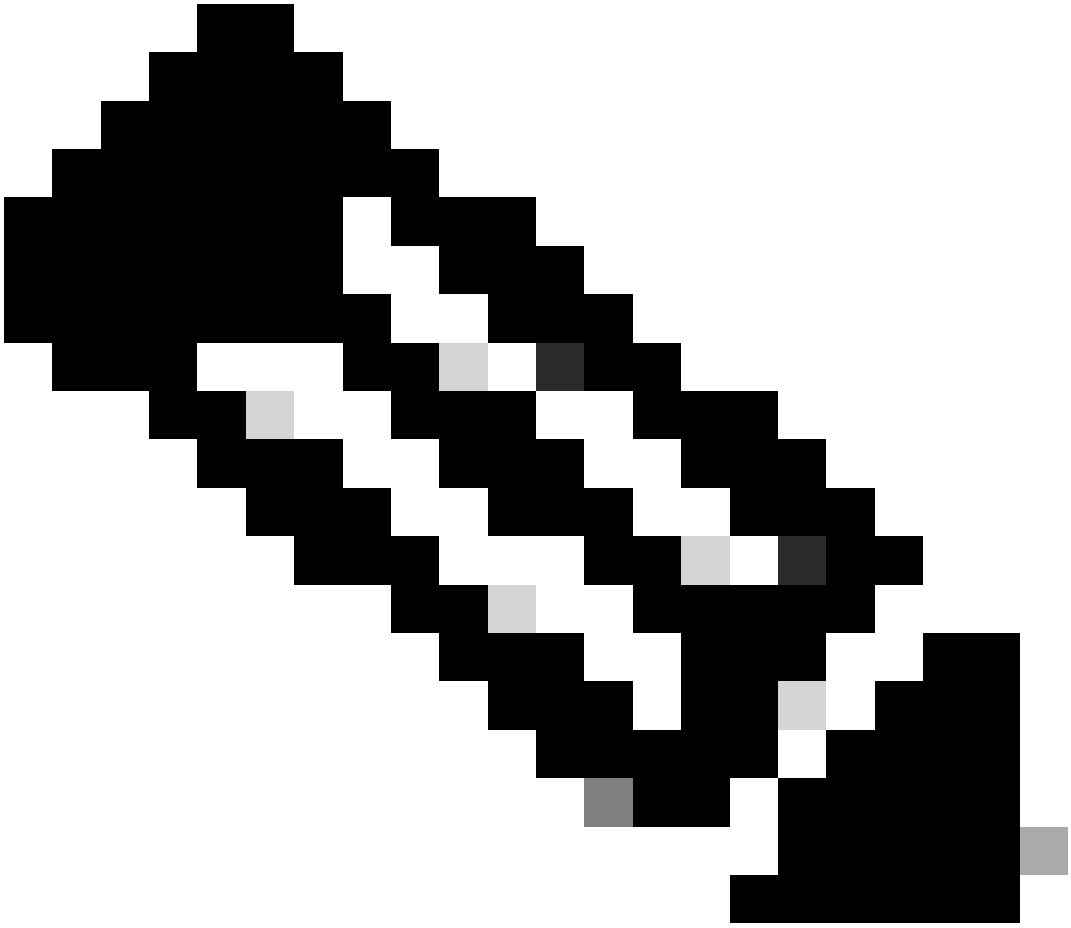
Problème 19. Échec de la copie Dap.xml sur ASDM

La copie du fichier dap.xml vers ASA via la fenêtre Gestion des fichiers dans ASDM échoue avec l'erreur « disk0:/dap.xml is a special system file. Téléchargement d'un fichier nommé dap.xml dans disk0 : n'est pas autorisé » :



Dépannage - Actions recommandées

Référez-vous au bogue logiciel Cisco ID CSCvt62162 « Cannot copy dap.xml using File Management in ASDM 7.13.1 ». La solution de contournement consiste à copier le fichier directement sur l'ASA en utilisant des protocoles comme FTP ou TFTP.



Remarque : Ce défaut a été corrigé dans les versions récentes du logiciel ASDM. Consultez les détails du défaut pour plus d'informations.

Problème 20. Aucune stratégie IKE ni aucune proposition IPSEC visible sur l’ASDM

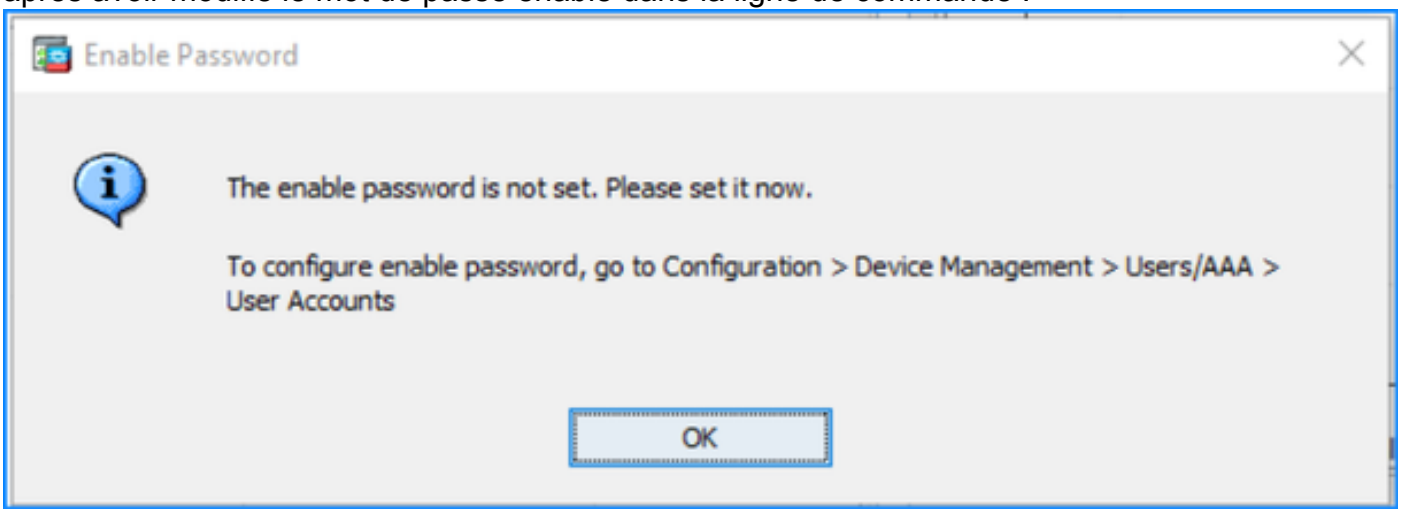
L'ASDM n'affiche pas les stratégies IKE et les propositions IPSEC dans la fenêtre Configurations > Site-to-Site VPN.

Dépannage - Actions recommandées

Reportez-vous à l'ID de bogue Cisco CSCwm42701 du logiciel « ASDM display blank in IKE policies and IPSEC propositions tab ».

Problème 21. ASDM affiche le message « The enable password is not set. Veuillez le définir maintenant. »

ASDM affiche le message « Le mot de passe actif n'est pas défini. Veuillez le définir maintenant. » après avoir modifié le mot de passe enable dans la ligne de commande :



Dépannage - Actions recommandées

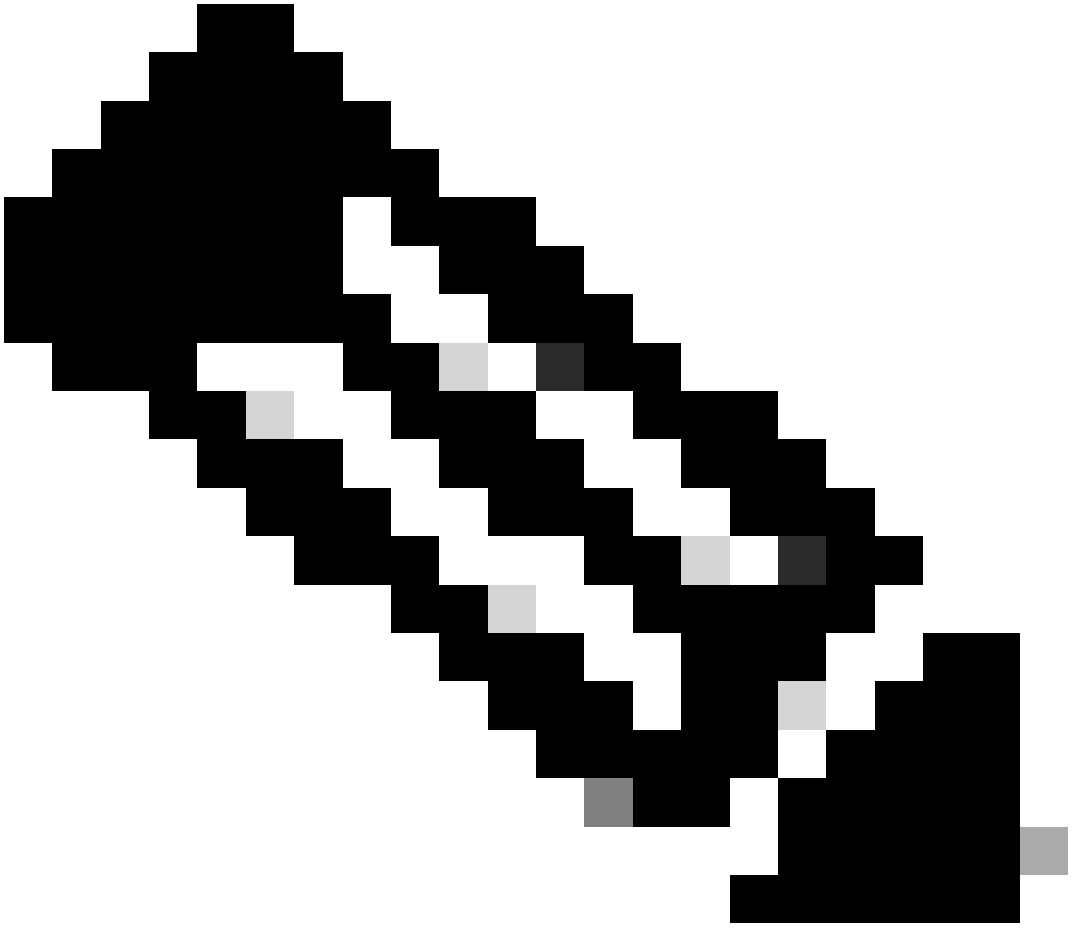
Référez-vous au bogue logiciel Cisco ID CSCvq42317 « ASDM invite to change enable password after it was set on CLI ».

Problème 22. L'objet ASDN disparaît après actualisation de l'interface ASDM

Lors de l'ajout d'un groupe d'objets et d'un hôte d'objets à un groupe d'objets existant et après l'actualisation de l'ASDM, le groupe d'objets disparaît de la liste ASDM. Les noms d'objet doivent commencer par des numéros pour que ce défaut corresponde.

Dépannage - Actions recommandées

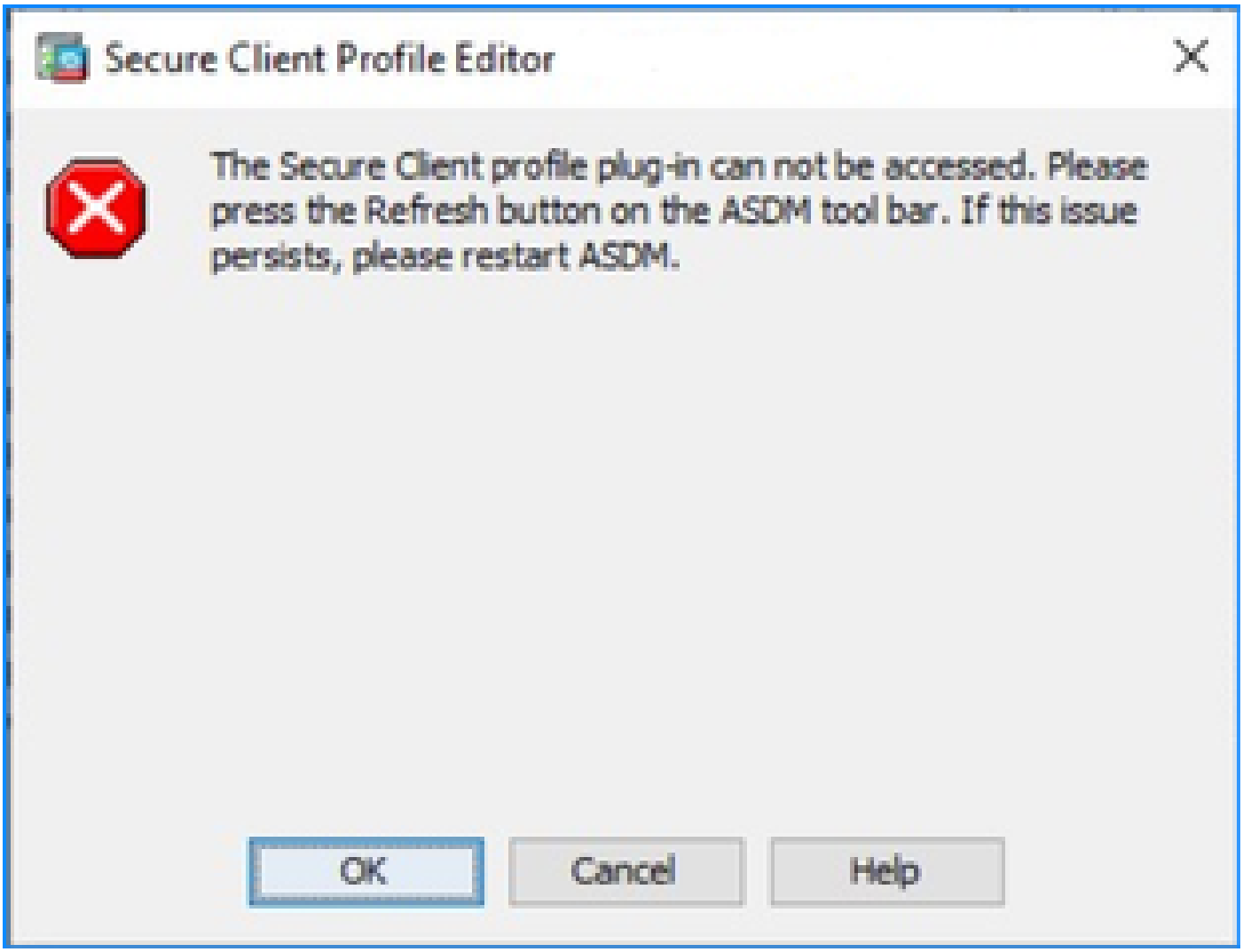
Référez-vous au bogue logiciel Cisco ID CSCwf71723 « ASDM loss configured objects/object groups ».



Remarque : Ce défaut a été corrigé dans les versions récentes du logiciel ASDM. Consultez les détails du défaut pour plus d'informations.

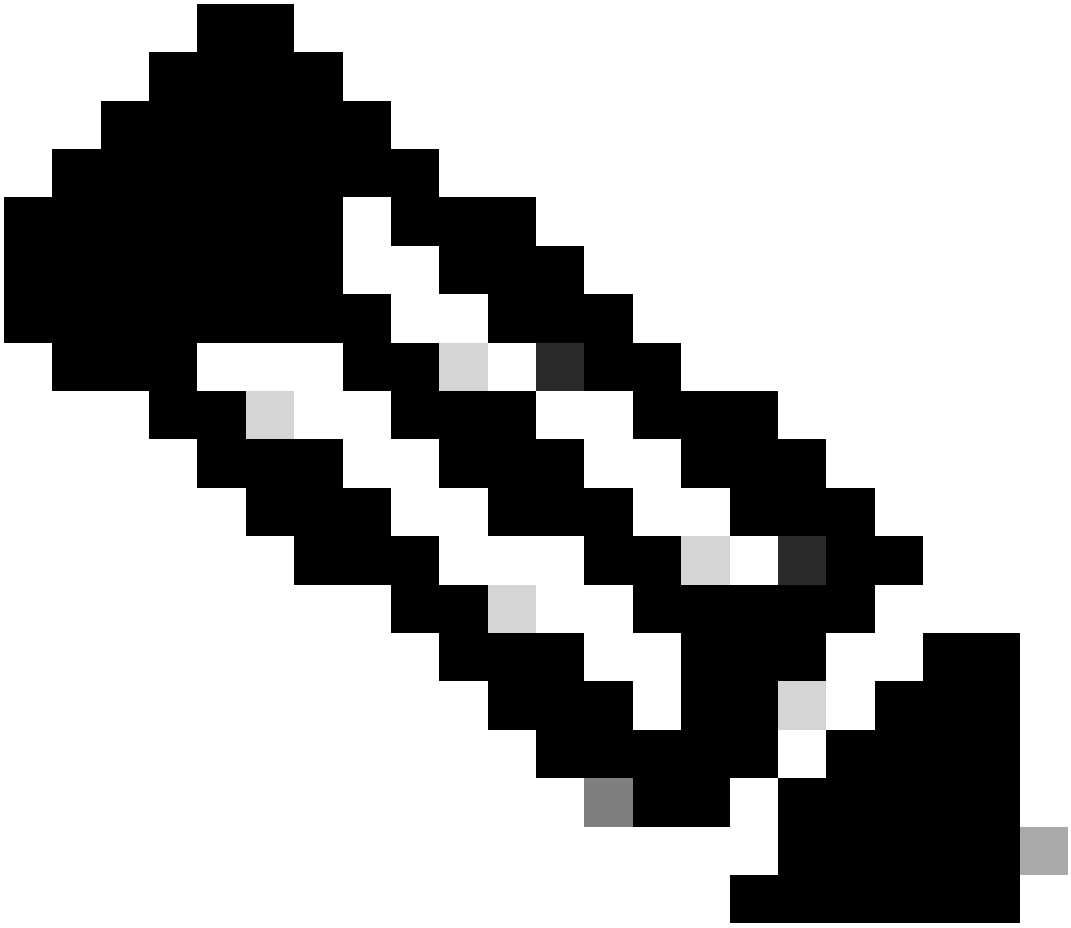
Problème 23. Impossible de modifier les profils client AnyConnect pour les versions antérieures à 4.5

Les profils clients AnyConnect ne peuvent pas être modifiés pour les profils AnyConnect antérieurs à la version 4.5. Le message d'erreur est « Le plug-in de profil client sécurisé est inaccessible. Appuyez sur le bouton Actualiser de la barre d'outils ASDM. Si ce problème persiste, redémarrez l'application ASDM. » :



Dépannage - Actions recommandées

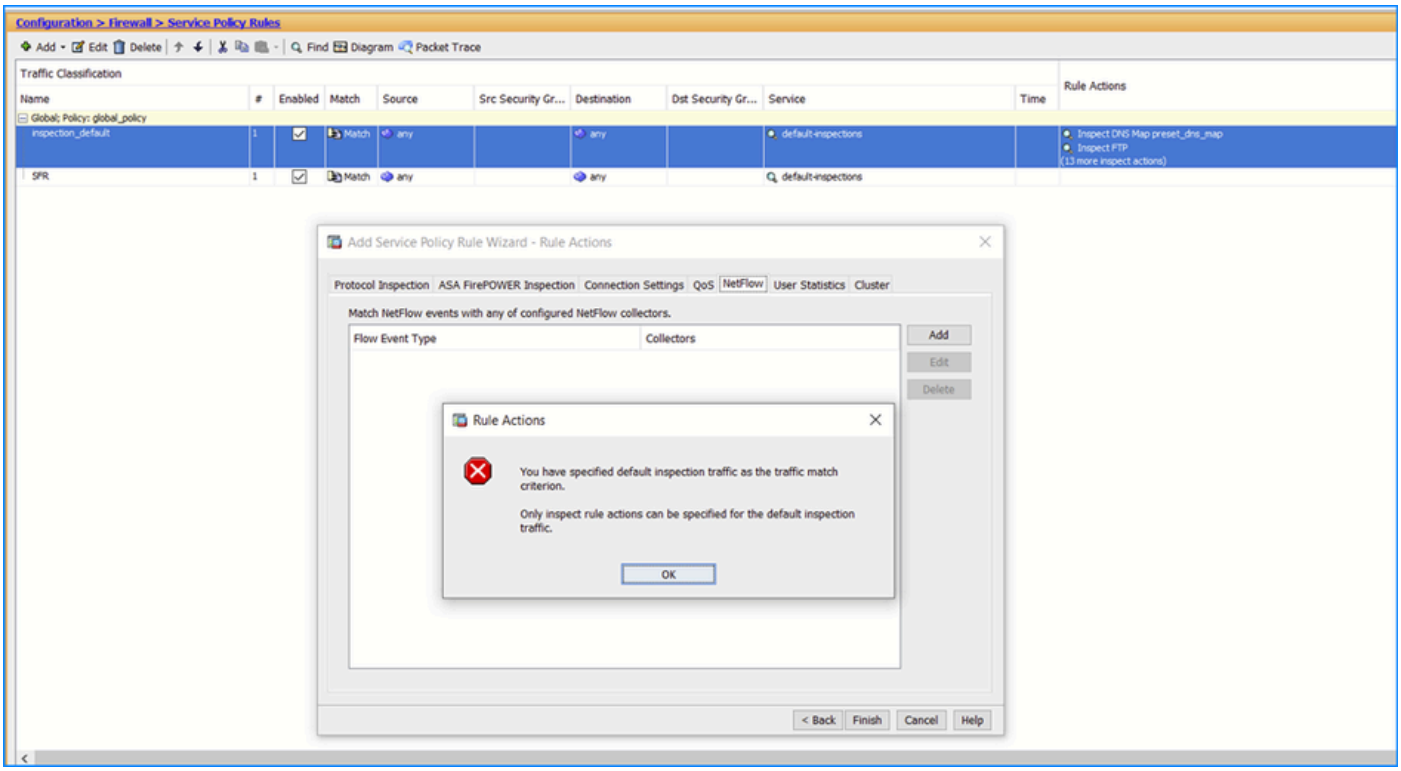
Référez-vous au bogue logiciel Cisco ID CSCwf16947 « ASDM - Unable to load Anyconnect Profile Editor ».



Remarque : Ce défaut a été corrigé dans les versions récentes du logiciel ASDM. Consultez les détails du défaut pour plus d'informations.

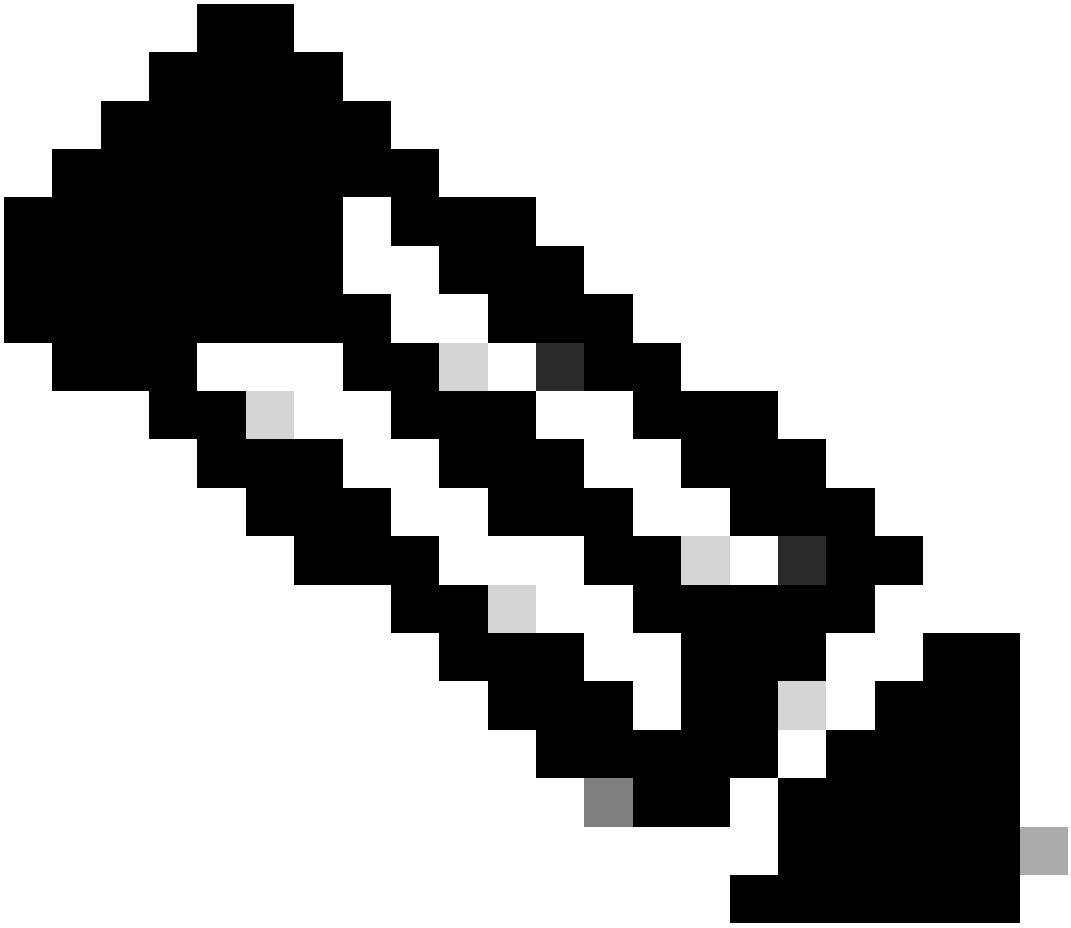
Problème 24. Impossible d'accéder à l'onglet Edit Service Policy > Rule Actions > ASA FirePOWER Inspection

Dans la version 7.8.2 d'ASDM, les utilisateurs ne peuvent pas accéder à l'onglet Edit Service Policy > Rule Actions > ASA FirePOWER Inspection et l'erreur s'affiche : "Vous avez spécifié le trafic d'inspection par défaut comme critère de correspondance du trafic. Seules les actions de règle d'inspection peuvent être spécifiées pour le trafic d'inspection par défaut." Cela se produit même lorsqu'une liste de contrôle d'accès a été sélectionnée pour la redirection :



Dépannage - Actions recommandées

Référez-vous au bogue logiciel Cisco ID CSCvg15782 « ASDM - Unable to view modify SFR traffic redirection after upgrade to version 7.8(2) ». La solution de contournement consiste à utiliser l'interface de ligne de commande pour modifier la configuration policy-map.



Remarque : Ce défaut a été corrigé dans les versions récentes du logiciel ASDM. Consultez les détails du défaut pour plus d'informations.

Problème 25. Image AnyConnect version 5.1 et éditeur de profil AnyConnect sur ASDM

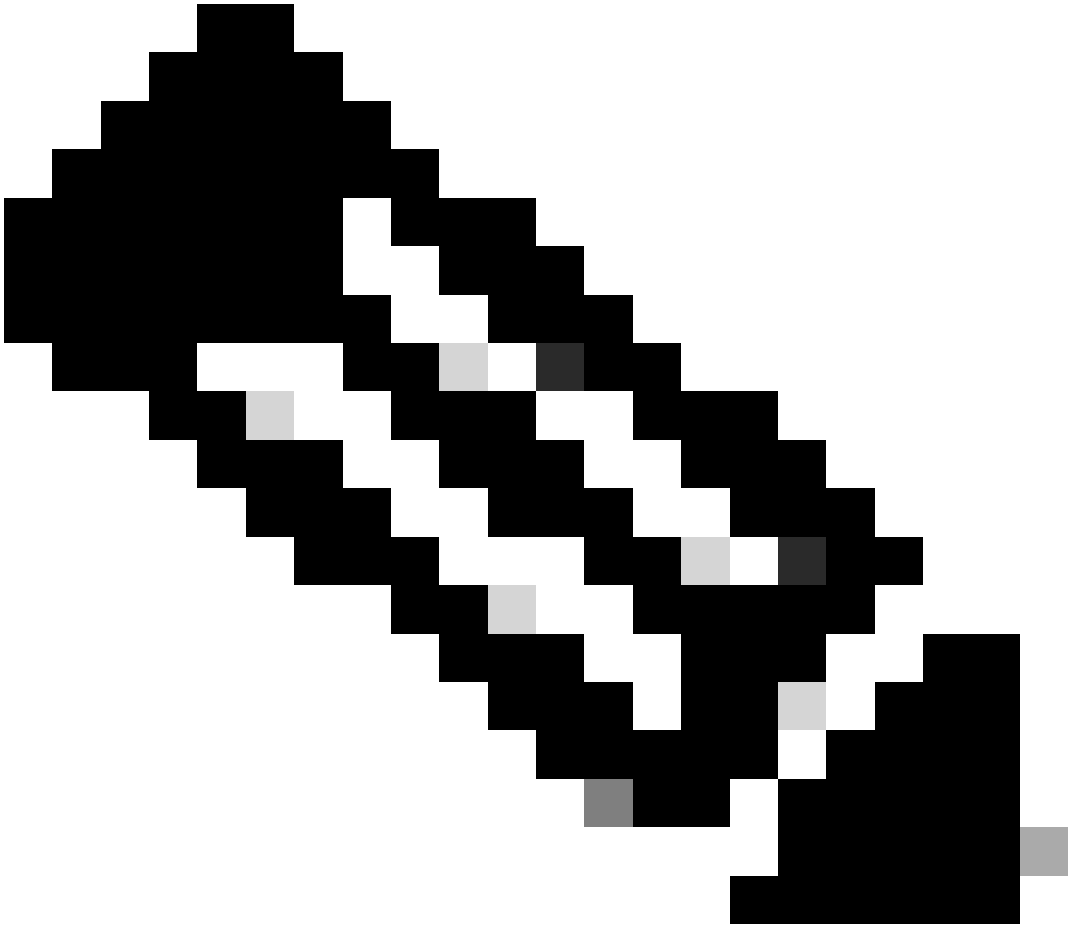
Les symptômes suivants sont observés pour la version 5.1 du logiciel Secure Client :

1. Les noms des modules de stratégie de groupe ne sont pas répertoriés lors du chargement des packages Win/Mac/Linux
2. L'ASDM ne parvient pas à ouvrir AnyConnect Profile Editor.

Dépannage - Actions recommandées

Référez-vous au bogue logiciel Cisco ID CSCwh7417 « ASDM : Impossible de charger

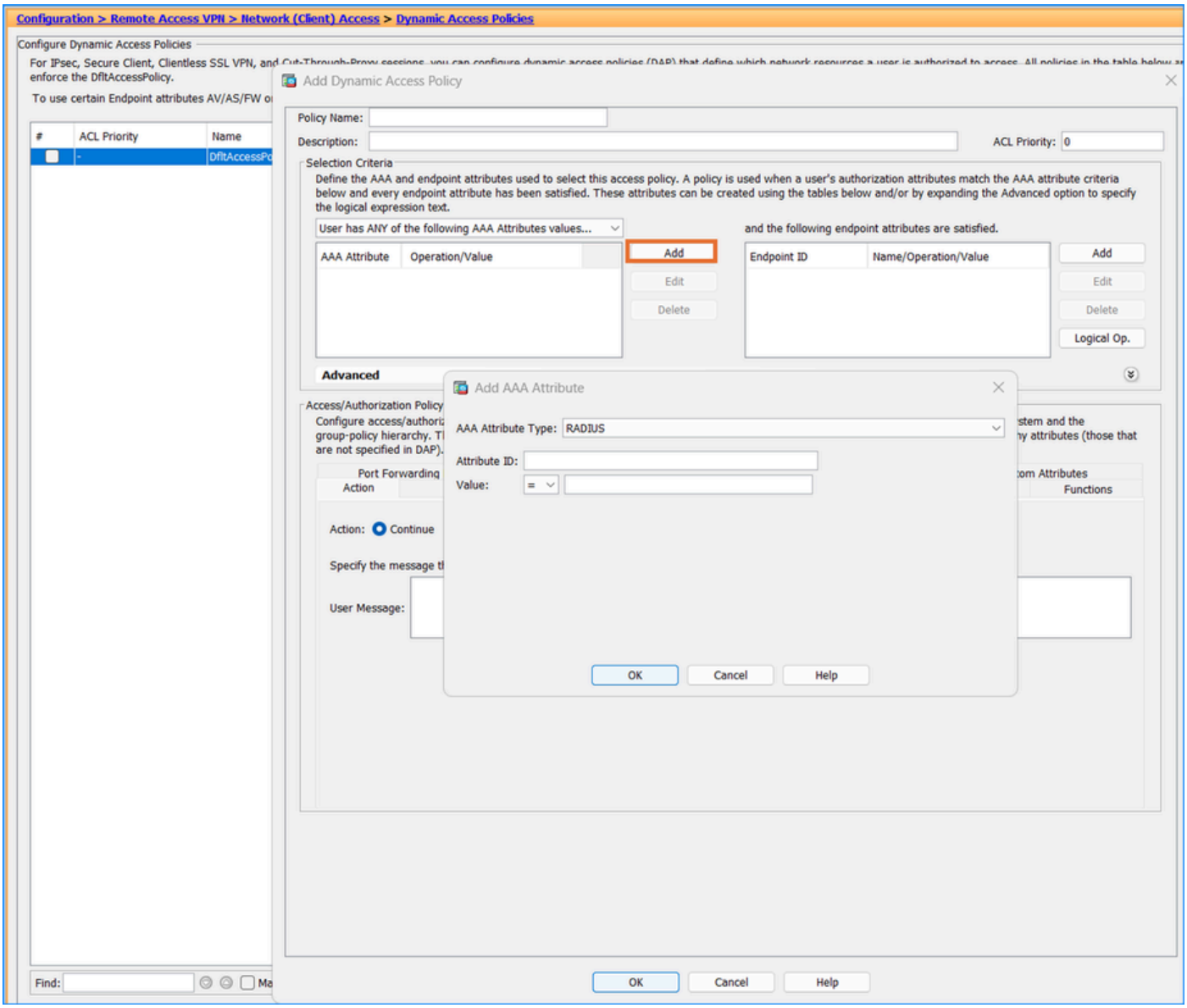
AnyConnect Profile Editor et la stratégie de groupe lors de l’utilisation de l’image CSC 5.1 ». La solution de contournement consiste à utiliser des versions inférieures du client sécurisé.



Remarque : Ce défaut a été corrigé dans les versions récentes du logiciel ASDM. Consultez les détails du défaut pour plus d'informations.

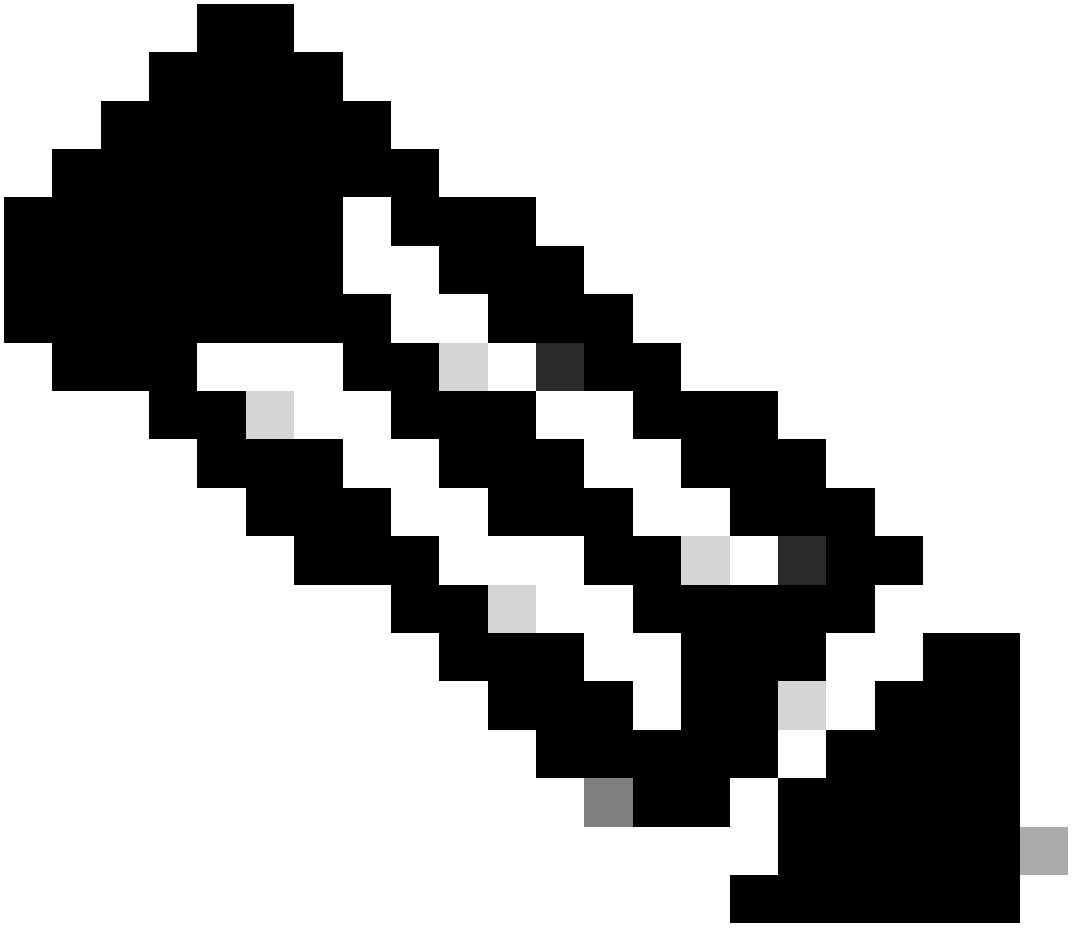
Problème 26. Le type d'attribut AAA (Radius/LDAP) n'est pas visible dans ASDM

Les attributs de type AAA (Radius/LDAP) ne sont pas visibles dans ASDM > Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Add > On AAA attribute field > Add > Select Radius or LDAP:



Dépannage - Actions recommandées

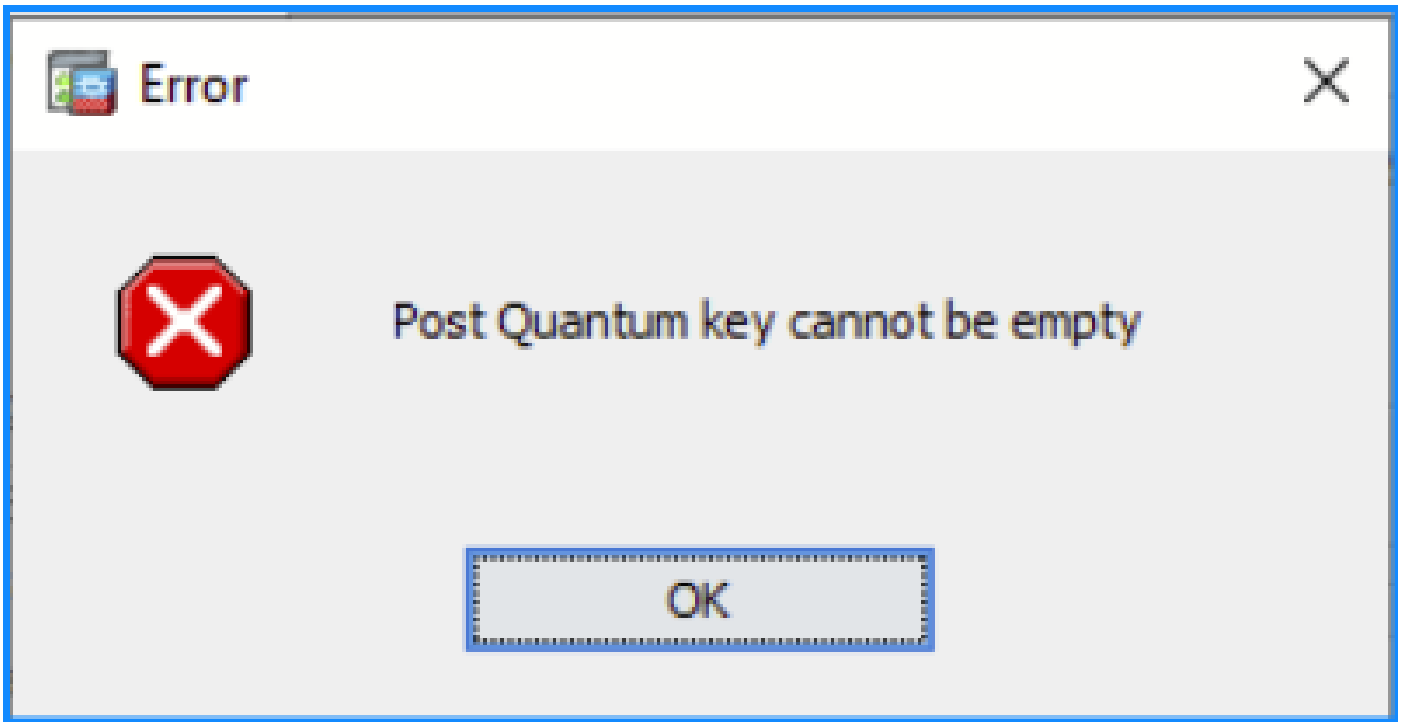
Référez-vous au bogue logiciel Cisco ID CSCwa9370 « ASDM : ASDM : DAP config missing AAA Attributes type (Radius/LDAP) » et ID de bogue Cisco CSCwd16386 « ASDM : DAP config missing AAA Attributes type (Radius/LDAP) ».



Remarque : Ces défauts ont été corrigés dans les versions récentes du logiciel ASDM. Consultez les détails du défaut pour plus d'informations.

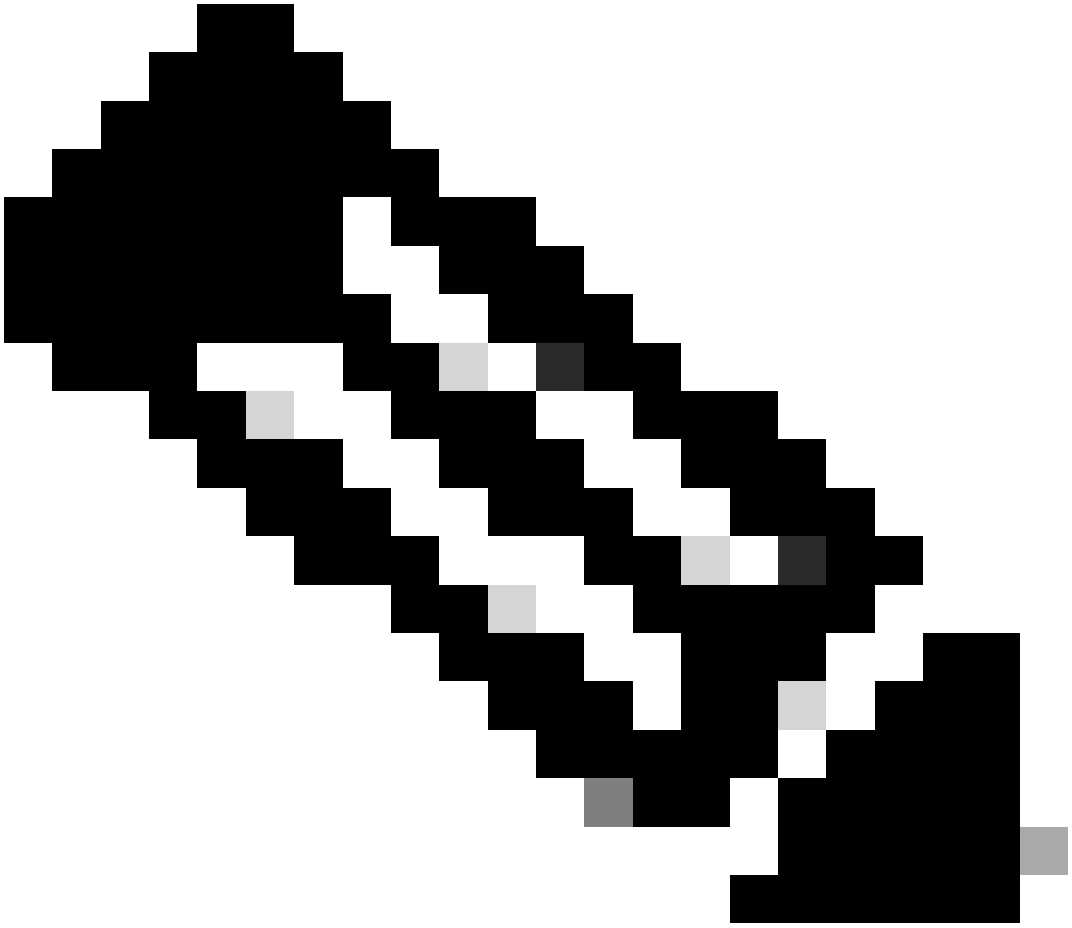
Problème 27. L'erreur « La clé post-quantique ne peut pas être vide » s'affiche sur l'ASDM

L'erreur « La clé Post Quantum ne peut pas être vide » est affichée lors de la modification de la section Avancé dans ASDM > Configuration > Remote Access VPN > Network (Client) Access > IPsec (IKEv2) Connection Profiles :



Dépannage - Actions recommandées

Référez-vous au message d'erreur « Configuration ASDM IKev2 - Post Quantum Key cannot be empty » de l'ID de bogue logiciel Cisco CSCwe58266.



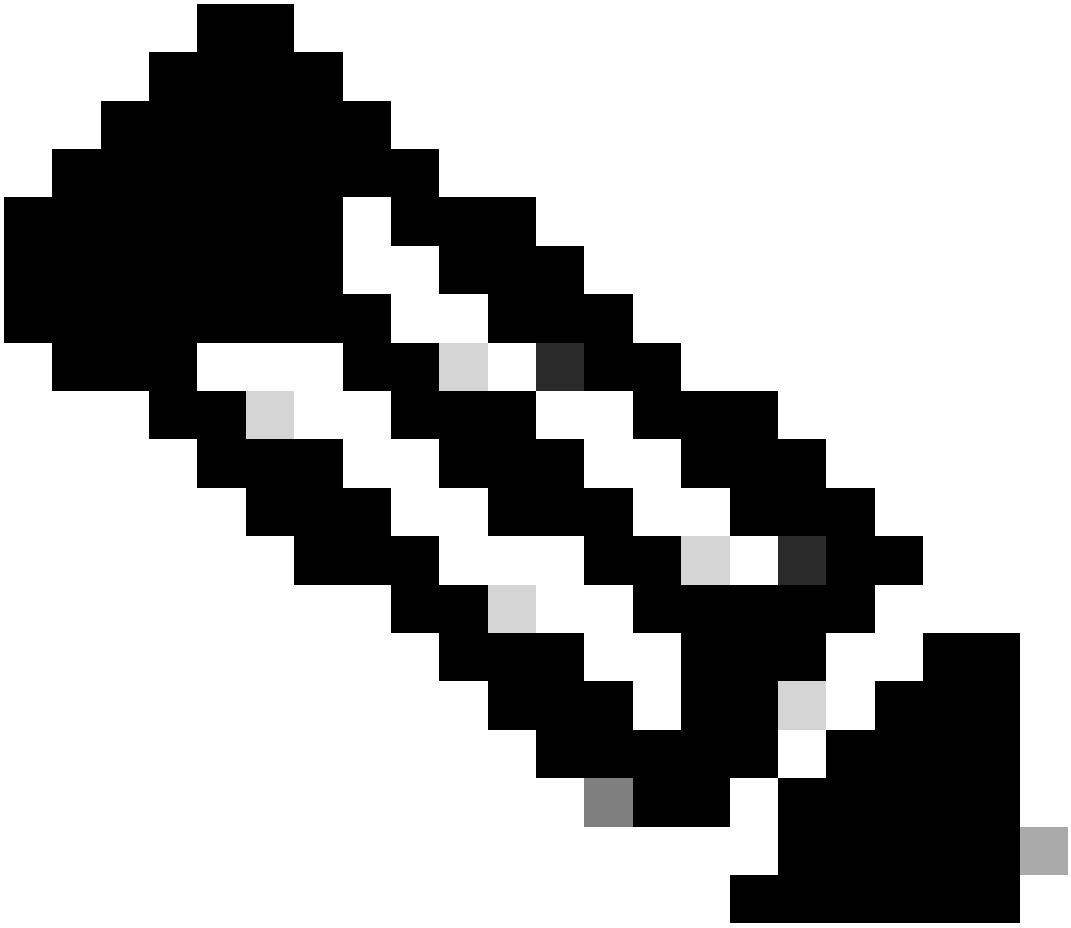
Remarque : Ce défaut a été corrigé dans les versions récentes du logiciel ASDM. Consultez les détails du défaut pour plus d'informations.

Problème 28. ASDM n'affiche aucun résultat lors de l'utilisation de l'option "où utilisé"

L'application ASDM n'affiche aucun résultat lorsque vous utilisez l'option « Utilisation » disponible en sélectionnant Configuration > Pare-feu > Objets > Objets/groupes réseau et en cliquant avec le bouton droit sur un objet.

Dépannage - Actions recommandées

Référez-vous à l'option « Where used » du bogue logiciel Cisco ID CSCwd98702 dans ASDM not working ».



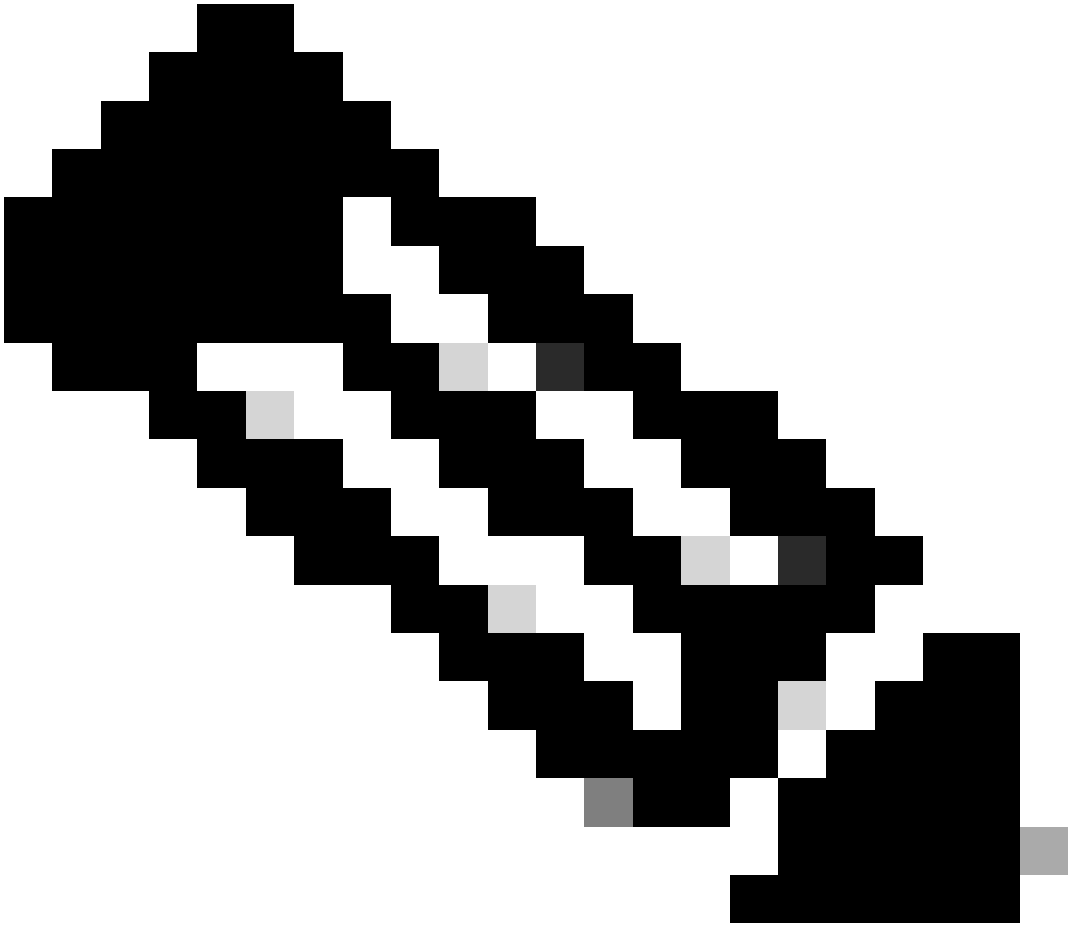
Remarque : Ce défaut a été corrigé dans les versions récentes du logiciel ASDM. Consultez les détails du défaut pour plus d'informations.

Problème 29. Message d'avertissement « [L'objet réseau] ne peut pas être supprimé car il est utilisé dans les éléments suivants » lors de la suppression d'un objet réseau

ASDM n'affiche pas le message d'avertissement « [L'objet réseau] ne peut pas être supprimé car il est utilisé dans les éléments suivants » lors de la suppression d'un objet réseau qui est référencé dans un groupe réseau dans Configuration > Pare-feu > Objets > Network Objects/Groups.

Dépannage - Actions recommandées

Référez-vous au bogue logiciel Cisco ID CSCwe67056 "[Objet réseau] ne peut pas être supprimé car il est utilisé dans le suivant" avertissement ne s'affiche pas".



Remarque : Ce défaut a été corrigé dans les versions récentes du logiciel ASDM. Consultez les détails du défaut pour plus d'informations.

Problème 30. Problèmes d'utilisation avec l'onglet Network Objects/Group dans ASDM

Un ou plusieurs de ces symptômes sont observés :

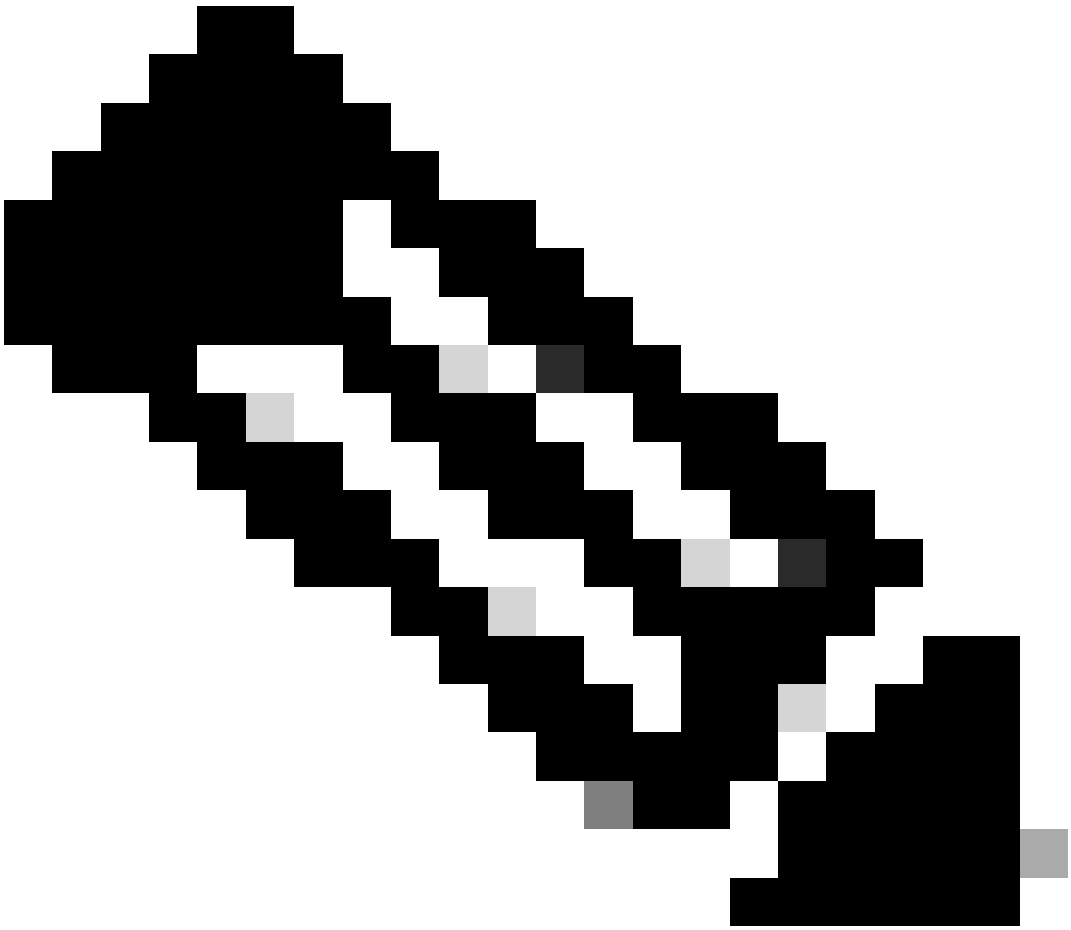
- La saisie de texte « Nom » dans la section « Créer un nouveau membre d'objet » de la fenêtre « Ajouter/Modifier un groupe d'objets » est marquée comme « facultative ». Cependant, le bouton "Ajouter**>>**" pour créer et ajouter l'objet est désactivé sauf si un nom est entré.
- L'onglet « Utilisations » qui s'ouvre lorsqu'un utilisateur clique sur « Cas d'emploi... » Le menu contextuel répertorie uniquement les entités (ACL, route-maps, object-groups) qui référencent directement l'objet. Il doit également répertorier récursivement les deuxième, troisième, etc. les références d'ordre (c'est-à-dire une liste de contrôle d'accès qui utilise un

groupe d'objets contenant un objet doivent également être répertoriées comme « utilisation » de l'objet).
- L'opération "Supprimer" disponible dans le menu contextuel affiche également ce comportement. Il supprime automatiquement toute entité qui fait directement référence à l'objet (si l'entité devient vide lorsque l'objet est supprimé). Il ne fonctionne pas de cette façon quand un deuxième, troisième, et ainsi de suite. la référence de commande deviendrait vide en raison de la suppression de l'objet et de la première référence de commande.

L'utilisateur peut être amené à penser que l'ASDM empêche les entités qui deviendraient vides en raison de la suppression de l'objet dans la configuration restante. Ce n'est cependant pas nécessairement le cas.

Dépannage - Actions recommandées

Référez-vous à l'ID de bogue Cisco CSCwe86257 du logiciel « Utilisabilité des objets réseau/onglet Groupe dans ASDM ».

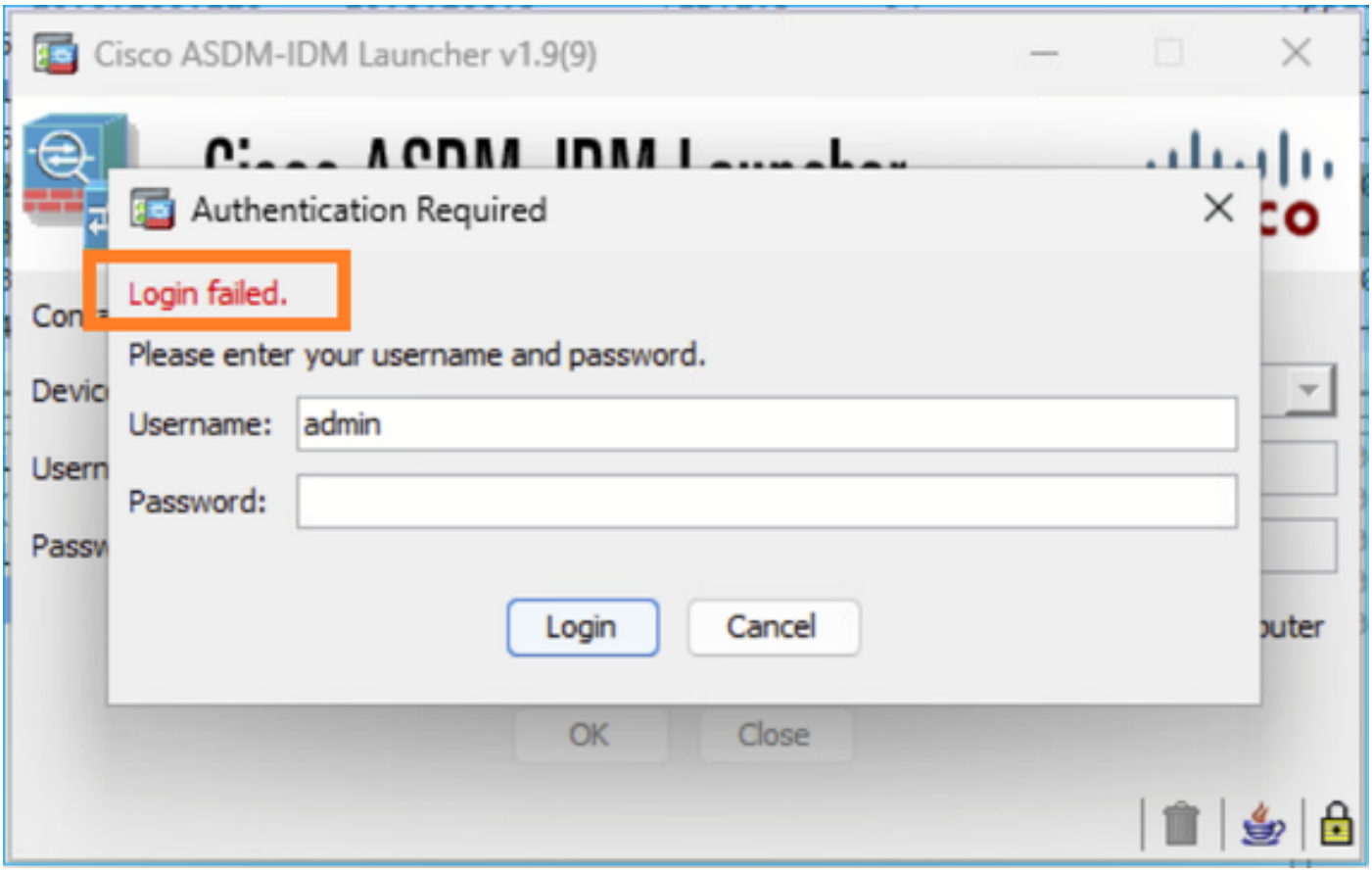


Remarque : Ce défaut a été corrigé dans les versions récentes du logiciel ASDM. Consultez les détails du défaut pour plus d'informations.

Dépannage des problèmes d'authentification ASDM

Problème 1. Échec de la connexion ASDM

L'erreur affichée sur l'interface utilisateur ASDM est :



Dépannage - Actions recommandées

Cette erreur est visible lorsque HTTP et Webvpn Cisco Secure Client (AnyConnect) sont tous deux activés sur la même interface. Par conséquent, toutes les conditions doivent être remplies :

1. AnyConnect/Cisco Secure Client est activé sur une interface
2. Le serveur HTTP est activé sur la même interface et le même port que AnyConnect/Cisco Secure Client

Exemple :

<#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
```

Conseil de dépannage : Activez « debug http 255 » et vous pouvez voir le conflit entre ASDM et 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
```

En guise de note complémentaire, malgré l'échec de connexion, les syslogs ASA montrent que l'authentification est réussie :

<#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

Solution De Contournement

Solution 1

Modifiez le port TCP pour le serveur HTTP ASA, par exemple :

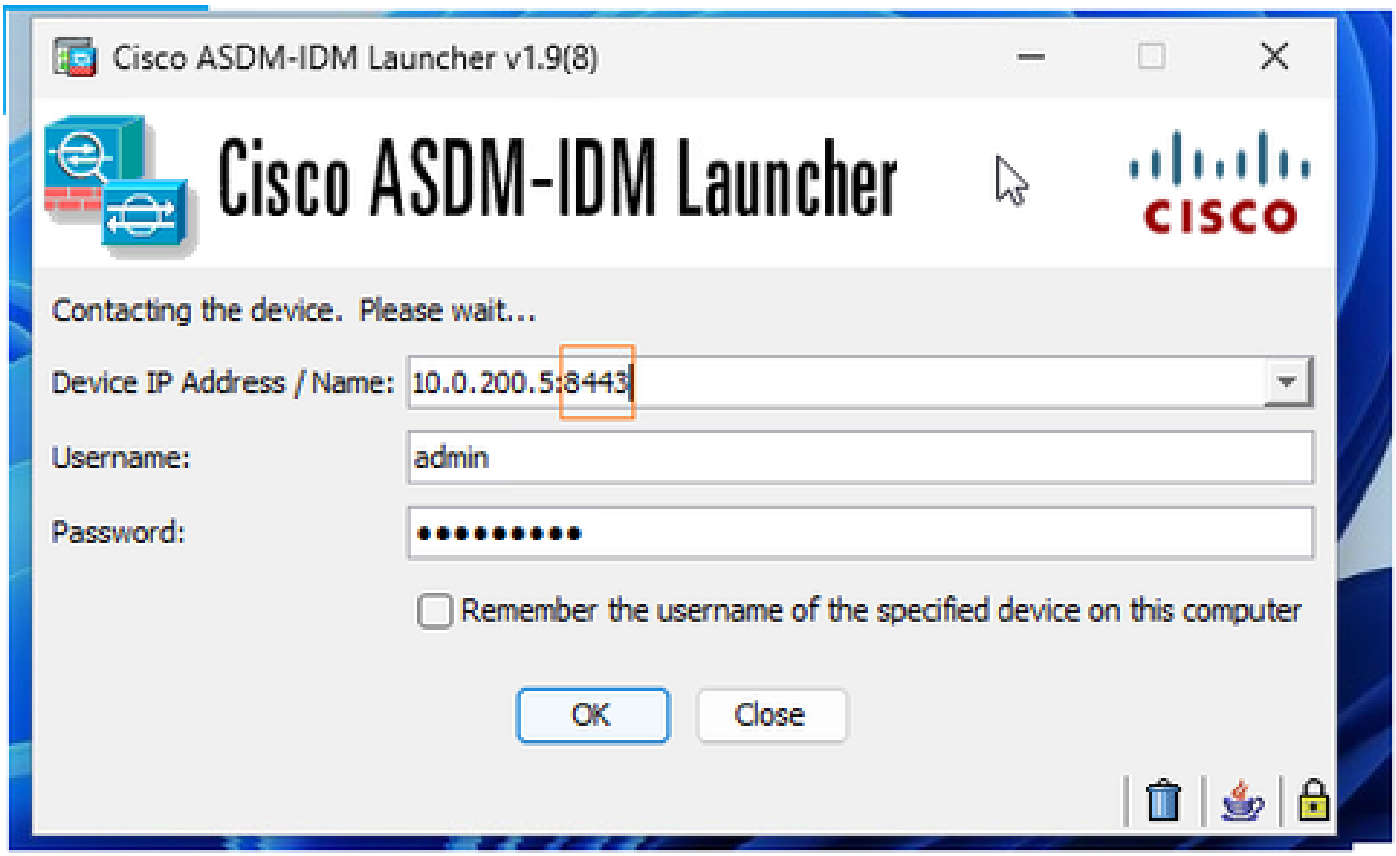
<#root>

ciscoasa#

configure terminal

ciscoasa(config)#

http server enable 8443



Solution 2

Modifiez le port TCP du client sécurisé AnyConnect/Cisco, par exemple :

<#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
```

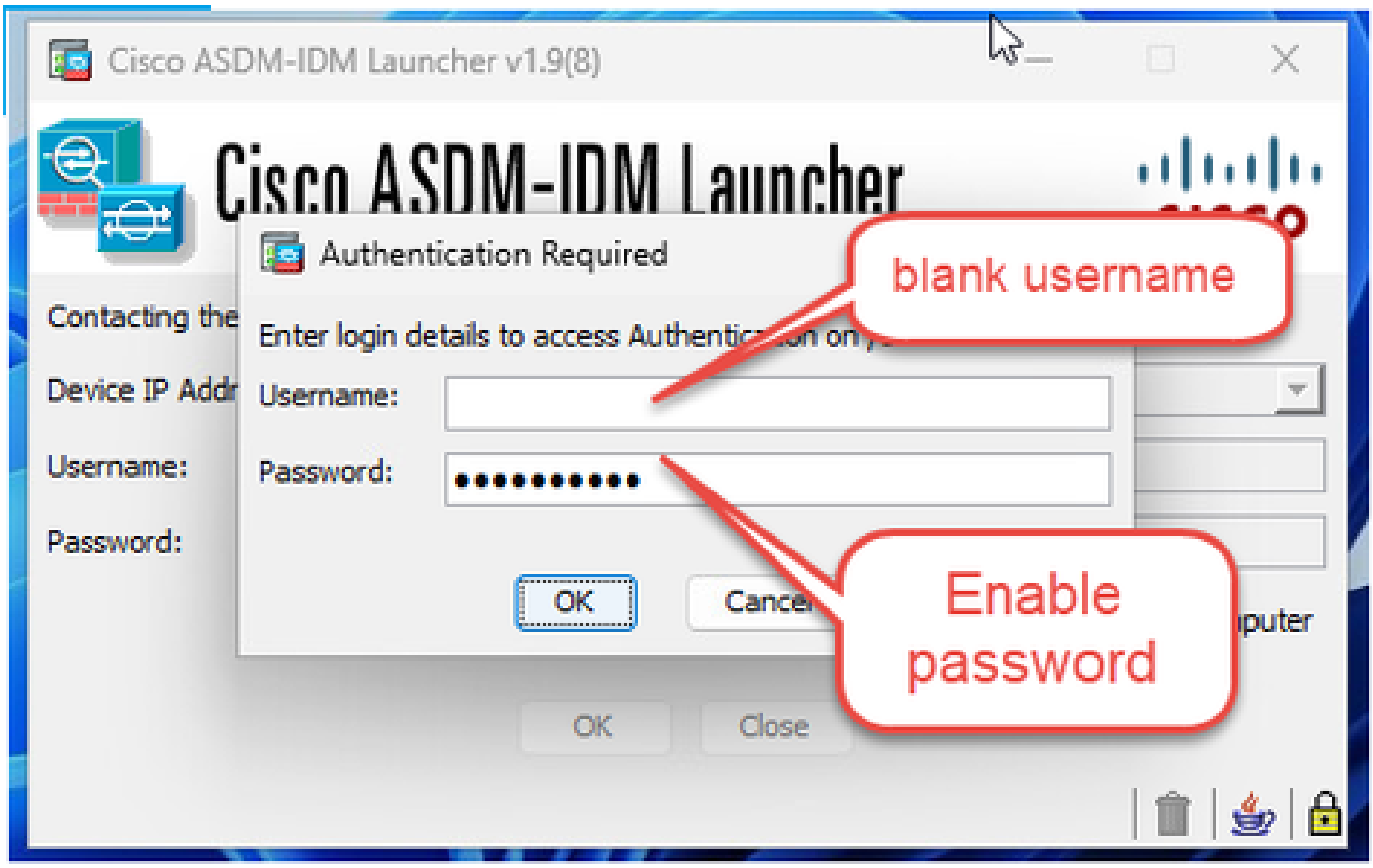
Solution 3

Une solution alternative consiste à supprimer la configuration « aaa authentication http console » :

<#root>

```
ciscoasa(config)#
no aaa authentication http console LOCAL
```

Dans ce cas, vous pouvez vous connecter à ASDM en utilisant simplement le mot de passe enable :



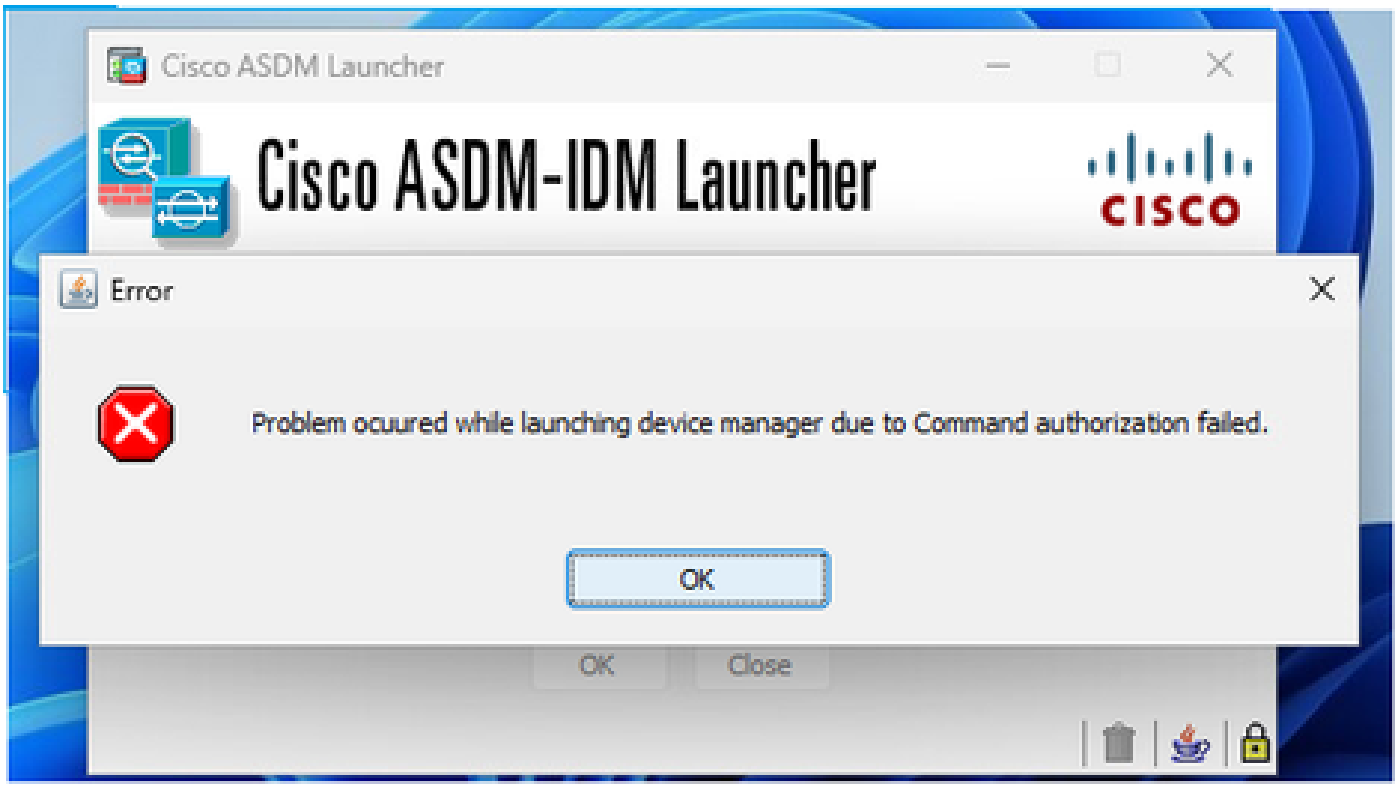
Défaut Connexe

ID de bogue Cisco CSCwb67583

Ajouter un avertissement lorsque webvpn et ASDM sont activés sur la même interface

Problème 2. Échec de l'autorisation de la commande ASDM

L'erreur affichée sur l'interface utilisateur ASDM est :



Dépannage - Étapes recommandées

Vérifiez votre configuration AAA sur ASA et assurez-vous que :

- Vous avez également configuré une authentification.
- Si vous utilisez un serveur d'authentification distant, il est accessible et autorise les commandes.

Référence

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

Problème 3. Configuration de l’accès en lecture seule ASDM

Parfois, vous souhaitez fournir un accès en lecture seule aux utilisateurs ASDM.

Dépannage - Étapes recommandées

Créez un nouvel utilisateur avec un niveau de privilège personnalisé (5), par exemple :

<#root>

```
asa(config)#
```

username [username] password [password] privilege 5

Cette commande crée un utilisateur avec un niveau de privilège de 5, qui est le niveau de « surveillance uniquement ». Remplacez `[username]` et `[password]` par le nom d'utilisateur et le mot de passe souhaités.

Détails

L'autorisation de commande locale vous permet d'attribuer des commandes à l'un des 16 niveaux de privilège (0 à 15). Par défaut, chaque commande est affectée au niveau de privilège 0 ou 15. Vous pouvez définir chaque utilisateur à un niveau de privilège spécifique et chaque utilisateur peut entrer n'importe quelle commande au niveau de privilège affecté ou à un niveau inférieur. ASA prend en charge les niveaux de privilège utilisateur définis dans la base de données locale, un serveur RADIUS ou un serveur LDAP (si vous mappez des attributs LDAP à des attributs RADIUS).

Procédure

Étape 1	Choisissez Configuration > Device Management > Users/AAA > AAA Access > Authorization.
Étape 2	Cochez la case Enable authorization for ASA command access > Enable.
Étape 3	Sélectionnez LOCAL dans la liste déroulante Groupe de serveurs.
Étape 4	Lorsque vous activez l'autorisation de commande locale, vous pouvez attribuer manuellement des niveaux de privilège à des commandes individuelles ou à des groupes de commandes ou activer les privilèges de compte d'utilisateur prédéfinis. · Cliquez sur Set ASDM Defined User Roles pour utiliser des privilèges de compte utilisateur prédéfinis. La boîte de dialogue Configuration des rôles utilisateur définis par ASDM apparaît. Cliquez sur Yes pour utiliser les privilèges de compte d'utilisateur prédéfinis : Admin (niveau de privilège 15, avec accès complet à toutes les commandes CLI ; Lecture seule (niveau de privilège 5, avec accès en lecture seule) ; et Surveillance uniquement (niveau de privilège 3, avec accès à la section Surveillance uniquement). · Cliquez sur Configurer les privilèges de commande pour configurer manuellement les niveaux de commande. La boîte de dialogue Configuration des privilèges de commande apparaît. Vous pouvez afficher toutes les commandes en sélectionnant Tous les modes dans la liste déroulante Mode de commande, ou vous pouvez choisir un mode de configuration pour afficher les commandes disponibles dans ce mode. Par exemple, si vous choisissez contexte, vous pouvez afficher toutes les commandes disponibles en mode de configuration

	contextuelle. Si vous pouvez entrer une commande en mode d'exécution utilisateur ou privilégié, ainsi qu'en mode de configuration, et que la commande exécute différentes actions dans chaque mode, vous pouvez définir le niveau de privilège pour ces modes séparément. La colonne Variant affiche show, clear ou cmd. Vous ne pouvez définir le privilège que pour la forme show, clear ou configure de la commande. La forme configure de la commande est généralement celle qui entraîne une modification de la configuration, soit sous la forme de la commande non modifiée (sans le préfixe show ou clear), soit sous la forme no. Pour modifier le niveau d'une commande, double-cliquez dessus ou cliquez sur Modifier. Vous pouvez définir le niveau entre 0 et 15. Vous pouvez uniquement configurer le niveau de privilège de la commande principale. Par exemple, vous pouvez configurer le niveau de toutes les commandes aaa, mais pas le niveau de la commande aaa authentication et de la commande aaa authorization séparément. Pour modifier le niveau de toutes les commandes qui apparaissent, cliquez sur Select All, puis sur Edit. Cliquez sur OK pour accepter vos modifications.
Étape 5	Cliquez sur Apply. Les paramètres d'autorisation sont attribués et les modifications sont enregistrées dans la configuration en cours.

Référence

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

Problème 4. ASDM Multi-Factor Authentication (MFA)

Dépannage - Étapes recommandées

Au moment de la rédaction du présent document, l'ASDM ne prend pas en charge l'AMF (ou l'AMF2). Cette limitation inclut l'AMF avec des solutions telles que PingID, etc.

Référence

ID de bogue Cisco CSCvs85995

ENH : Accès ASDM avec authentification à deux facteurs ou MFA

Problème 5. Configuration de l'authentification externe ASDM

Dépannage - Étapes recommandées

Vous pouvez utiliser LDAP, RADIUS, RSA SecurID ou TACACS+ pour configurer l'authentification externe sur ASDM.

Références

- 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

Problème 6. L'authentification ASDM LOCAL échoue

Dépannage - Étapes recommandées

Si vous utilisez l'authentification externe et l'authentification LOCALE comme mode de secours, l'authentification locale ne fonctionne que si votre serveur externe est en panne ou ne fonctionne pas. Dans ce scénario uniquement, l'authentification LOCAL prend le relais et vous pouvez vous connecter aux utilisateurs LOCAUX.

En effet, l'authentification externe est prioritaire sur l'authentification LOCAL.

Exemple :

<#root>

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

Référence

- 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

Problème 7. Mot de passe unique ASDM

Dépannage - Étapes recommandées

- La prise en charge de l'authentification ASDM OTP (one-time-password) a été ajoutée dans ASA version 8.x - 9.x et en mode routé unique uniquement.
- L'authentification OTP ASDM pour le mode transparent et/ou le mode multicontexte du pare-feu ASA n'entre pas dans cette catégorie.

Référez-vous à l'ID de bogue Cisco CSCtf23419
ENH : Prise en charge de l'authentification ASDM OTP en mode multicontexte et transparent

Problème 8. Le profil de connexion n’affiche pas toutes les méthodes

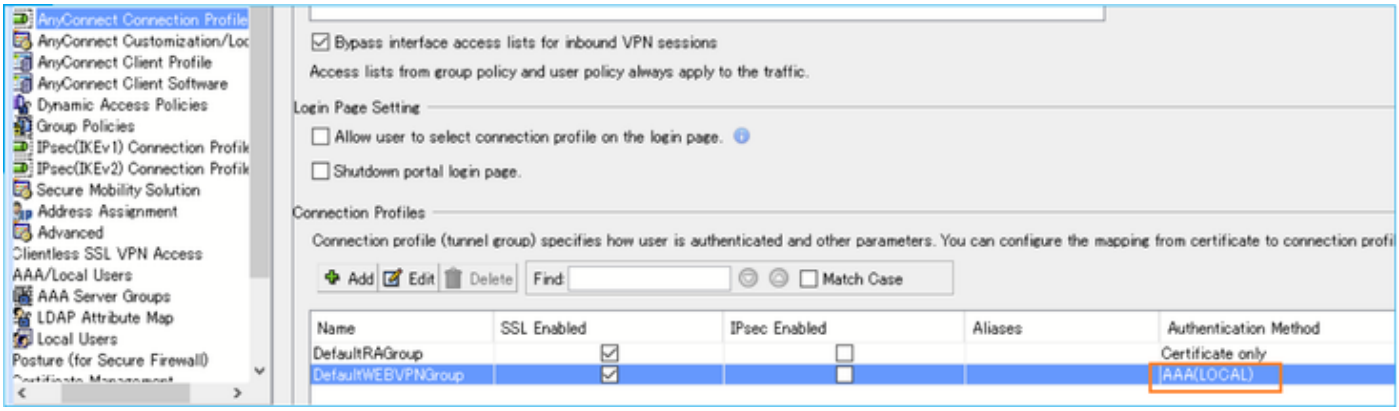
Le problème dans ce cas est une non-correspondance entre la configuration CLI ASA et l'interface utilisateur ASDM.

Plus précisément, l'interface CLI offre :

<#root>

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

Tandis que l'interface utilisateur ASDM ne mentionne pas la méthode de certificat :



Dépannage - Étapes recommandées

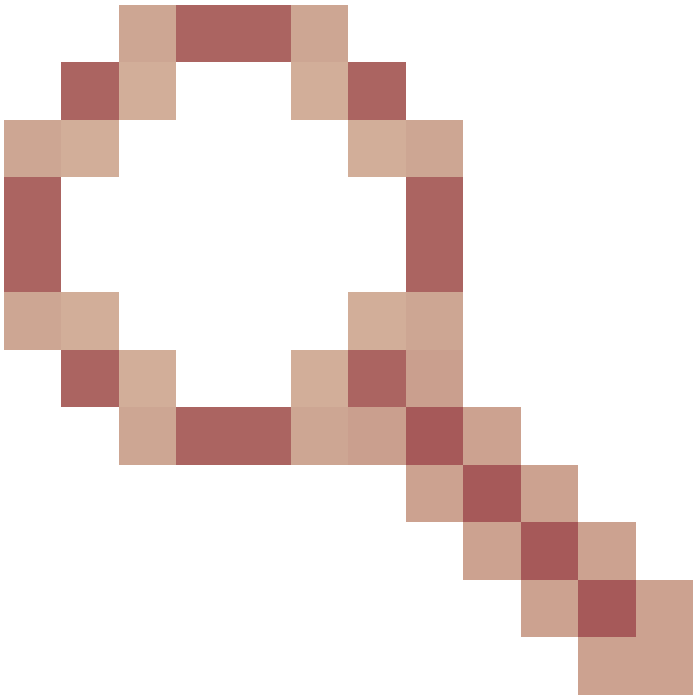
C'est une question de cosmétique. La méthode ne s'affiche pas dans l'ASDM, mais l'authentification de certificat est utilisée.

Problème 9. La session ASDM n'expire pas

Le symptôme est que le délai d'expiration de session de l'interface utilisateur graphique ASDM n'est pas pris en compte.

Dépannage - Étapes recommandées

Cela se produit lorsque la commande "aaa authentication http console LOCAL" n'est pas définie sur l'ASA géré.



Référez-vous à l'ID de bogue Cisco CSCwj70826
ENH : ajouter un avertissement : définition du délai d'expiration de la session, nécessite « aaa authentication http console LOCAL »

Solution de contournement

Configurez la commande « aaa authentication http console LOCAL » sur l'ASA géré.

Problème 10. Échec de l’authentification LDAP ASDM

Dépannage - Étapes recommandées

Étape 1

Assurez-vous que la configuration est en place, par exemple :

<#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

Étape 2

Vérifiez l'état du serveur LDAP :

<#root>

```
asa#
```

show aaa-server

Bon scénario :

<#root>

```
Server status:
```

ACTIVE

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

Scénario incorrect :

<#root>

```
Server status:
```

FAILED

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

Étape 3

Vérifiez que l'authentification LOCAL fonctionne correctement en désactivant temporairement l'authentification LDAP.

Étape 4

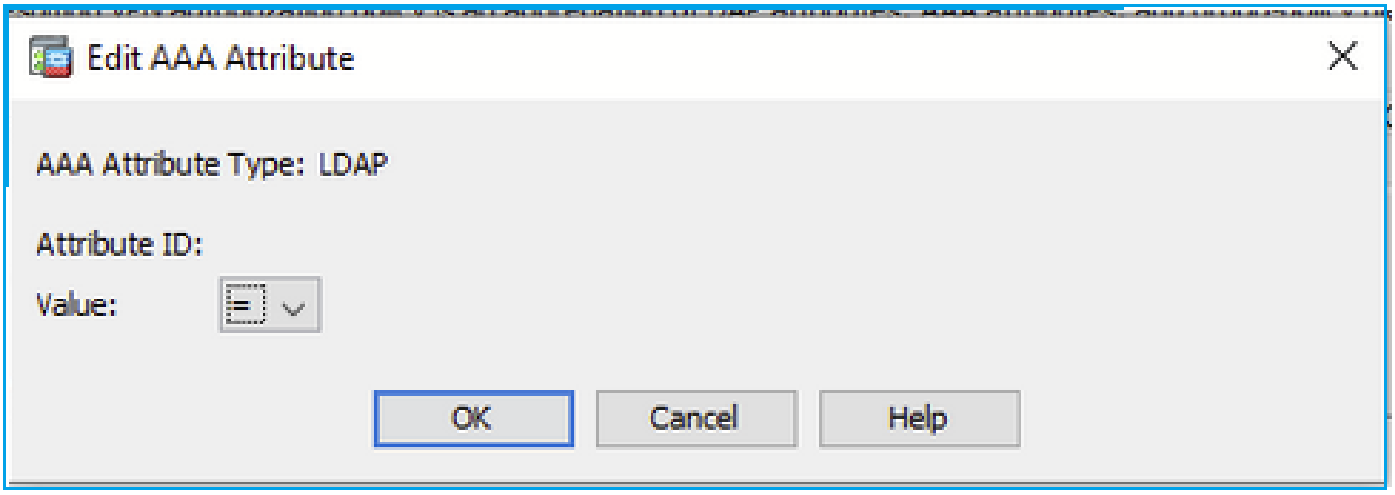
Sur ASA, exécutez les débogages LDAP et essayez d'authentifier l'utilisateur :

```
<#root>

#

debug ldap 255
```

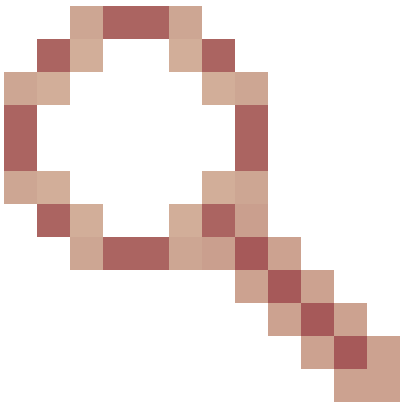
Dans les débogages, recherchez les lignes qui contiennent des indications telles que « Failed ».

Problème 11. La configuration de l'ASDM Webvpn DAP est manquante

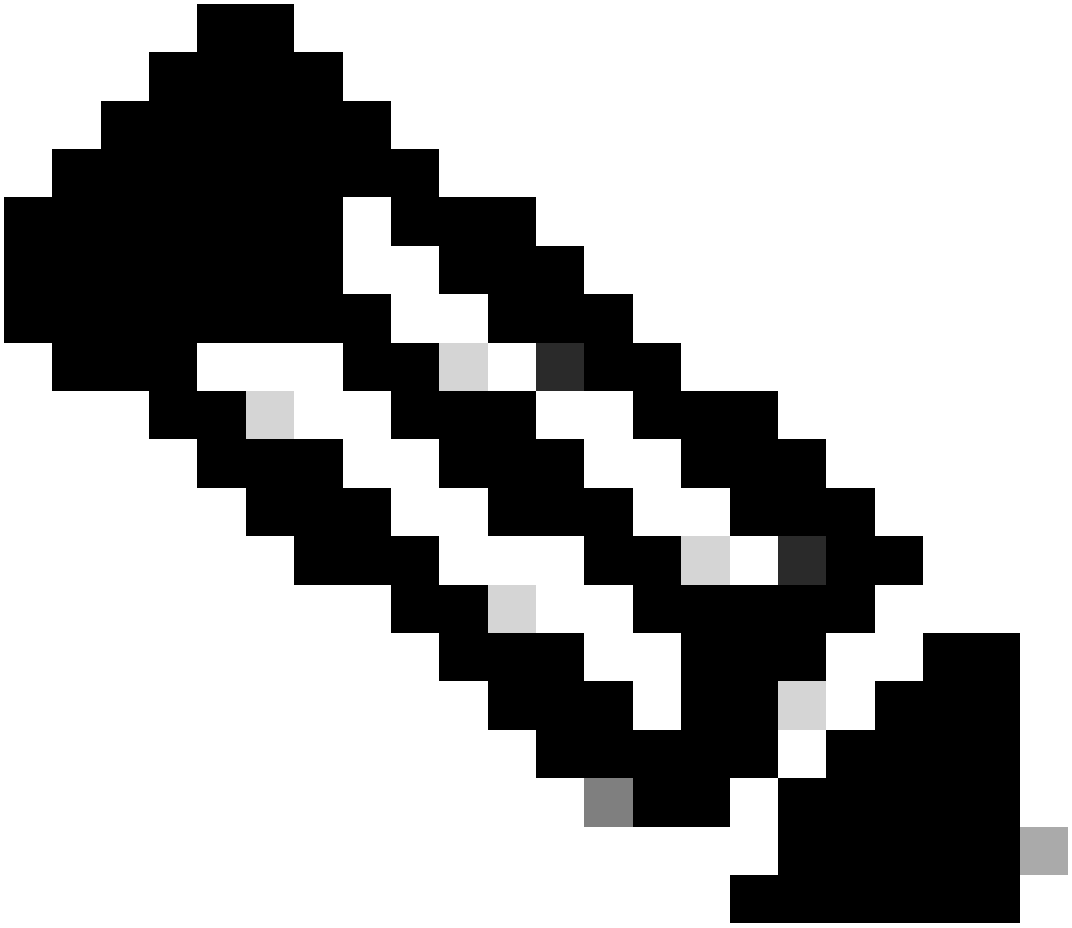
Sous la configuration DAP sur l'ASDM, les attributs AAA de type (Radius/LDAP) ne sont pas visibles uniquement si = et != sont affichés dans la liste déroulante :



Dépannage - Étapes recommandées



Il s'agit d'un défaut logiciel suivi par l'ID de bogue Cisco CSCwa99370
ASDM : type d'attribut AAA manquant dans la configuration LDAP (Radius/LDAP)

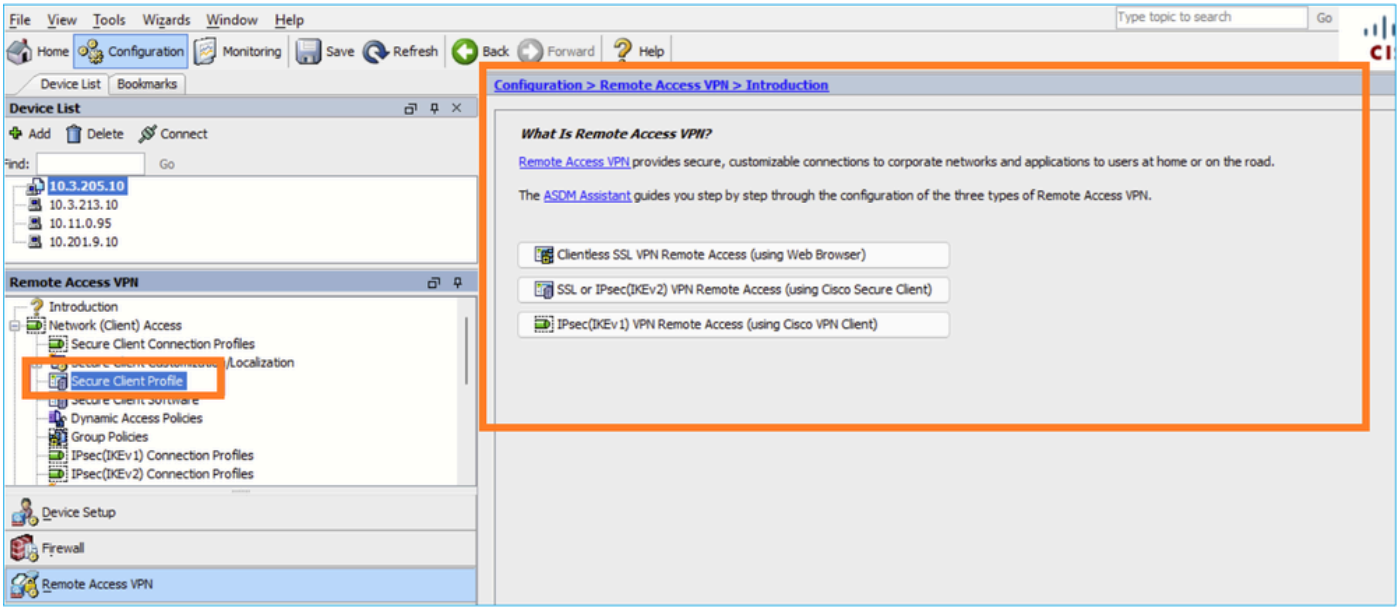


Remarque : Ce défaut a été corrigé dans les versions récentes du logiciel ASDM. Consultez les détails du défaut pour plus d'informations.

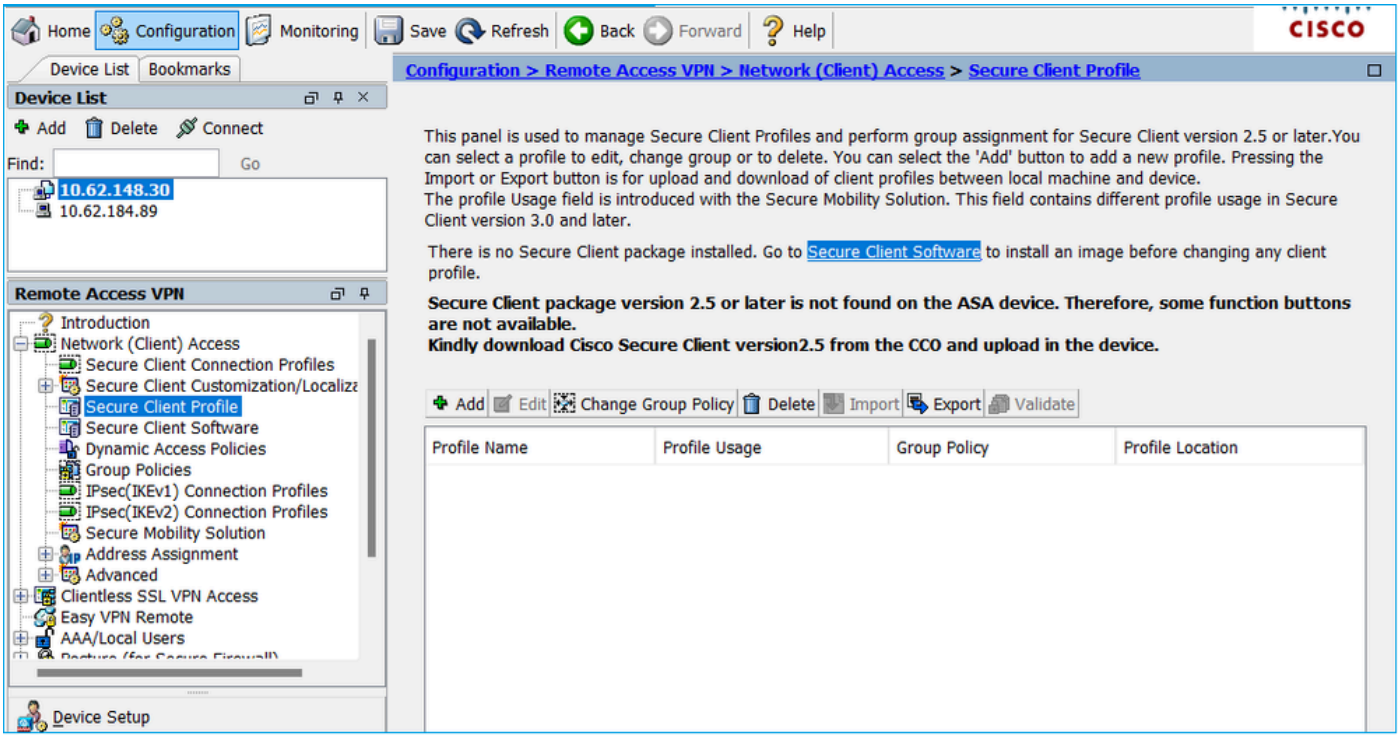
Dépannage d'ASDM Autres problèmes

Problème 1. Impossible d'accéder au profil client sécurisé sur ASDM

L'interface utilisateur ASDM affiche ceci :



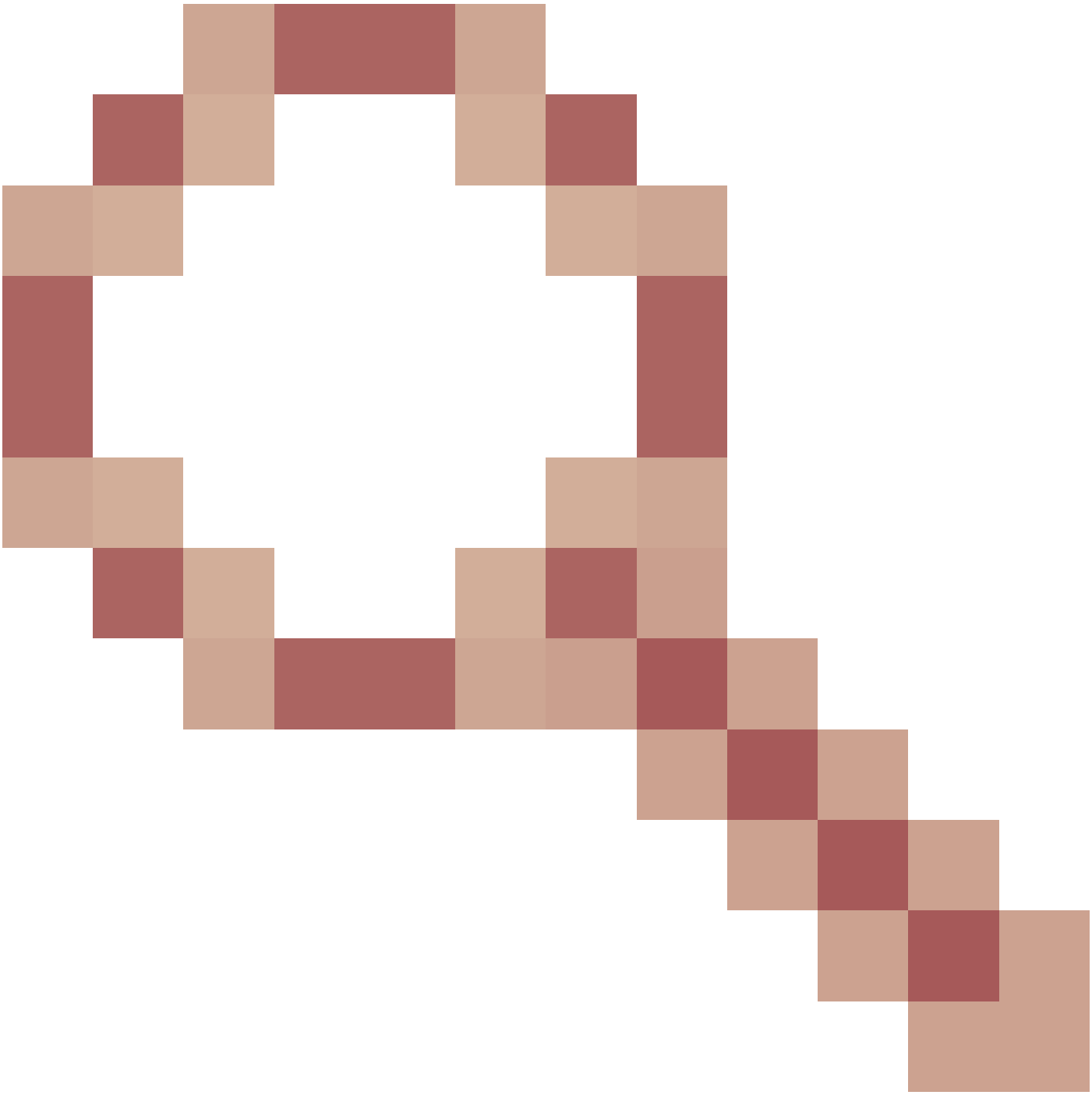
Le résultat attendu de l'interface utilisateur est :



Dépannage - Étapes recommandées

Il s'agit d'un défaut connu :

ID de bogue Cisco CSCwi56155



Impossible d'accéder au profil client sécurisé sur ASDM

Contournements :

Rétrograder AnyConnect

ou

Mettre à niveau ASDM vers la version 7.20.2

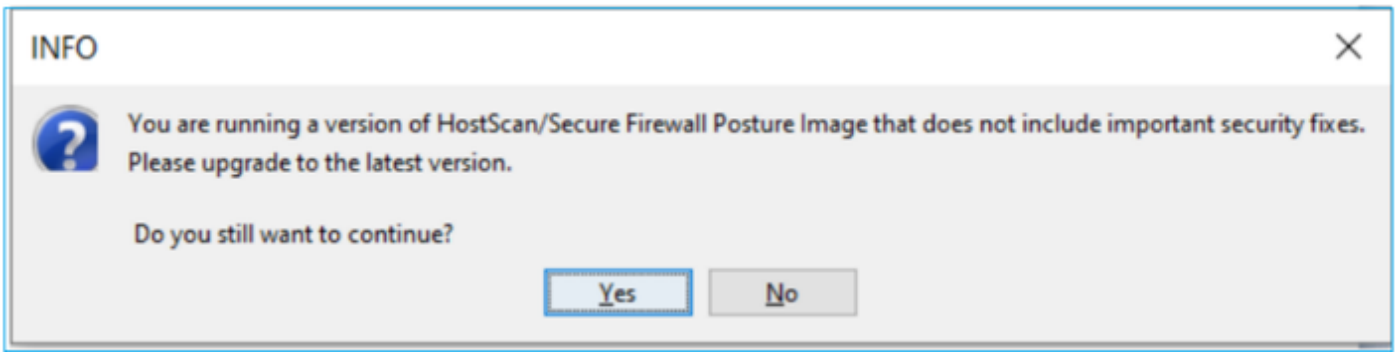
Consultez les notes de défaut pour plus de détails. En outre, vous pouvez vous abonner au défaut, de sorte que vous receviez une notification sur les mises à jour de défaut.

Problème 2. ASDM affiche une fenêtre contextuelle pour hostscan - l'image n'inclut

pas de correctifs de sécurité importants

L'interface utilisateur ASDM affiche :

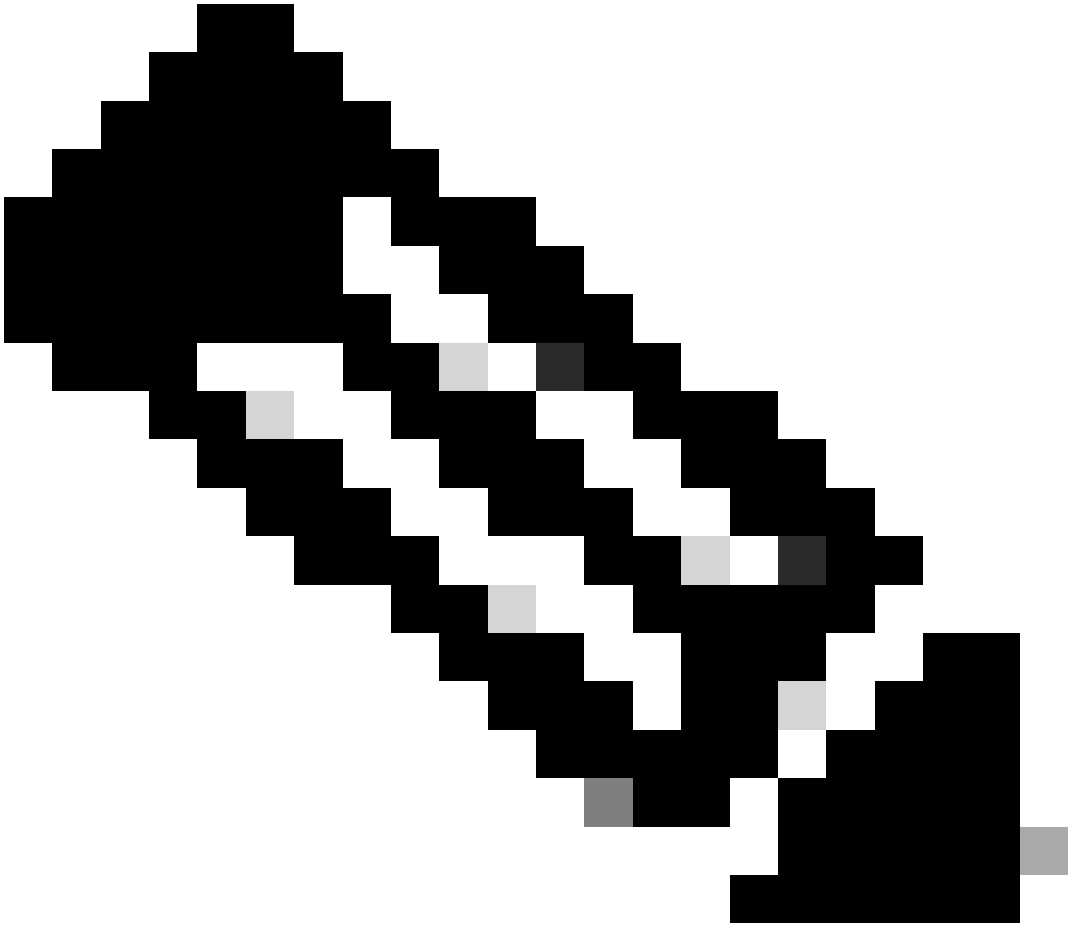
"Vous exécutez une version de l'image de position de HostScan/SecureFirewall qui n'inclut pas de correctifs de sécurité importants. Effectuez une mise à niveau vers la dernière version. Voulez-vous toujours continuer ?"



Dépannage - Étapes recommandées

Il s'agit d'un défaut connu :

ID de bogue Cisco CSCwc62461
Lorsque vous vous connectez à ASDM, une fenêtre contextuelle pour hostscan - l'image n'inclut pas de correctifs de sécurité importants



Remarque : Ce défaut a été corrigé dans les versions récentes du logiciel ASDM. Consultez les détails du défaut pour plus d'informations.

Solution de contournement:

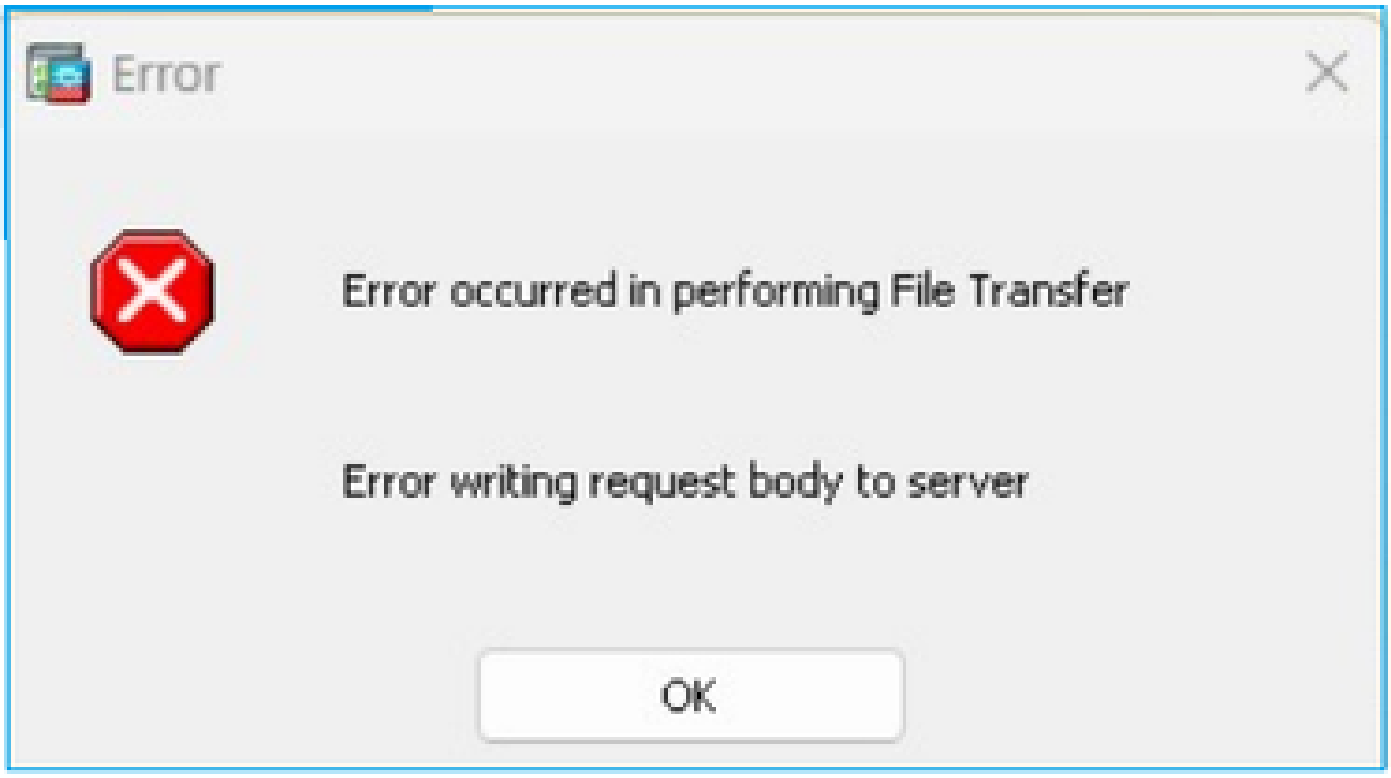
Cliquez sur « Oui » dans la boîte de message contextuelle pour continuer.

Problème 3. ASDM "Erreur lors de l'écriture du corps de la requête sur le serveur" lors de la copie d'une image sur ASDM

L'interface utilisateur ASDM affiche :

Erreur lors du transfert de fichiers

Erreur d'écriture du corps de requête sur le serveur



Dépannage - Actions recommandées

Il s'agit d'un défaut connu suivi par :

ID de bogue Cisco CSCtf74236
ASDM "Erreur d'écriture du corps de la requête sur le serveur" lors de la copie de l'image

Solution de contournement

Utilisez SCP/TFTP pour transférer le fichier.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.