Solucionar Problemas de Configuração, Autenticação e Outros Problemas do ASDM

Contents

Introdução

Este documento descreve o processo de solução de problemas de configuração, autenticação e outros problemas do Adaptive Security Appliance Device Manager (ASDM).

Background

O documento faz parte da série de solução de problemas do ASDM, juntamente com estes documentos:

Link1<>

Link2<>

Link3<>

Identificar e Solucionar Problemas de Configuração do ASDM

Problema 1. O ASDM não exibe nenhuma lista de controle de acesso (ACL) aplicada a uma interface

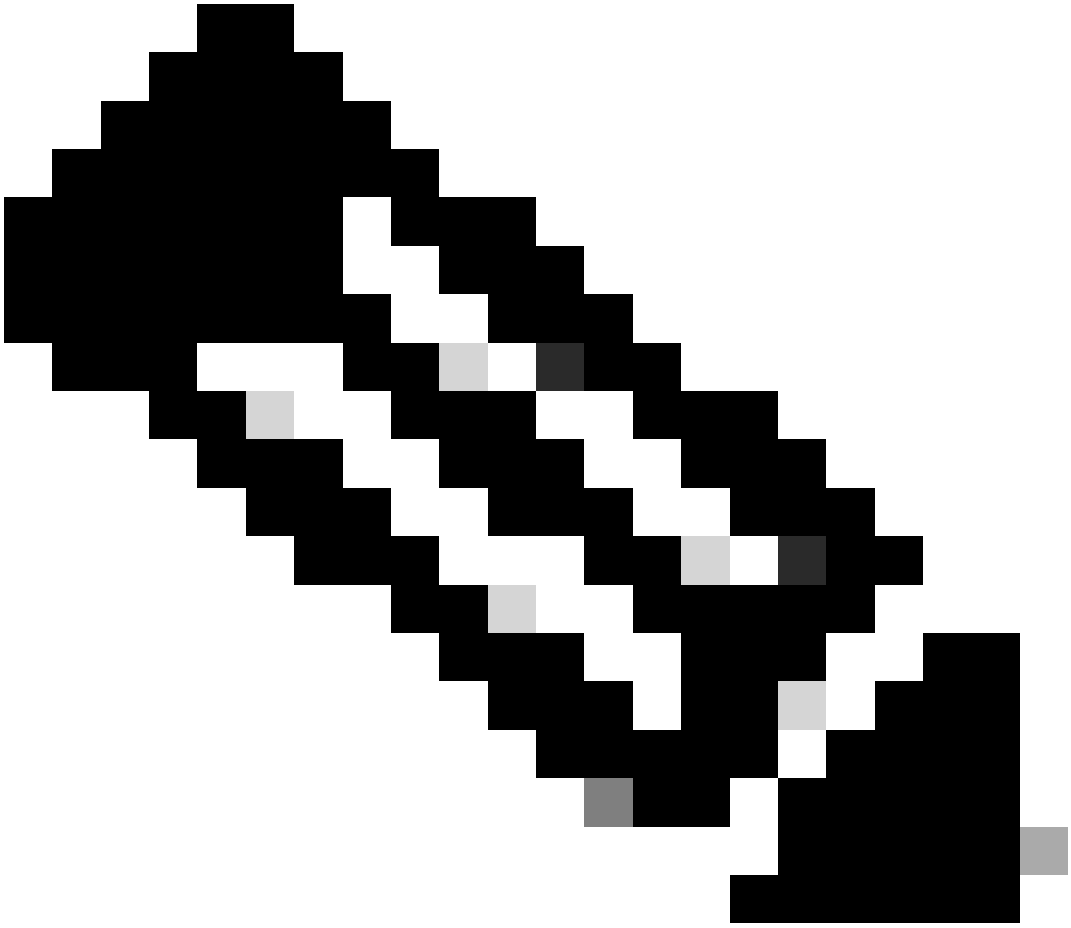
O ASDM não exibe nenhuma lista de controle de acesso (ACL) aplicada a uma interface, mesmo que haja um grupo de acesso válido aplicado à interface em questão. Em vez disso, a mensagem diz "0 incoming rules" (0 regras de entrada). Esses sintomas são observados nas ACLs L3 e L2 configuradas na configuração do grupo de acesso para uma 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
```

Solução de problemas - Ações recomendadas

Consulte o bug da Cisco ID do software CSCwj14147 "O ASDM falha ao carregar a configuração do grupo de acesso se as acls 2 e 3 forem misturadas.".



Note: Esse defeito foi corrigido em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

Problema 2. Inconsistência na contagem de ocorrências entre a CLI do ASA e a interface do usuário do ASDM

As entradas de contagem de ocorrências no ASDM não são consistentes com as contagens de ocorrências da lista de acesso conforme relatado pelo comando show access-list na saída do firewall.

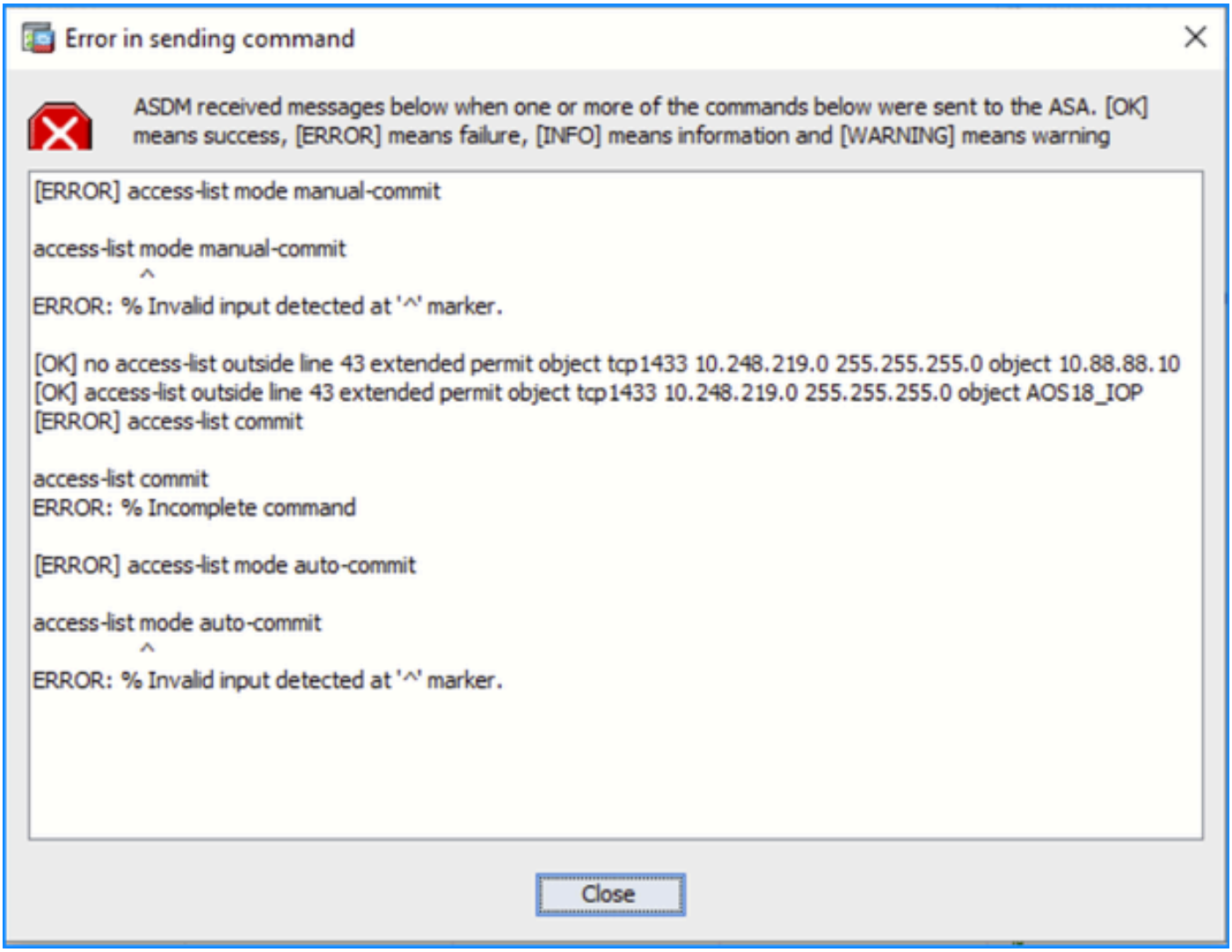
Solução de problemas - Ações recomendadas

Consulte o bug do software Cisco ID CSCtq38377 "ENH: O ASDM deve usar o hash de ACL calculado no ASA e não calculado localmente" e o bug da Cisco ID CSCtq38405"ENH: O ASA precisa de um mecanismo para fornecer informações de hash de ACL ao ASD"

Problema 3. "ERRO: % entrada inválida detectada no marcador '^'." mensagem de erro ao editar uma ACL no ASDM

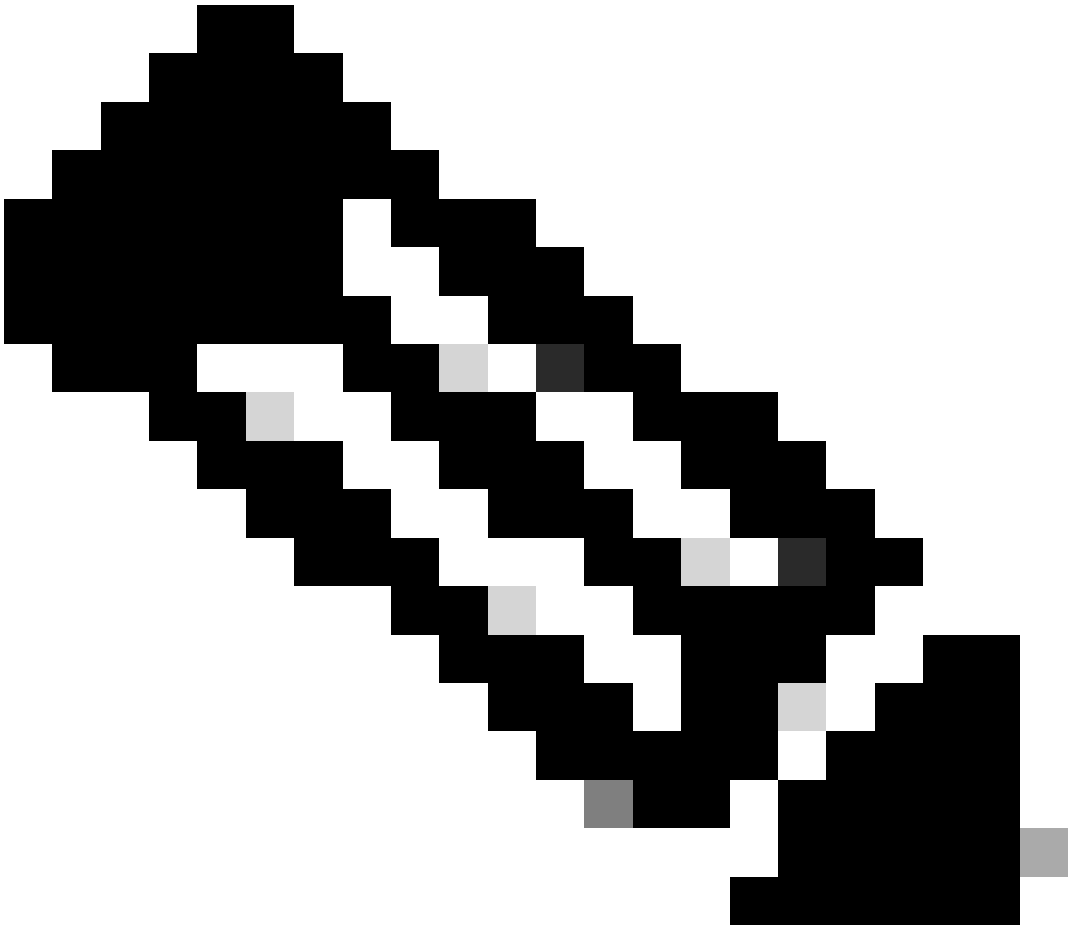
O comando "ERROR: % entrada inválida detectada no marcador '^'." é mostrada ao editar uma ACL no ASDM:

```
[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.
```



Solução de problemas - Ações recomendadas

Consulte o bug do software Cisco ID CSCvq05064 "Edit an entry (ACL) from ASDM give an error. Ao usar o ASDM com o OpenJRE/Oracle - versão 7.12.2" e o bug da Cisco ID CSCvp88926 "Enviando comandos de adição ao excluir a lista de acesso".



Note: Esses defeitos foram corrigidos em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

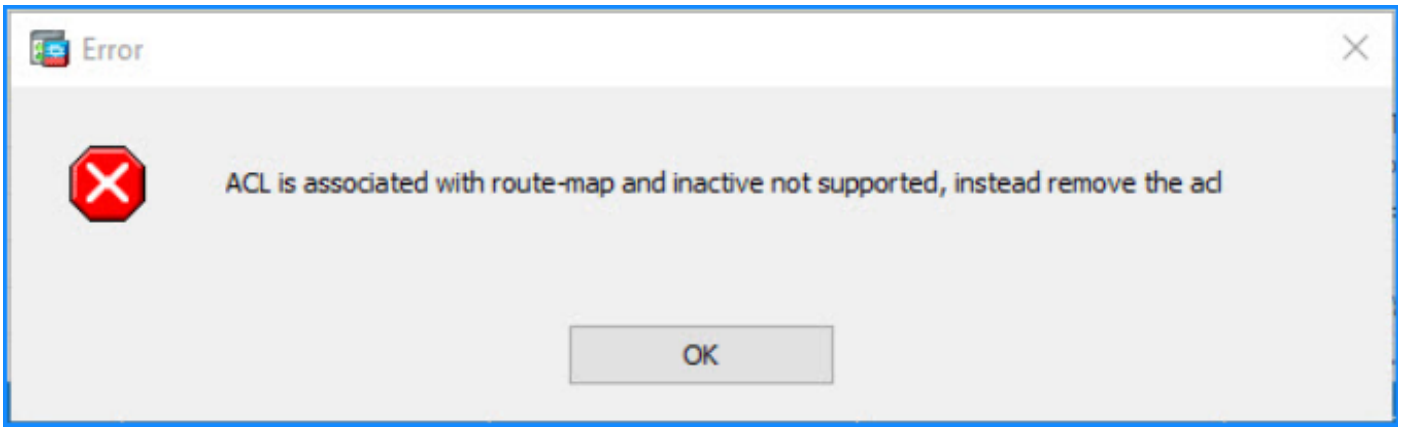
Problema 4. O comando "ERROR: A ACL está associada ao mapa de rotas e não é suportada como inativa. Em vez disso, remova a mensagem de erro "acl" em casos específicos

O comando "ERROR: A ACL está associada ao mapa de rota e não é suportada inativa. Em vez disso, a mensagem de erro "remove the acl" é mostrada em um destes casos:

1. Edite uma ACL no ASDM usada em uma configuração de roteamento baseada em política:

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

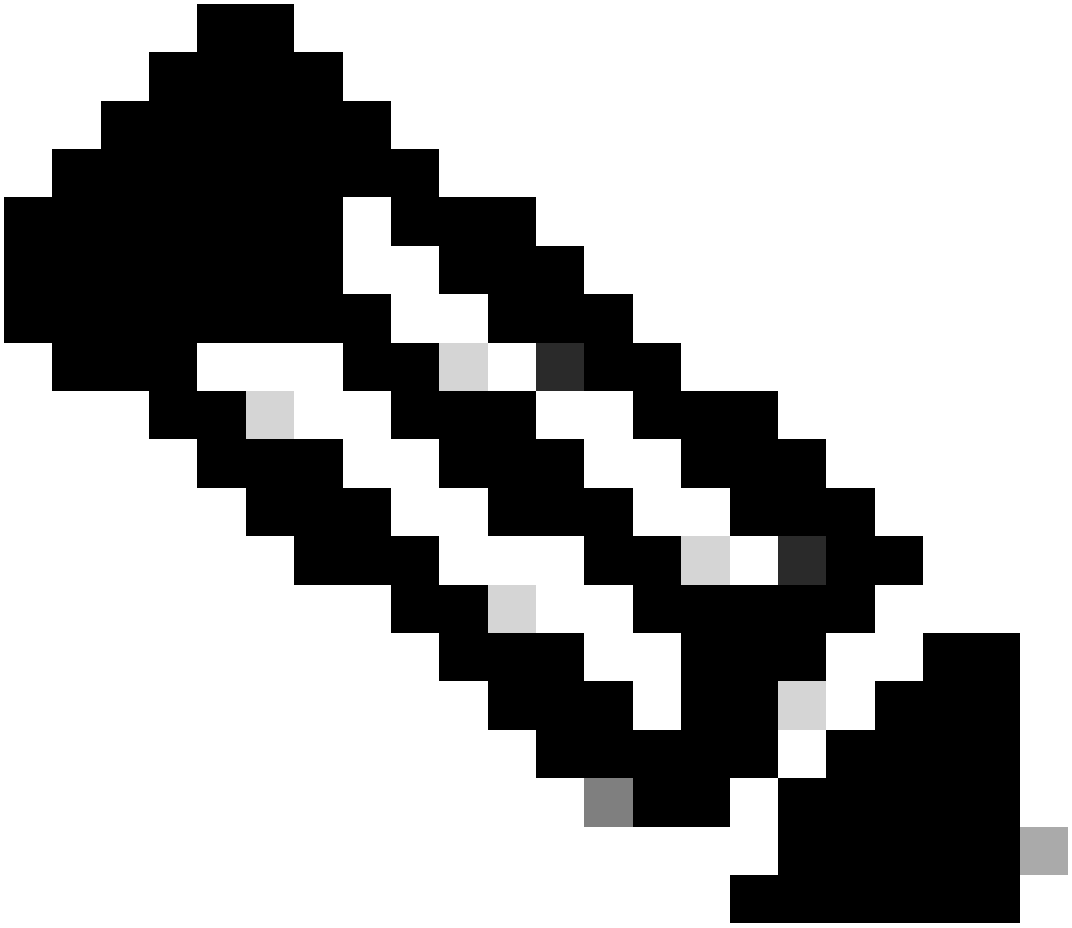
ERRO: A ACL está associada ao mapa de rota e não há suporte para inativo; em vez disso, remova a ACL



2. Edite uma ACL ASDM > Configuração -> VPN de Acesso Remoto -> Acesso à Rede (Cliente) > política de Acesso Dinâmico

Solução de problemas - Ações recomendadas

1. Consulte o bug da Cisco ID de software CSCwb57615 "Configuring pbr access-list with line number failed." A solução alternativa é excluir o parâmetro "line" da configuração.
2. Consulte o bug do software Cisco ID CSCwe3465 "Unable to Edit the ACL objects if it is already in use, getting the exception" (Não é possível editar os objetos ACL se ele já estiver em uso, obtendo a exceção).



Note: Esses defeitos foram corrigidos em versões recentes do software ASA. Verifique os detalhes do defeito para obter mais informações.

Problema 5. Nenhum log no Visualizador de Log em Tempo Real do ASDM para conexões implicitamente negadas

O Visualizador de Log em Tempo Real do ASDM não mostra logs para conexões implicitamente negadas.

Solução de problemas - Ações recomendadas

O deny implícito no final da lista de acesso não gera syslog. Se você quiser que todo o tráfego negado gere syslog, adicione a regra com a palavra-chave log no final da ACL.

Problema 6. O ASDM congela ao tentar modificar qualquer objeto de rede ou grupo de objetos

O ASDM congela ao tentar modificar qualquer objeto de rede ou grupo de objetos na página Configuration > Firewall > Access Rules na guia Addresses. O usuário não poderá editar nenhum dos parâmetros na janela de objeto de rede quando esse problema for encontrado.

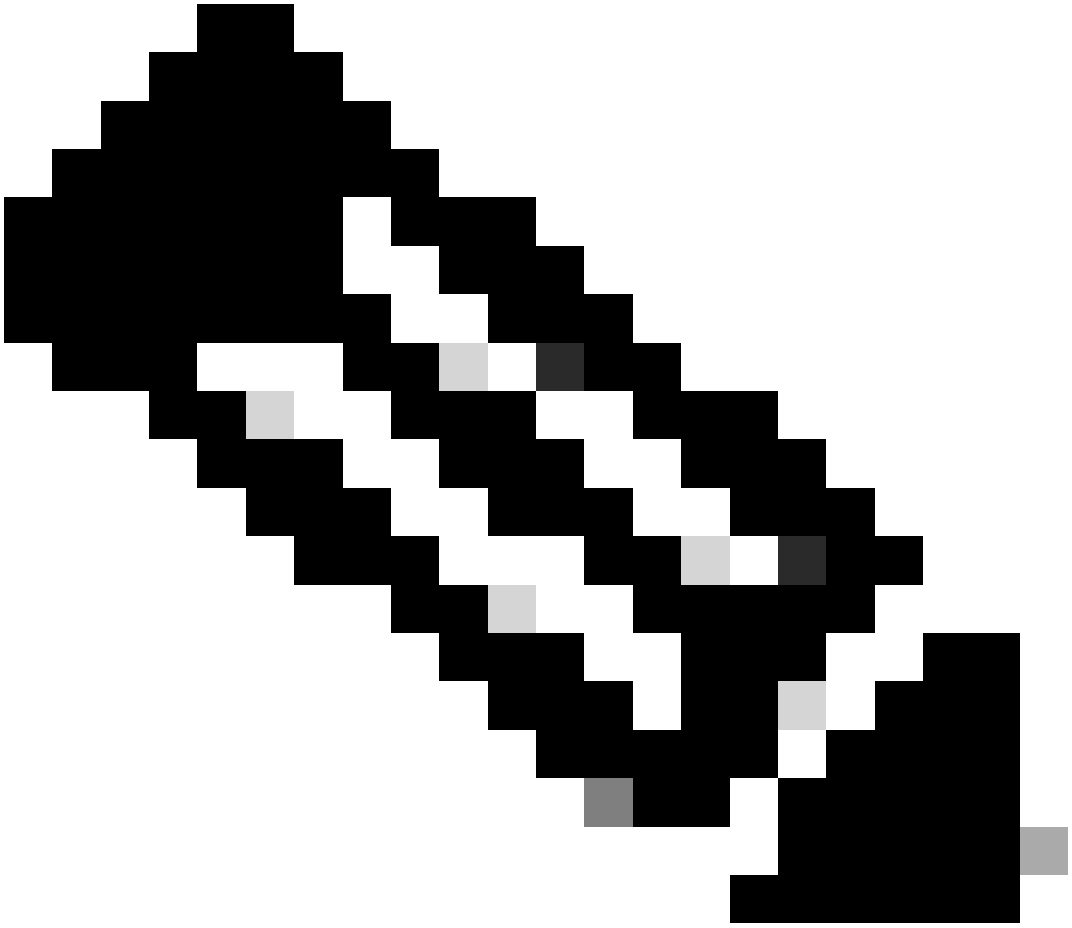
Solução de problemas - Ações recomendadas

Consulte o bug da Cisco ID CSCwj1250 "ASDM congela ao editar objetos de rede ou grupos de objetos de rede". A solução é desativar a coleta de estatísticas do host topN:

<#root>

```
ASA(config)#
```

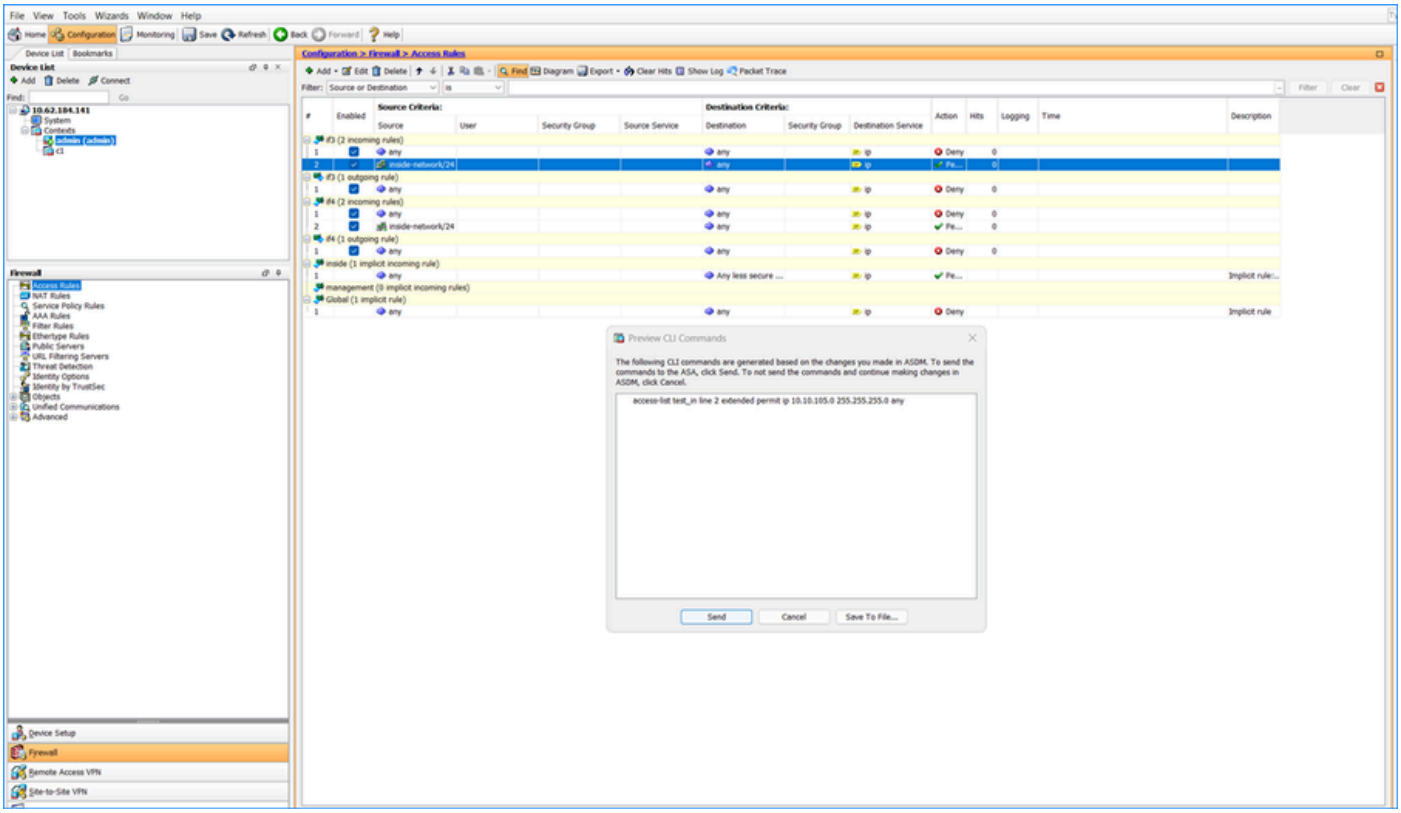
no hpm topN enable



Note: Esse defeito foi corrigido em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

Problema 7. O ASDM pode mostrar regras adicionais da lista de controle de acesso para diferentes interfaces

O ASDM pode mostrar regras adicionais da lista de controle de acesso para diferentes interfaces se uma lista de controle de acesso no nível da interface for modificada. Neste exemplo, uma regra de entrada nº 2 foi adicionada à interface if3 ACL. O ASDM também mostra #2 para a interface if4, enquanto essa regra não foi configurada pelo usuário. A visualização do comando mostra corretamente uma única alteração pendente. Esse é um problema de exibição da interface do usuário.



Solução de problemas - Ações recomendadas

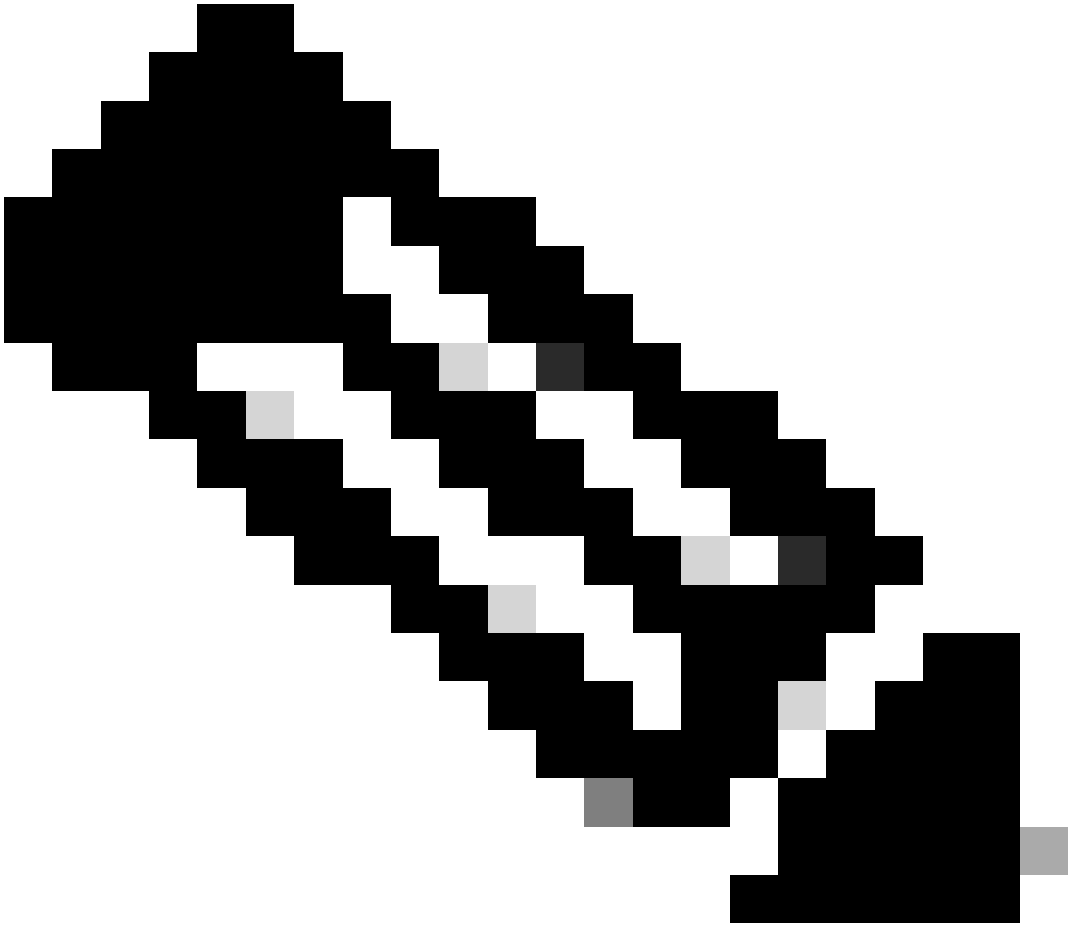
Consulte o bug da Cisco ID do software CSCwm71434 "O ASDM pode exibir entradas duplicadas da lista de acesso da interface".

Problema 8. Os registros em tempo real não estão disponíveis no Visualizador de registros em tempo real

Nenhum registro é mostrado no Visualizador de registros em tempo real

Solução de problemas - Ações recomendadas

1. Verifique se o registro está configurado. Consulte o Livro 1 do ASDM: Guia de configuração do ASDM para operações gerais do Cisco ASA Series, 7.22, Capítulo: Registro.
2. Consulte o bug do software Cisco ID CSCvf82966 "ASDM - Logging: Unable to View Real-Time logs" (Não foi possível exibir logs em tempo real).

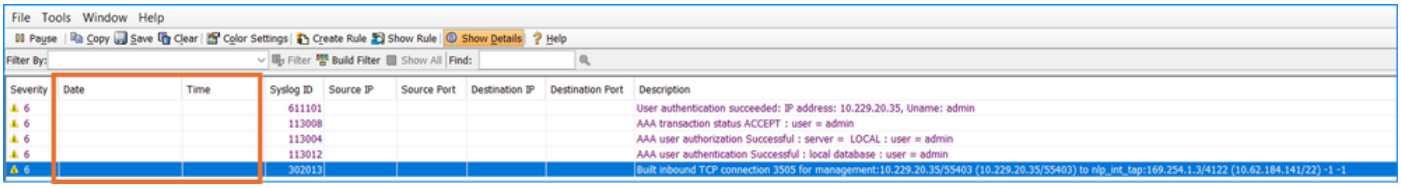


Note: Esse defeito foi corrigido em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

Referências

- Livro 1 do ASDM: Guia de configuração do ASDM para operações gerais do Cisco ASA Series, 7.22, Capítulo: Registro.

Problema 9. As colunas Data e Hora estão vazias no Visualizador de Log em Tempo Real



Solução de problemas - Ações recomendadas

1. Verifique se o formato de carimbo de data/hora de registro RFC5424 é usado:

```
<#root>

#

show run logging


logging enable

logging timestamp rfc5424
```

2. Se o formato de carimbo de data/hora de registro RFC5424 for usado, consulte o bug do software Cisco ID CSCvs5212 "ASDM ENH: potencialidade para Visualizadores de registro de eventos para exibir syslogs ASA com rfc5424 formato de carimbo de data/hora". A solução alternativa é evitar o uso do formato RFC5424:

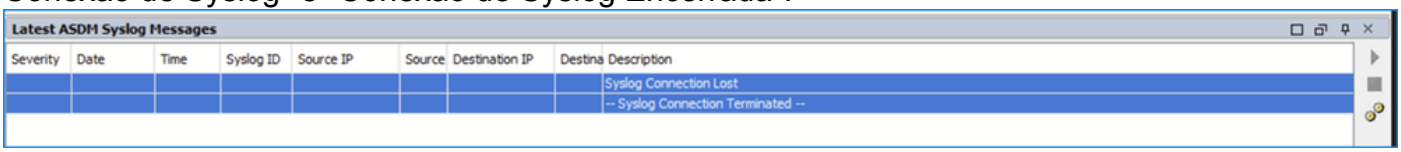
```
<#root>

firewall(config)#

no logging timestamp rfc5424


firewall(config)#

logging timestamp
```

3. Além disso, consulte o bug da Cisco com defeito de software ID CSCwh70323 "Timestamp entry missing for some syslog messages sent to syslog server" (Entrada de timestamp ausente para algumas mensagens de syslog enviadas ao Servidor syslog).

Note: Esse defeito foi corrigido em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

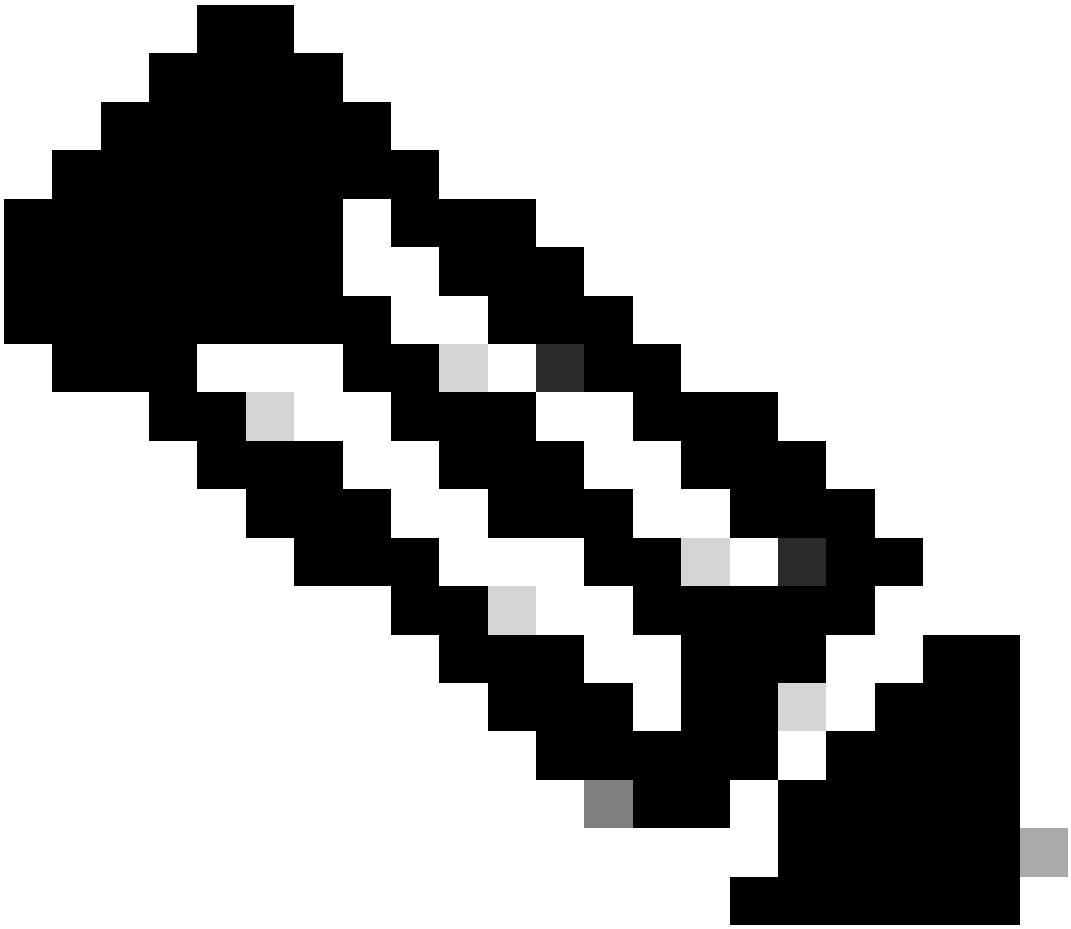
Problema 10. O registro no ASDM pode falhar após a alternância para um contexto diferente em um ASA multicontexto

A guia Últimas Mensagens de Syslog do ASDM na Home mostra as mensagens "Perda de Conexão de Syslog" e "Conexão de Syslog Encerrada":



Solução de problemas - Ações recomendadas

Verifique se o registro está configurado. Consulte o bug do software Cisco ID CSCvz15404 "ASA: Modo de contexto múltiplo: O registro do ASDM para, quando alternado para um contexto diferente".



Note: Esse defeito foi corrigido em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

Problema 11. Sessão ASDM encerrada abruptamente ao alternar entre diferentes contextos

Sessão ASDM encerrada abruptamente ao alternar entre contextos diferentes com a mensagem de erro "O número máximo de sessões de gerenciamento para o protocolo http ou usuário já existe. Tente novamente mais tarde". Esses registros são mostrados nas mensagens de 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
```

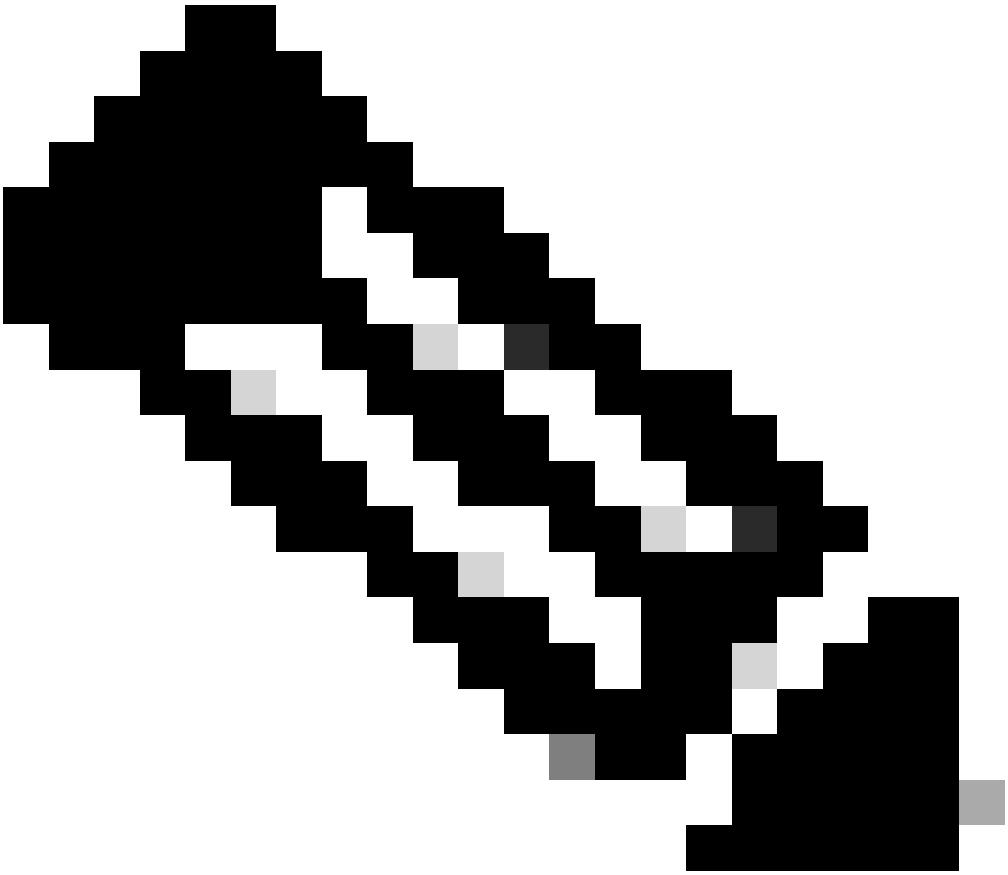
Solução de problemas - Ações recomendadas

1. Verifique se o uso do recurso Atual do ASDM atingiu o Limite. Nesse caso, o contador de Negado aumenta:

<#root>

```
firewall #

show resource usage resource ASDM


Resource                Current        Peak      Limit        Denied Context
ASDM

5

           5

5



10

 admin
```

2. Consulte o bug do software Cisco ID CSCvs72378 "Sessão ASDM sendo encerrada abruptamente ao alternar entre diferentes contextos".



Note: Esse defeito foi corrigido em versões recentes do software ASA. Verifique os detalhes do defeito para obter mais informações.

3. Se a versão do software tiver a correção para o bug da Cisco ID CSCvs72378, e o recurso atual atingir o limite, desconecte algumas das sessões ASDM existentes. Você pode fechar o ASDM ou, como alternativa, limpar as conexões HTTPS para o endereço IP do host que está executando o ASDM. Neste exemplo, supõe-se que o servidor HTTP no ASDM seja executado na porta HTTPS 443 padrão:

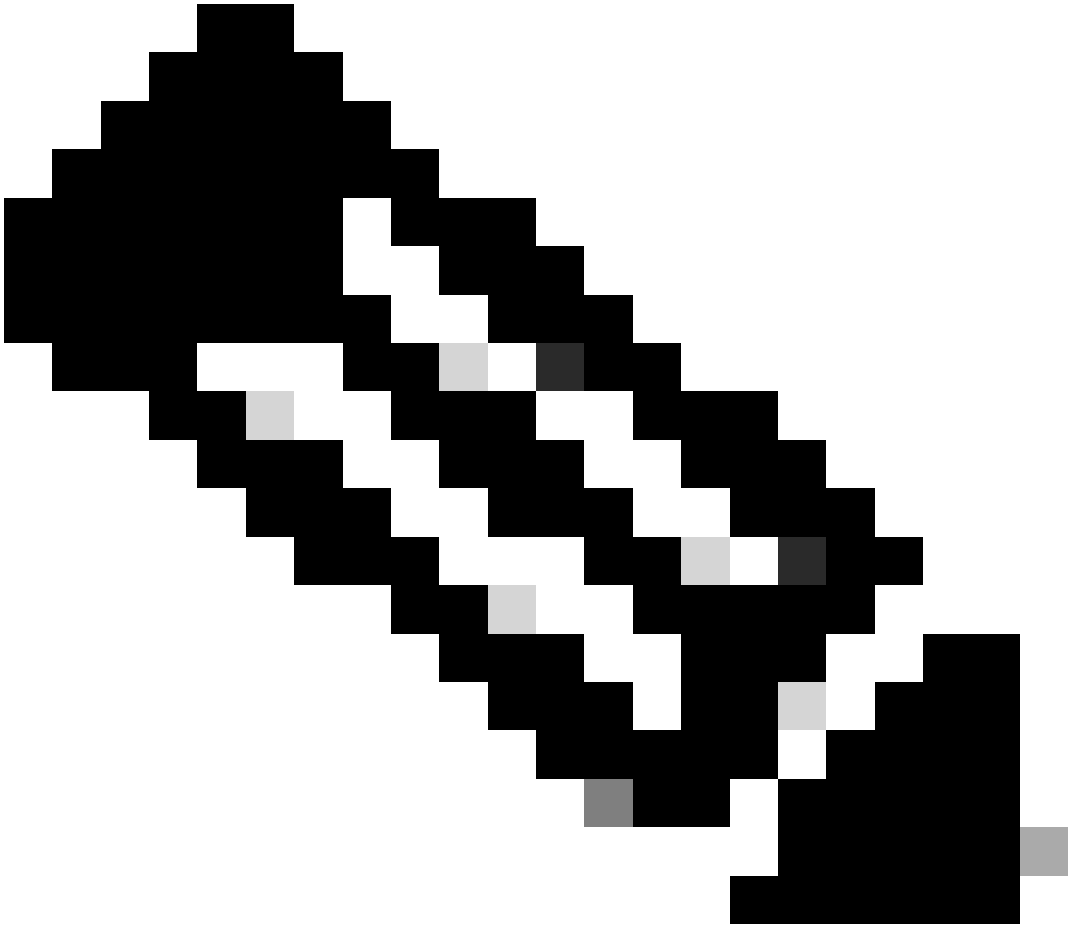
```
<#root>

#

show conn all protocol tcp port 443


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

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

Problema 12. O ASDM sai/termina aleatoriamente com a mensagem "O ASDM recebeu uma mensagem do dispositivo ASA para desconectar. O ASDM será encerrado agora."

No ASA multicontexto, o ASDM sai/termina aleatoriamente com a mensagem "O ASDM recebeu uma mensagem do dispositivo ASA para desconectar. O ASDM será encerrado agora.".

Solução de problemas - Ações recomendadas

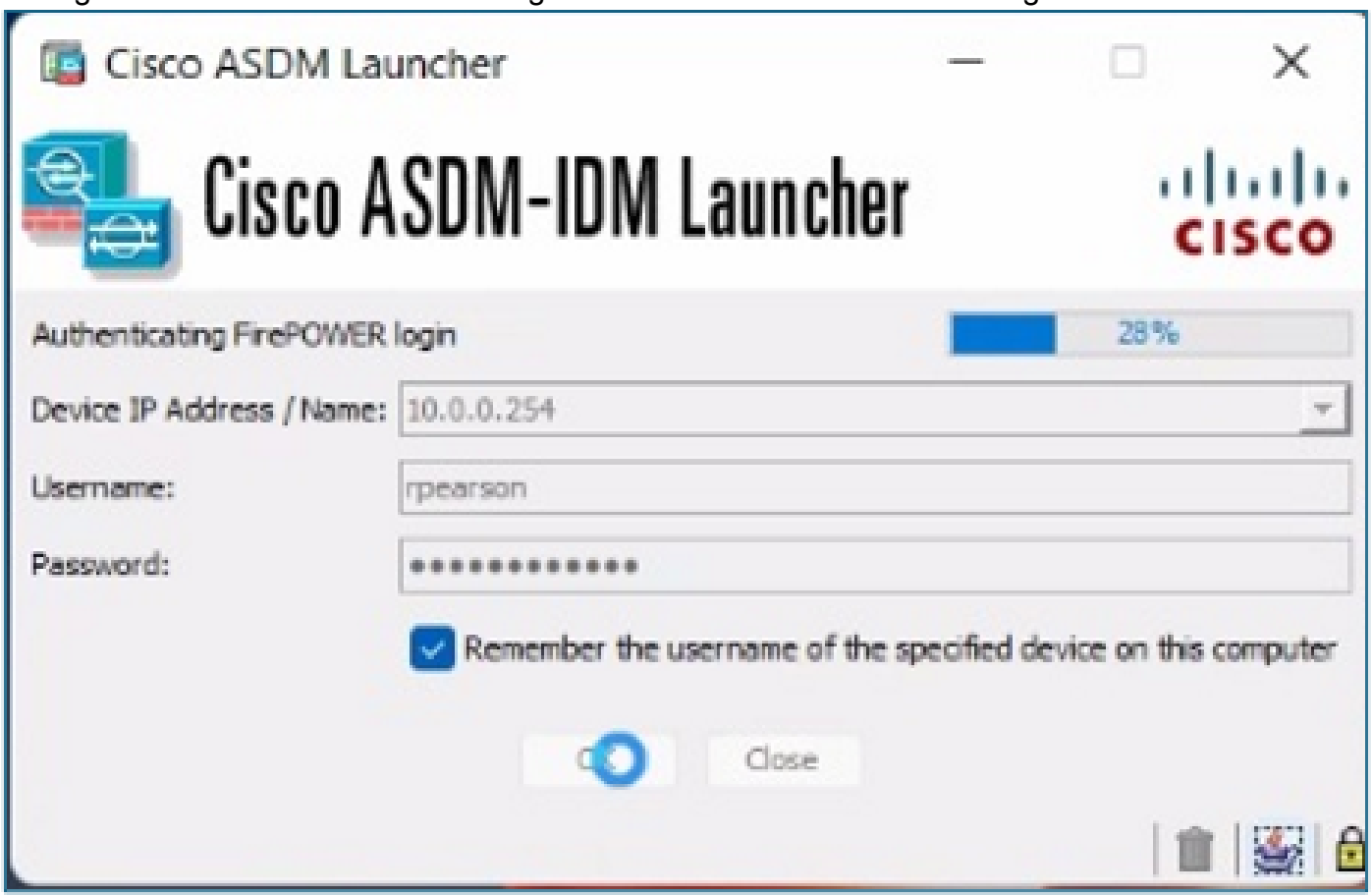
Consulte o bug da Cisco com defeito de software ID CSCwh04395 "O aplicativo ASDM sai/termina aleatoriamente com uma mensagem de alerta na configuração multicontexto".



Note: Esse defeito foi corrigido em versões recentes do software ASA. Verifique os detalhes do defeito para obter mais informações.

Problema 13. A carga do ASDM trava com a mensagem "Authentication FirePOWER login"

A carga do ASDM trava com a mensagem "Authentication FirePOWER login":



Os registros do console Java mostram a mensagem "Falha ao conectar ao FirePower, continuando sem ele":

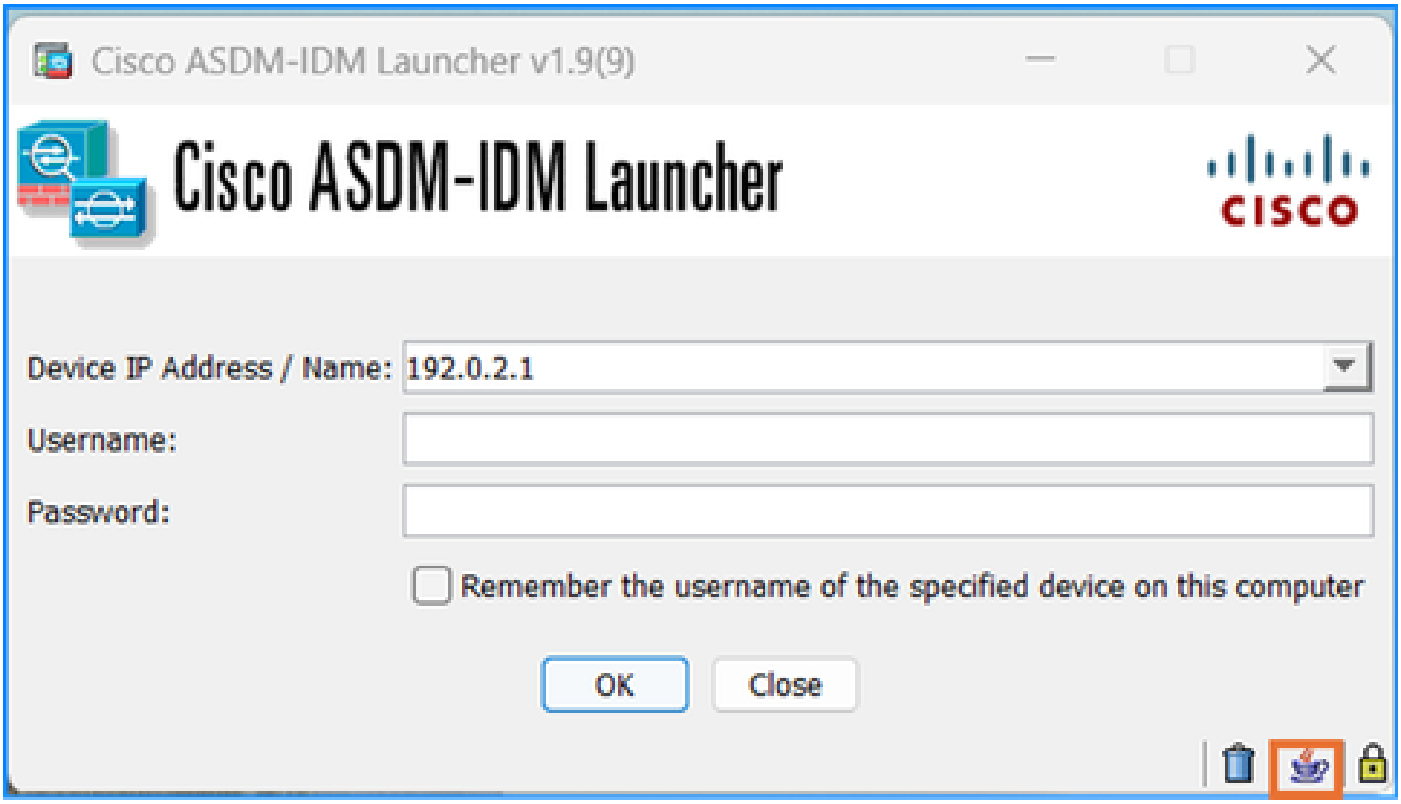
<#root>

```
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)
```

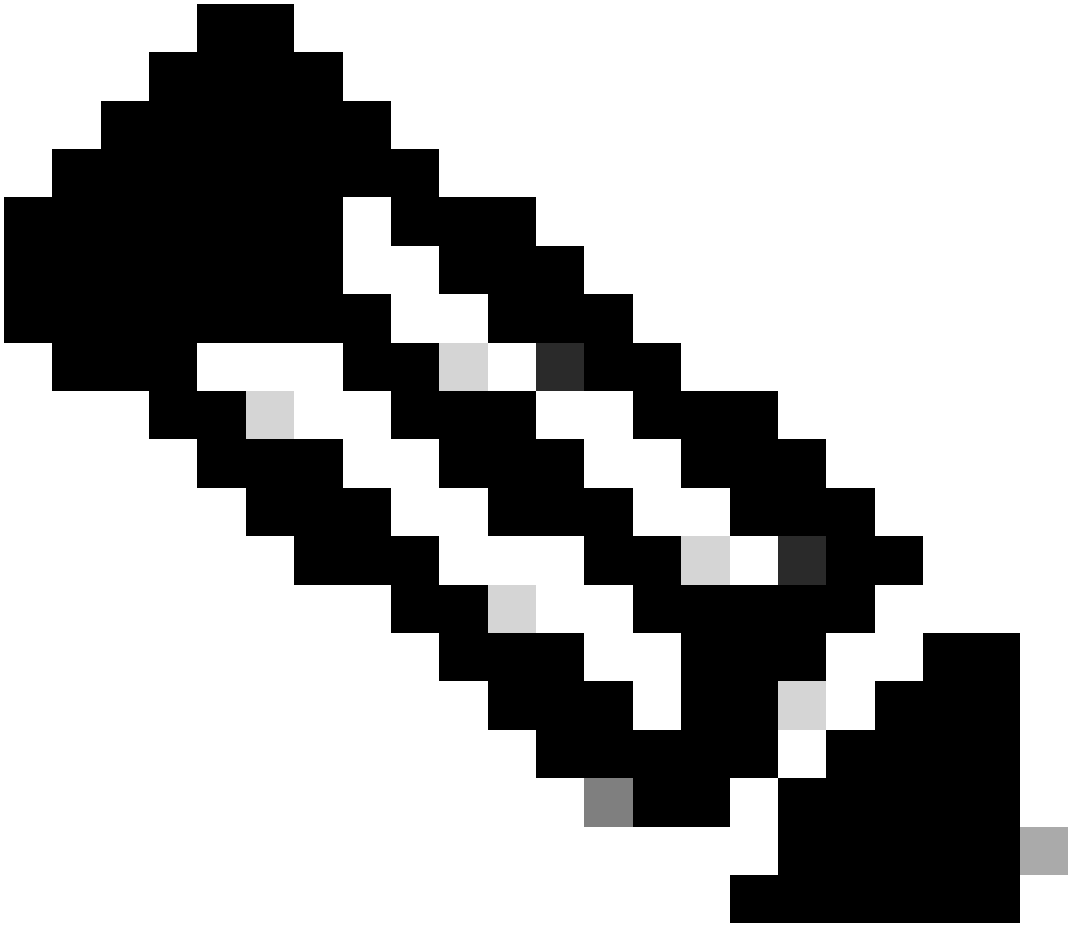
Para verificar esse sintoma, ative os registros do console Java:



Solução de problemas - Ações recomendadas

Consulte o bug do software Cisco ID CSCwe15164 "ASA: O ASDM não pode exibir guias SFR até que seja "ativado" por meio de sua CLI.". Etapas alternativas:

1. Feche o gerenciador ASDM.
2. Obtenha acesso SSH ao SFR e mude o usuário para a raiz (sudo su).
3. Depois de executar as etapas acima, reinicie o ASDM mais uma vez e ele poderá carregar as guias do Firepower (SFR).



Note: Esse defeito foi corrigido em versões recentes do software Firepower. Verifique os detalhes do defeito para obter mais informações.

Problema 14. O ASDM não mostra o gerenciamento/configuração do módulo Firepower

A configuração do módulo Firepower não está disponível no ASDM.

Solução de problemas - Ações recomendadas

1. Verifique se as versões do ASA, ASDM, módulo Firepower e sistema operacional são compatíveis. Consulte as Notas de versão do Cisco Secure Firewall ASA, Notas de versão do Cisco Secure Firewall ASDM, Compatibilidade do Cisco Secure Firewall ASA:

- O ASA 9.14/ASDM 7.14/Firepower 6.6 é a versão final do módulo ASA FirePOWER no ASA

5525-X, 5545-X e 5555-X.
- O ASA 9.12/ASDM 7.12/Firepower 6.4.0 é a versão final do módulo ASA FirePOWER no ASA 5515-X e 5585-X.
- O ASA 9.9/ASDM 7.9(2)/Firepower 6.2.3 é a versão final do módulo ASA FirePOWER no ASA 5506-X Series e 5512-X.
- As versões do ASDM são retrocompatíveis com todas as versões anteriores do ASA, a menos que especificado de outra forma. Por exemplo, o ASDM 7.13(1) pode gerenciar um ASA 5516-X no ASA 9.10(1).
- O ASDM não é compatível com o gerenciamento do módulo FirePOWER com ASA 9.8(4.45)+, 9.12(4.50)+, 9.14(4.14)+ e 9.16(3.19)+; você precisa usar o FMC para gerenciar o módulo com essas versões. Essas versões do ASA exigem o ASDM 7.18(1.152) ou posterior, mas o suporte do ASDM para o módulo ASA FirePOWER terminou com a versão 7.16.
- O ASDM 7.13(1) e o ASDM 7.14(1) não oferecem suporte ao ASA 5512-X, 5515-X, 5585-X e ao ASASM; você deve atualizar para o ASDM 7.13(1.101) ou 7.14(1.48) para restaurar o suporte ao ASDM.

2. Se as versões forem compatíveis, verifique se o módulo está em execução:

```
<#root>

firewall#

show module sfr details


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

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

App. Status:        Up


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

Data Plane Status:  Up


Console session:    Ready


Status:             Up


DC addr:            No DC Configured
Mgmt IP addr:       192.0.2.1
Mgmt Network mask:  255.255.255.0
```

```
Mgmt Gateway:        192.0.2.254
Mgmt web ports:      443
Mgmt TLS enabled:    true
```

Se o módulo estiver inoperante, o comando sw-module module reset poderá ser usado para reiniciar o módulo e depois recarregar o software do módulo.

Referências

- Notas da versão do Cisco Secure Firewall ASA
- Notas da versão do Cisco Secure Firewall ASDM
- Compatibilidade com o Cisco Secure Firewall ASA

Problema 15. Os Perfis de Cliente Seguro estão inacessíveis no ASDM

Os registros do console Java mostram a "java.lang.ArrayIndexOutOfBoundsException: Mensagem de erro de 3":

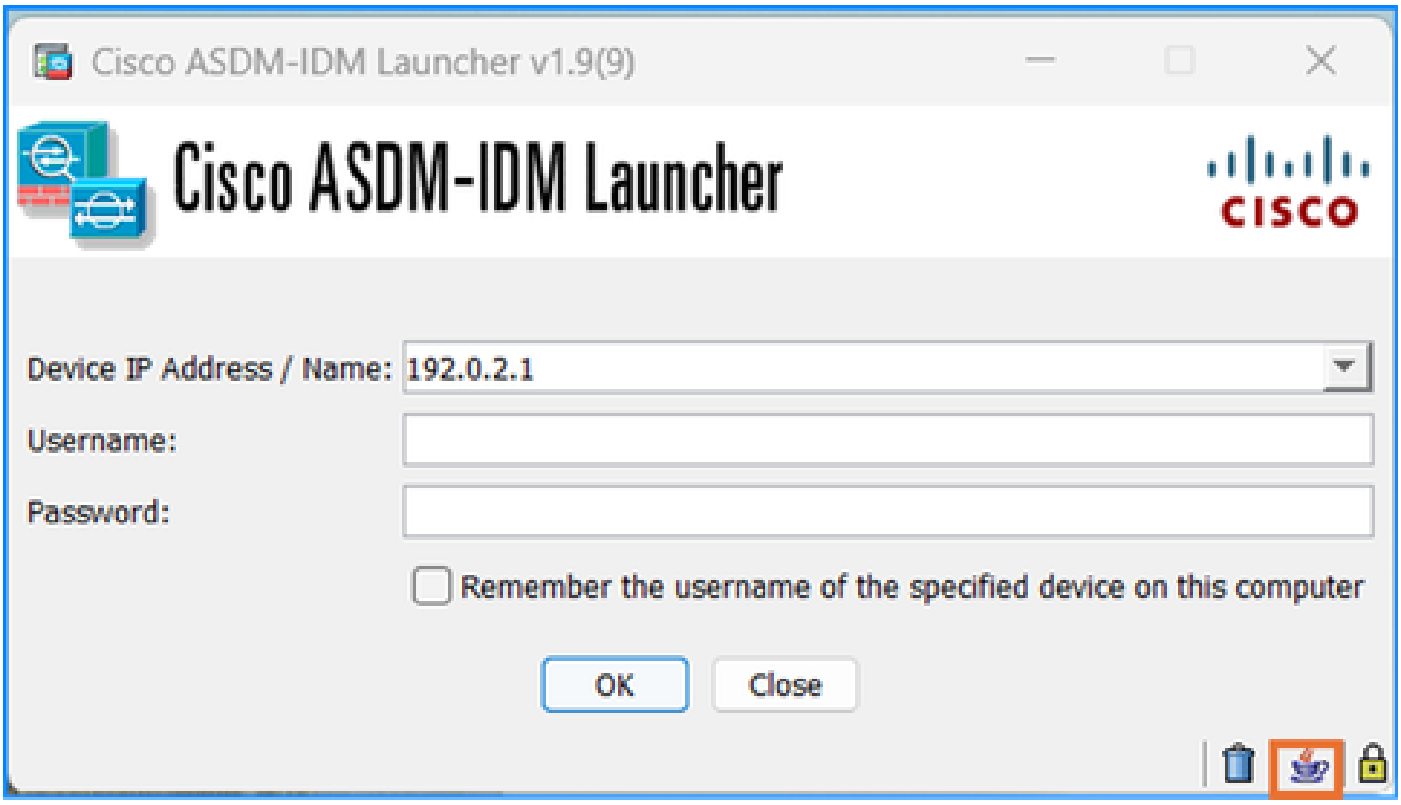
<#root>

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

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

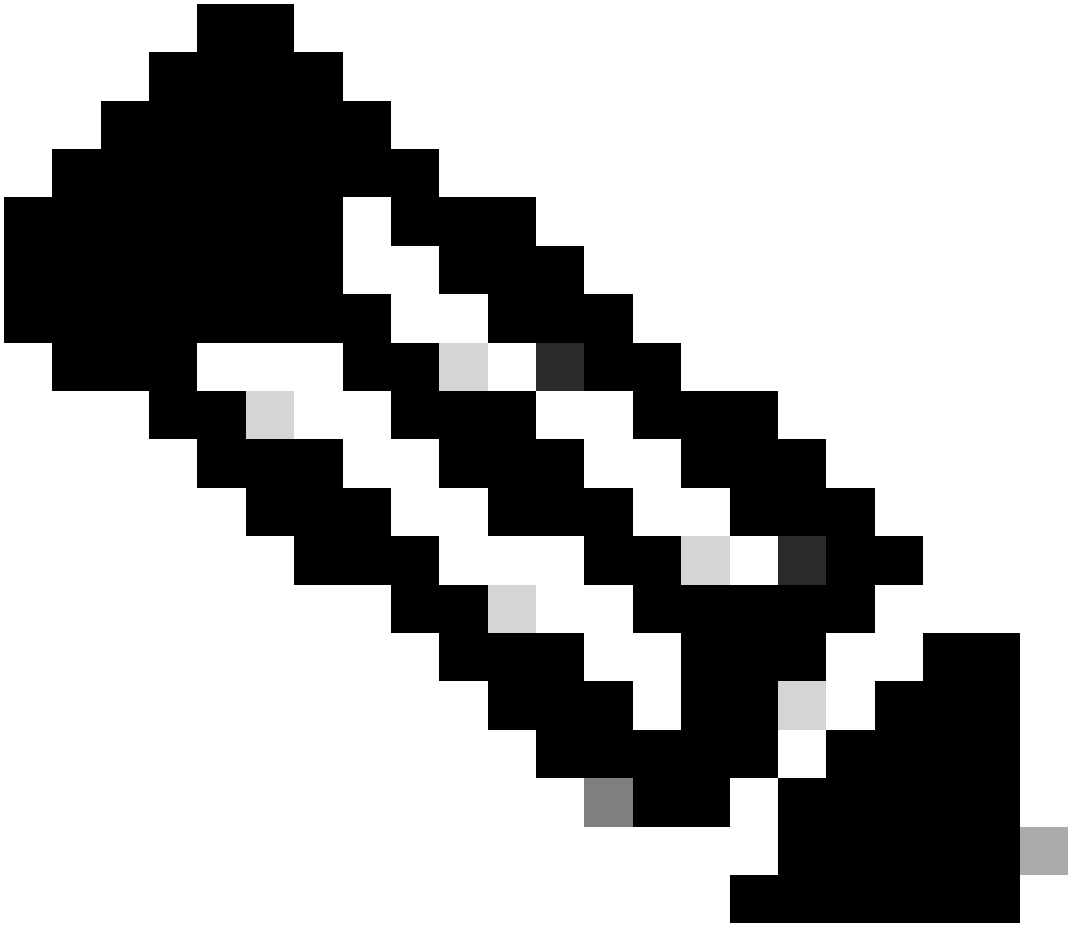
```
   at doz.a(doz.java:1256)
   at doz.a(doz.java:935)
   at doz.l(doz.java:1100)
```

Para verificar esse sintoma, ative os registros do console Java:



Solução de problemas - Ações recomendadas

Consulte o bug do software Cisco ID CSCwi56155 "Unable to access Secure Client Profile on ASDM" (Não foi possível acessar o Secure Client Profile no ASDM).



Note: Esse defeito foi corrigido em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

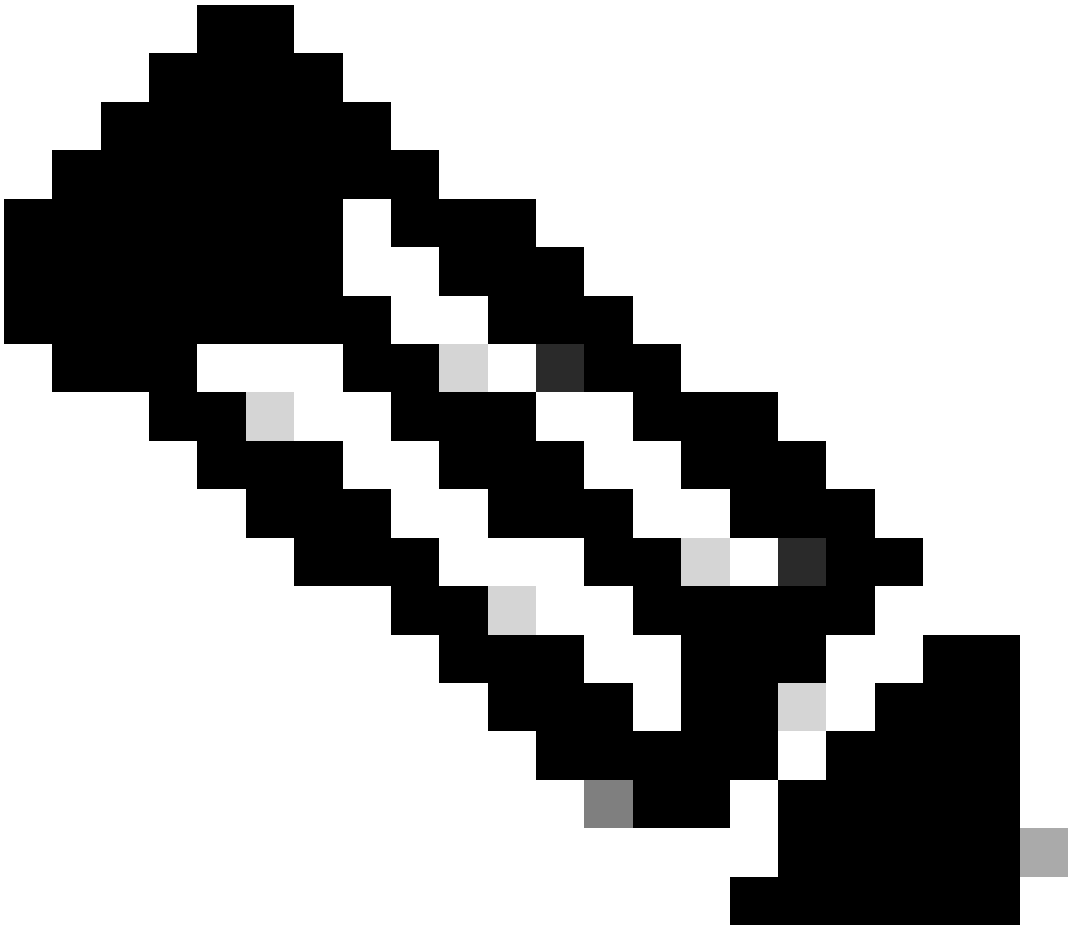
Problema 16. Não é possível editar os perfis XML do Perfil de Cliente Seguro no ASDM

Os perfis XML do Secure Client Profile na configuração do ASDM > Remote Access VPN > Network (Client) Access não poderão ser editados em um dispositivo ASA se houver uma imagem do AnyConnect presente no disco que seja anterior à versão 4.8.

A mensagem de erro "There is no profile editor plugin in your Secure Client Image on the device. Acesse Network (Client) Access > Secure Client Software e instale a Secure Client Image versão 2.5 ou posterior e tente novamente" é mostrado.

Solução de problemas - Ações recomendadas

Consulte o bug do software Cisco ID CSCwk64399 "ASDM- Unable to edit Secure Client Profile" (O ASDM não pode editar o perfil de cliente seguro). A solução é definir outra imagem do AnyConnect com uma prioridade mais baixa.



Note: Esse defeito foi corrigido em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

Problema 17. As imagens do Secure Client estão ausentes após as alterações de configuração

Depois de fazer alterações na Configuração do ASDM > Acesso à Rede (Cliente) > Perfil do Cliente Seguro, as imagens em Configuração > Acesso à Rede (Cliente) > Software do Cliente Seguro estão ausentes.

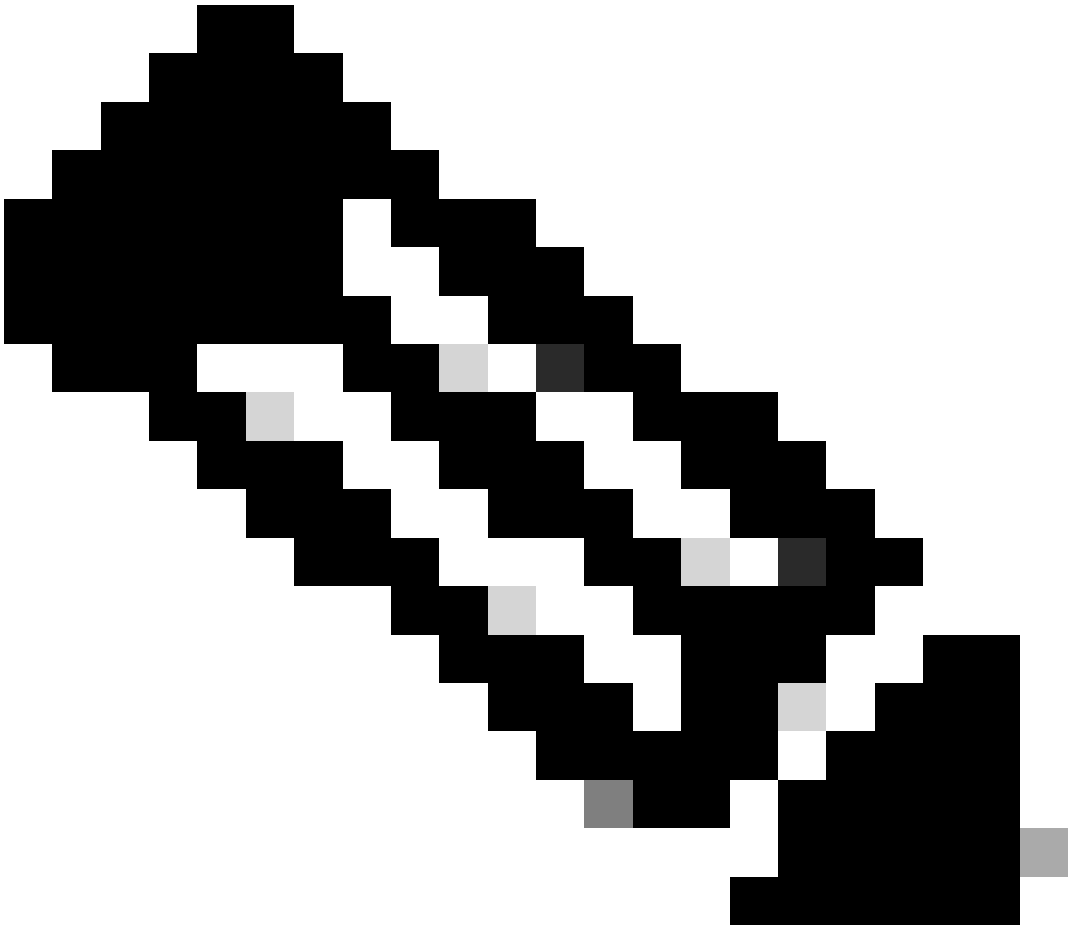
Solução de problemas - Ações recomendadas

Consulte o bug da Cisco ID do software CSCwf23826 "Secure Client Software is not displayed after modify the Secure Client Profile Editor in ASDM" (O software do cliente seguro não é exibido após a modificação do Secure Client Profile Editor no ASDM). As opções de solução:

- Clique no ícone Atualizar no ASDM

Ou

- Fechar e reabrir o ASDM



Note: Esse defeito foi corrigido em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

Problema 18. Comandos http server session-timeout e http server idle-timeout

ineficazes

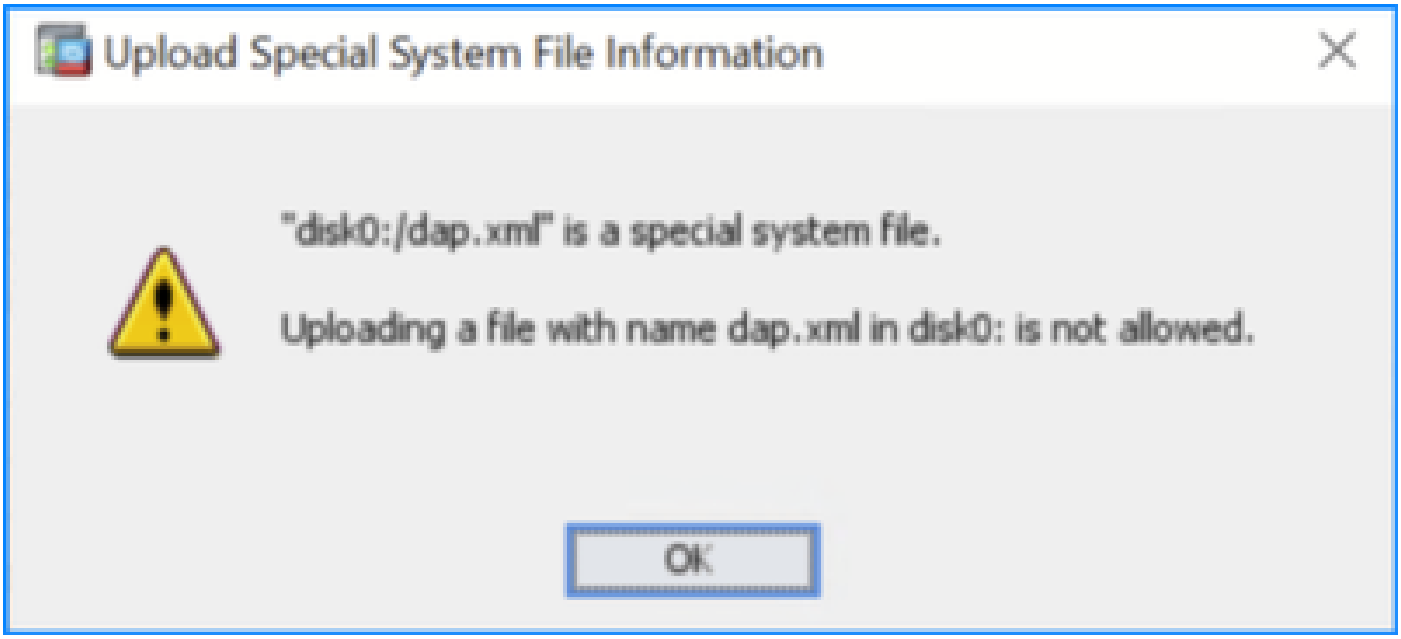
Os comandos http server session-timeout e http server idle-timeout não têm efeito no modo de contexto múltiplo ASA.

Solução de problemas - Ações recomendadas

Consulte o bug da Cisco ID do software CSCtx41707 "Support for http server timeout command in multi-context mode". Os comandos são configuráveis, mas os valores não têm efeito.

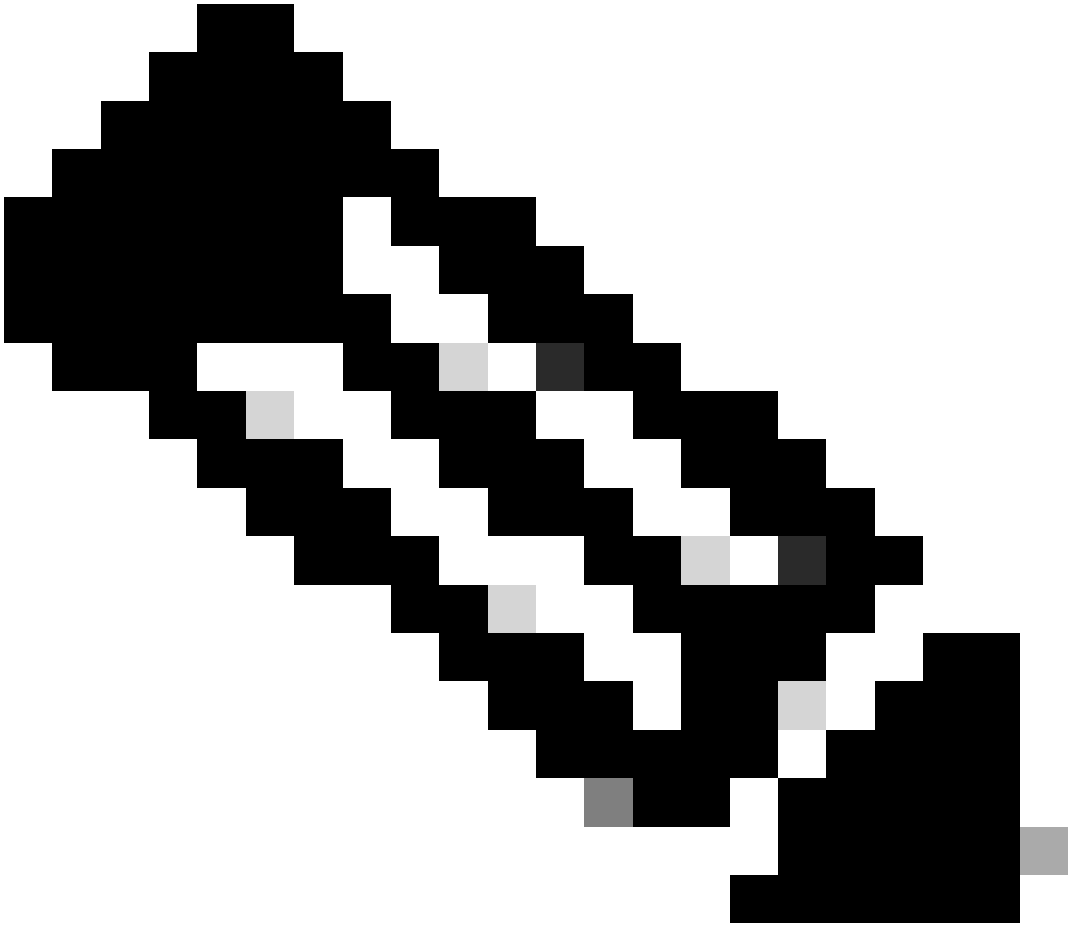
Problema 19. Falha de cópia Dap.xml no ASDM

A cópia do dap.xml para o ASA através da janela de gerenciamento de arquivos no ASDM falha com o erro "disk0:/dap.xml é um arquivo de sistema especial. Carregando um arquivo com o nome dap.xml em disk0: não é permitido":



Solução de problemas - Ações recomendadas

Consulte o bug da Cisco ID do software CSCvt62162 "Cannot copy dap.xml using File Management in ASDM 7.13.1". A solução alternativa é copiar o arquivo diretamente para o ASA usando protocolos como FTP ou TFTP.



Note: Esse defeito foi corrigido em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

Problema 20. Não há políticas IKE e propostas IPSEC visíveis no ASDM

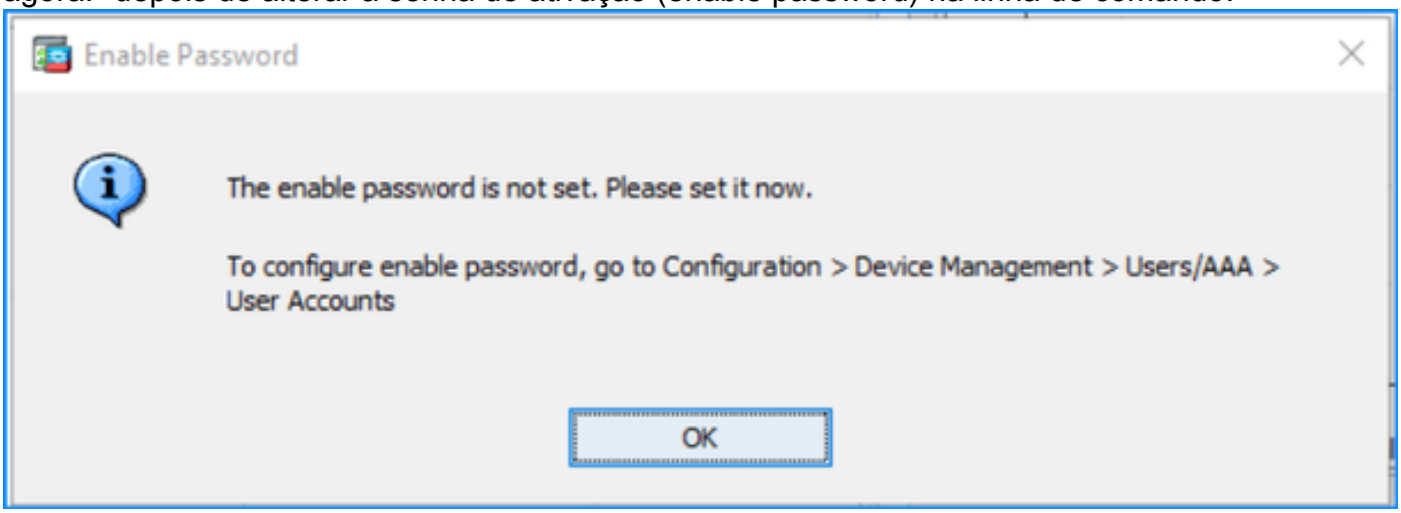
O ASDM não exibe políticas IKE e propostas IPSEC na janela Configurações > VPN Site a Site .

Solução de problemas - Ações recomendadas

Consulte o bug do software Cisco ID CSCwm42701 "ASDM display blank in IKE policies and IPSEC proposal tab".

Problema 21. O ASDM exibe a mensagem "A senha de ativação não está definida. Por favor, configure-o agora."

O ASDM exibe a mensagem "A senha de ativação não está definida. Por favor, configure-o agora." depois de alterar a senha de ativação (enable password) na linha de comando:



Solução de problemas - Ações recomendadas

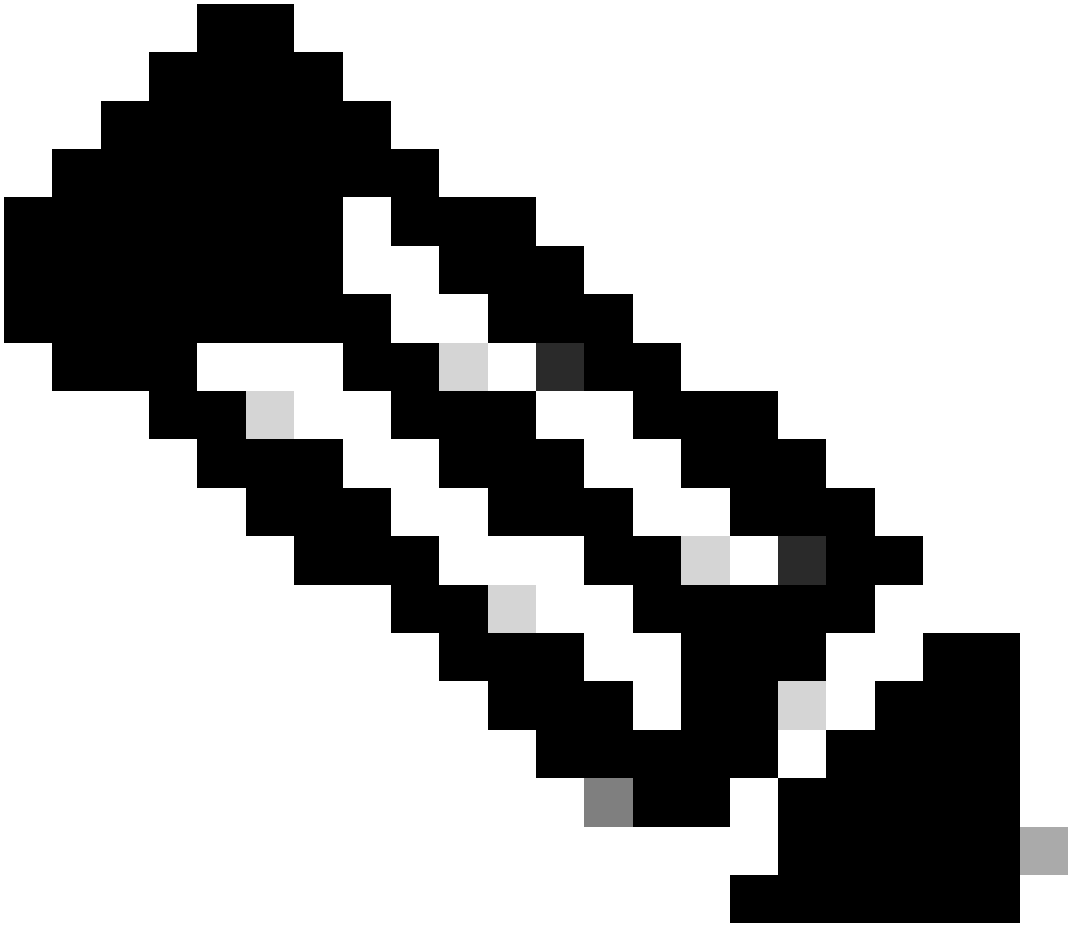
Consulte o bug do software Cisco ID CSCvq42317 "ASDM prompts to change enable password after it was set on CLI".

Problema 22. O objeto ASDN desaparece após a atualização da interface do usuário do ASDM

Ao adicionar um grupo de objetos e um host de objetos a um grupo de objetos existente e após atualizar o ASDM, o grupo de objetos desaparece da lista do ASDM. Os nomes de objeto devem começar com números para que esse defeito seja correspondente.

Solução de problemas - Ações recomendadas

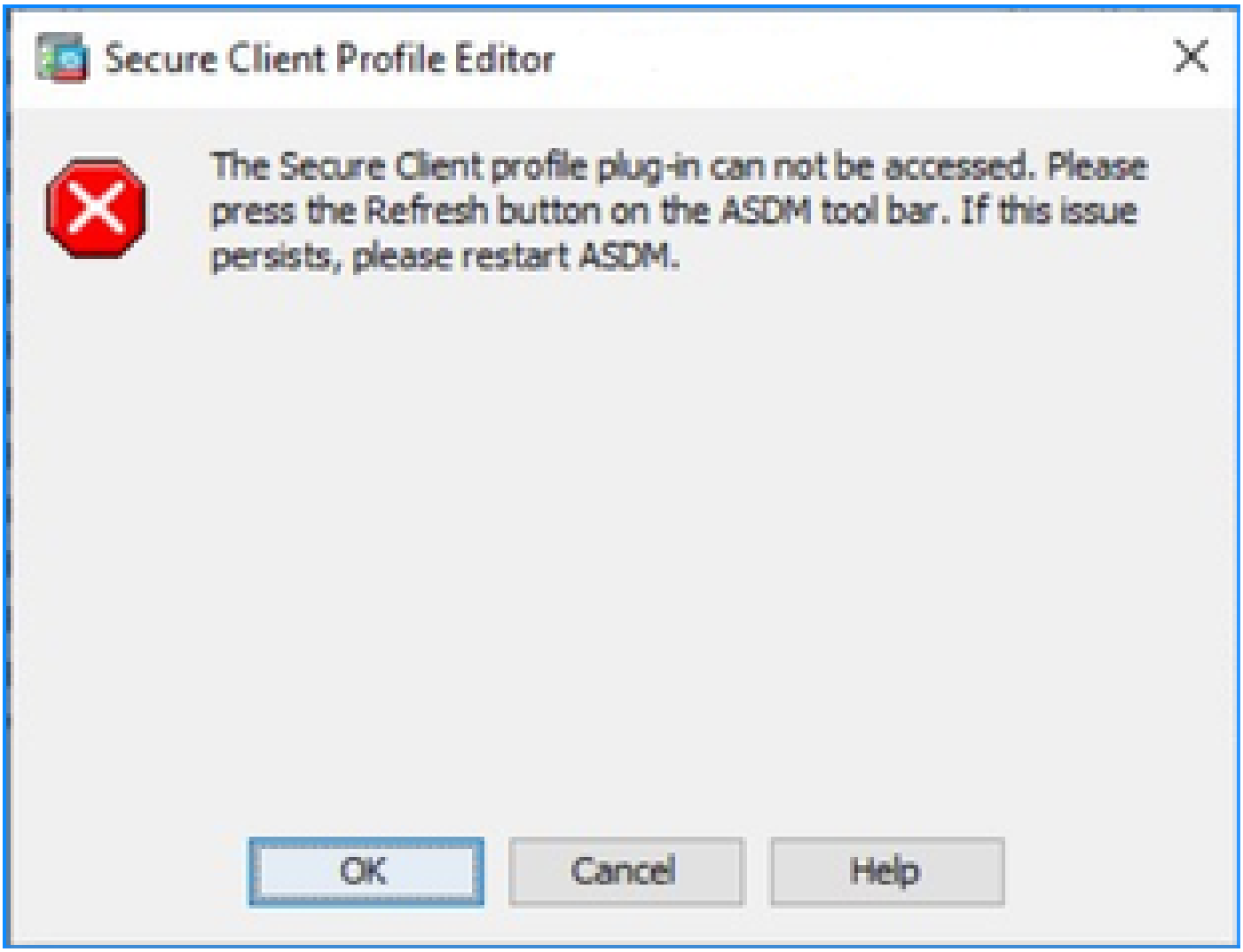
Consulte o bug do software Cisco ID CSCwf71723 "ASDM perdeu objetos/grupos de objetos configurados".



Note: Esse defeito foi corrigido em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

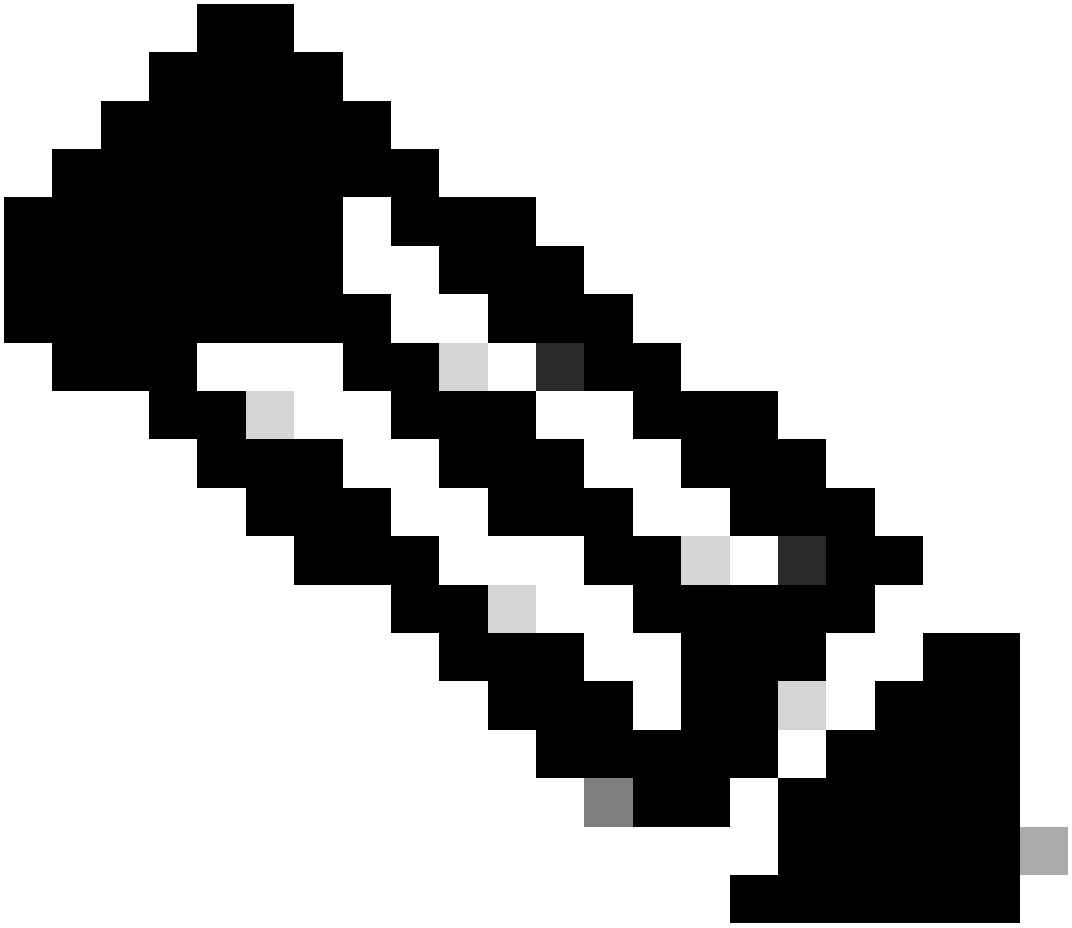
Problema 23. Não é possível editar perfis de cliente do AnyConnect para versões anteriores à 4.5

Os perfis do cliente AnyConnect não podem ser editados para o Perfil do AnyConnect anterior à versão 4.5. A mensagem de erro é "O plug-in do perfil do Secure Client não pode ser acessado. Pressione o botão Atualizar na barra de ferramentas do ASDM. Se o problema persistir, reinicie o ASDM.":



Solução de problemas - Ações recomendadas

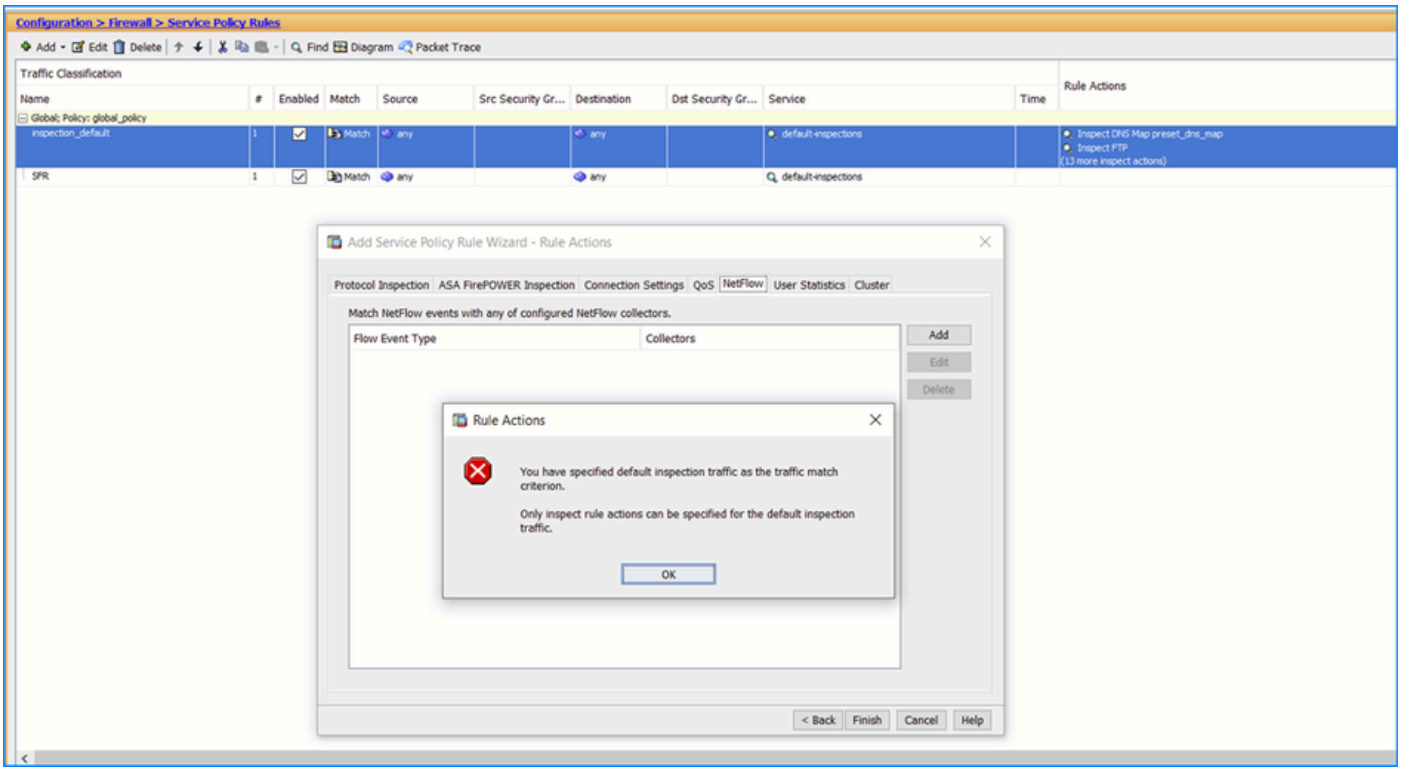
Consulte o bug da Cisco ID do software CSCwf16947 "ASDM - Unable to load Anyconnect Profile Editor".



Note: Esse defeito foi corrigido em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

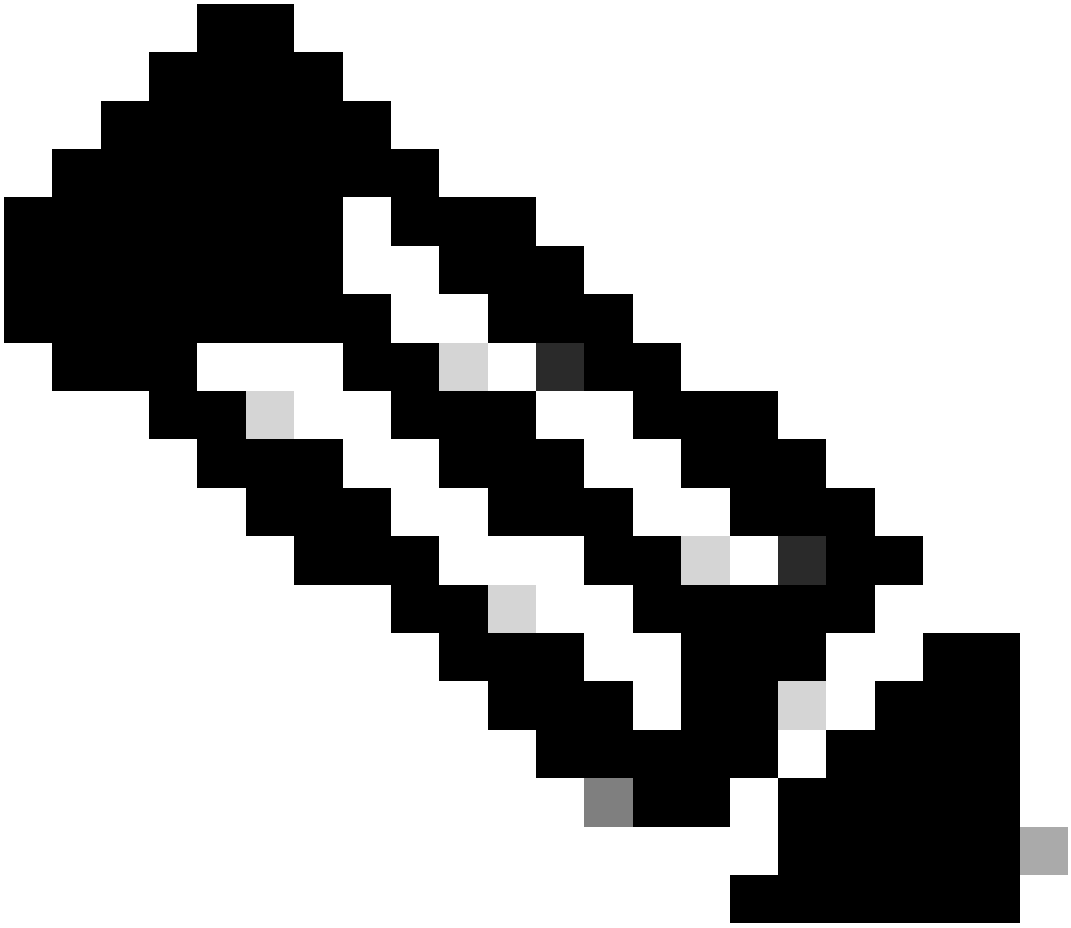
Problema 24. Não é possível navegar até a guia Edit Service Policy > Rule Actions > ASA FirePOWER Inspection.

No ASDM versão 7.8.2, os usuários não podem navegar para a guia Edit Service Policy > Rule Actions > ASA FirePOWER Inspection e o erro é exibido: "Você especificou o tráfego de inspeção padrão como o critério de correspondência de tráfego. Somente ações de regra de inspeção podem ser especificadas para o tráfego de inspeção padrão." Isso ocorre mesmo quando uma ACL foi selecionada para redirecionamento:



Solução de problemas - Ações recomendadas

Consulte o bug da Cisco ID do software CSCvg15782 "ASDM - Unable to view modify SFR traffic redirection after upgrade to version 7.8(2)" (O ASDM não consegue visualizar a modificação do redirecionamento de tráfego SFR após a atualização para a versão 7.8(2))). A solução é usar a CLI para editar a configuração do mapa de políticas.



Note: Esse defeito foi corrigido em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

Problema 25. Imagem do AnyConnect versão 5.1 e editor de perfil do AnyConnect no ASDM

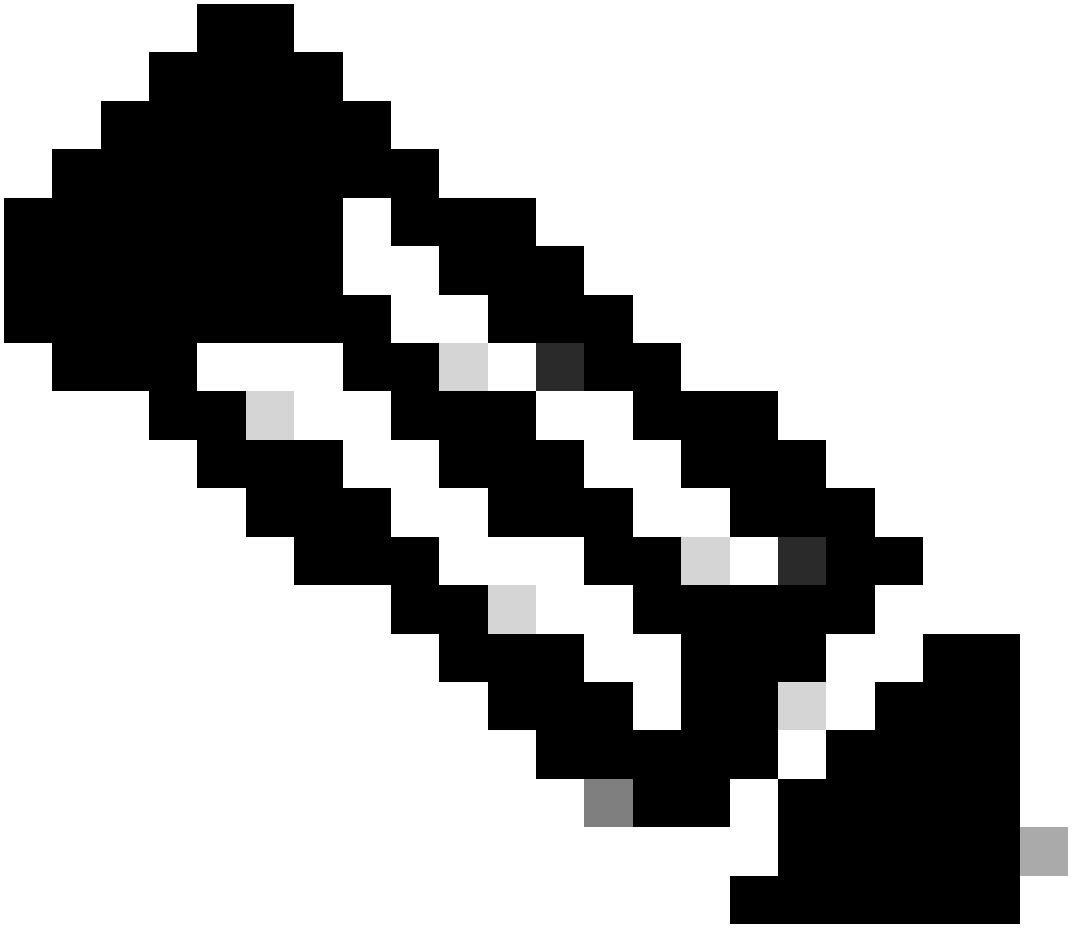
Estes sintomas são observados para o software Secure Client versão 5.1:

1. Os nomes de módulo de política de grupo não listados ao carregar os pacotes Win/Mac/Linux
2. O ASDM não consegue abrir o AnyConnect Profile Editor.

Solução de problemas - Ações recomendadas

Consulte o bug do software Cisco ID CSCwh74417 "ASDM : O Editor de perfis e a Diretiva de

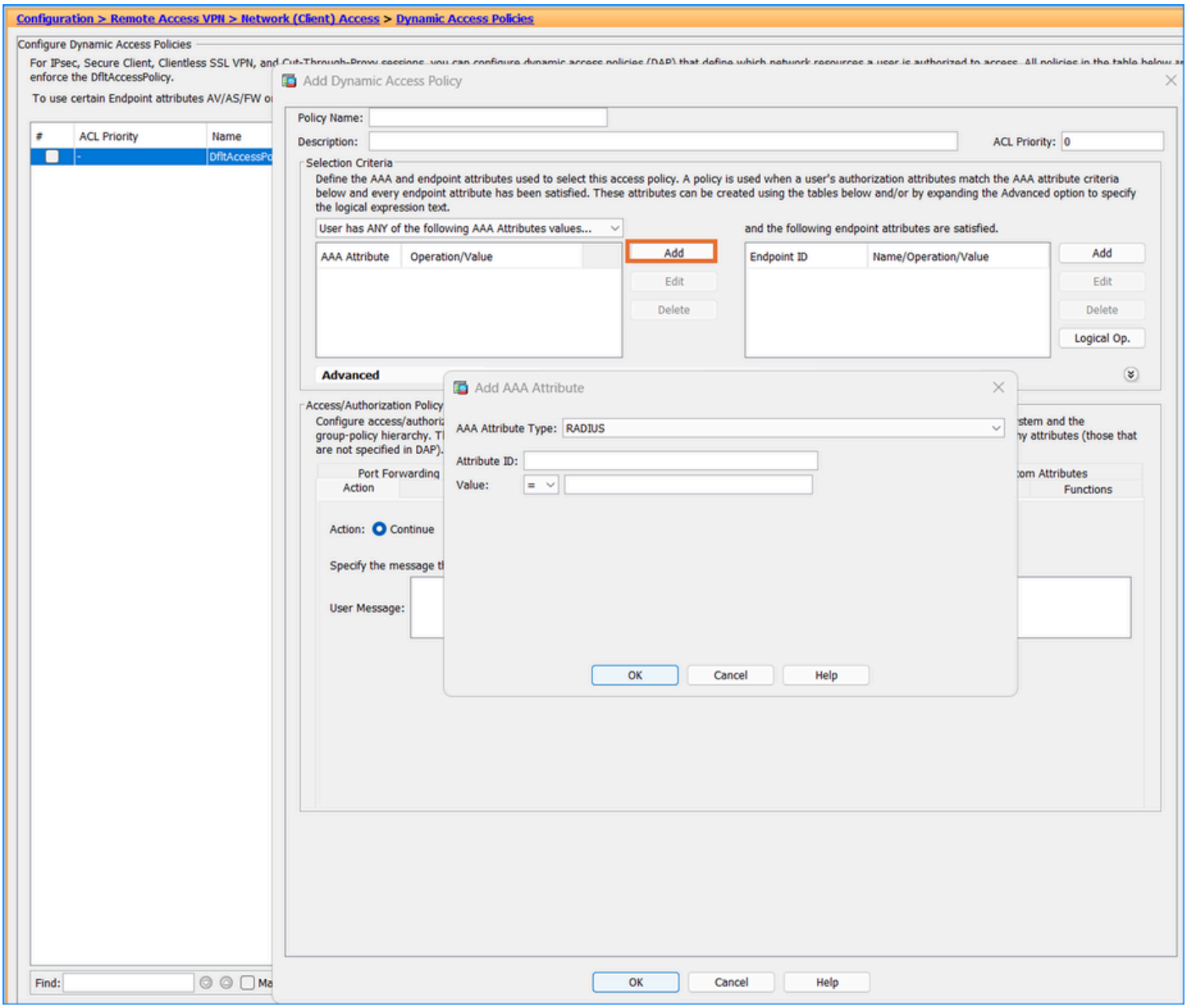
grupo do AnyConnect não podem ser carregados ao usar a imagem CSC 5.1". A solução é usar versões anteriores do Secure Client.



Note: Esse defeito foi corrigido em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

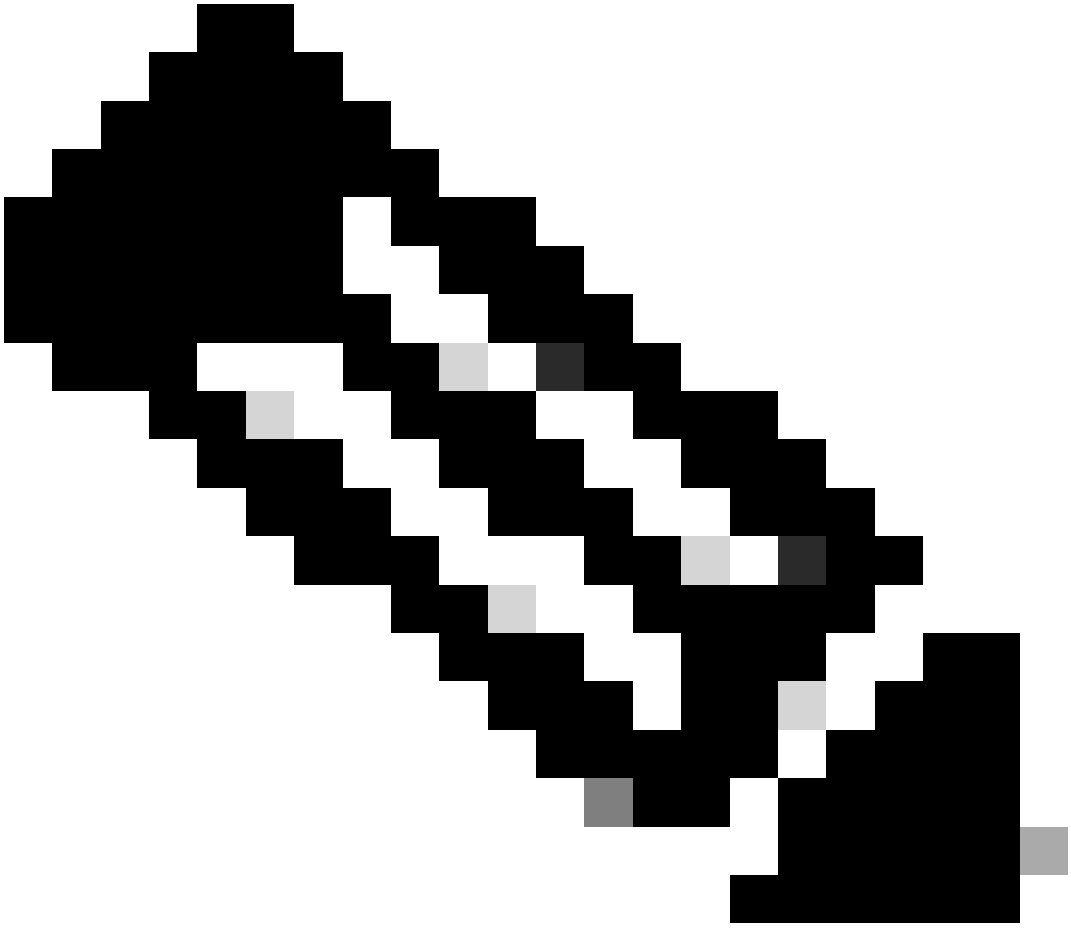
Problema 26. O tipo de atributos AAA (Radius/LDAP) não é visível no ASDM

Os Atributos de AAA (Radius/LDAP) não estão visíveis no ASDM > Configuração > VPN de Acesso Remoto > Acesso à Rede (Cliente) > Políticas de Acesso Dinâmico > Adicionar > No campo de atributo AAA > Adicionar > Selecionar Radius ou LDAP:



Solução de problemas - Ações recomendadas

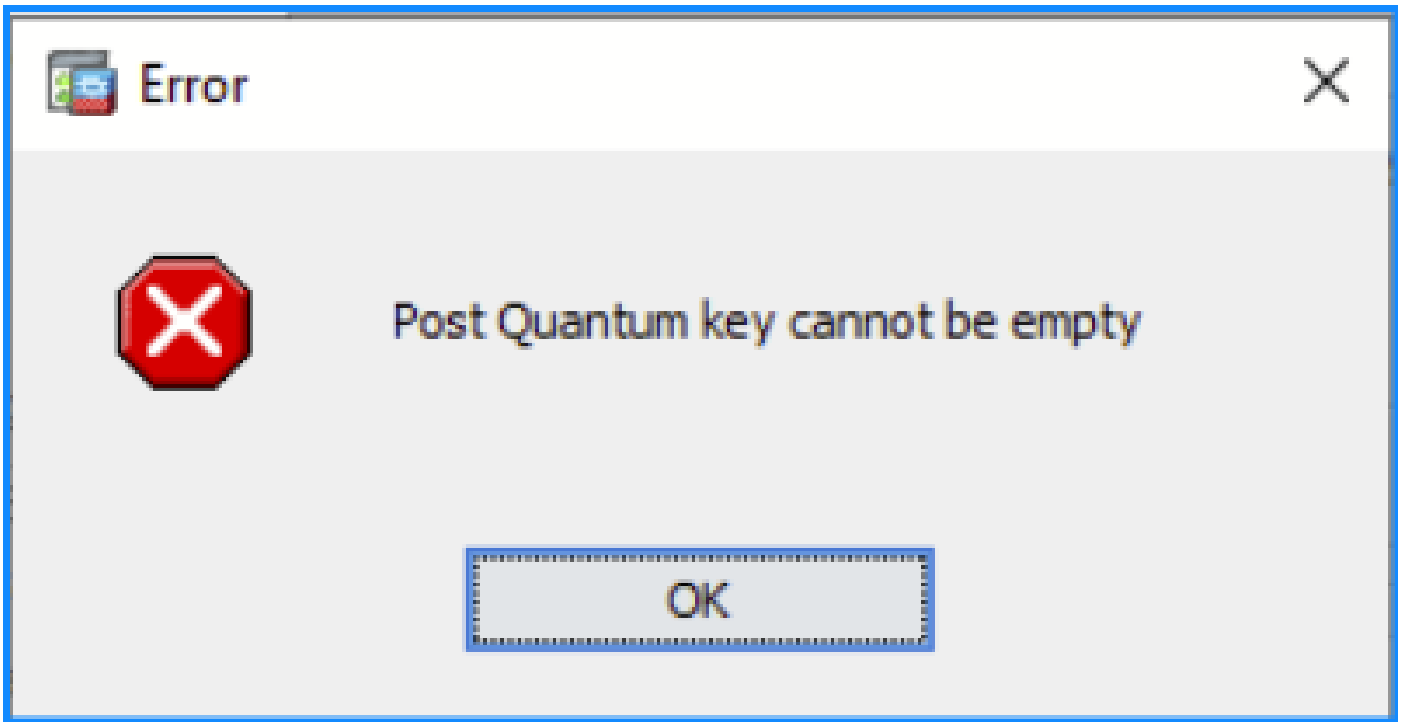
Consulte o bug do software Cisco ID CSCwa9370 "ASDM : ASDM:DAP config missing AAA Attributes type (Radius/LDAP)" e ID de bug da Cisco CSCwd16386 "ASDM:DAP config missing AAA Attributes type (Radius/LDAP)".



Note: Esses defeitos foram corrigidos em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

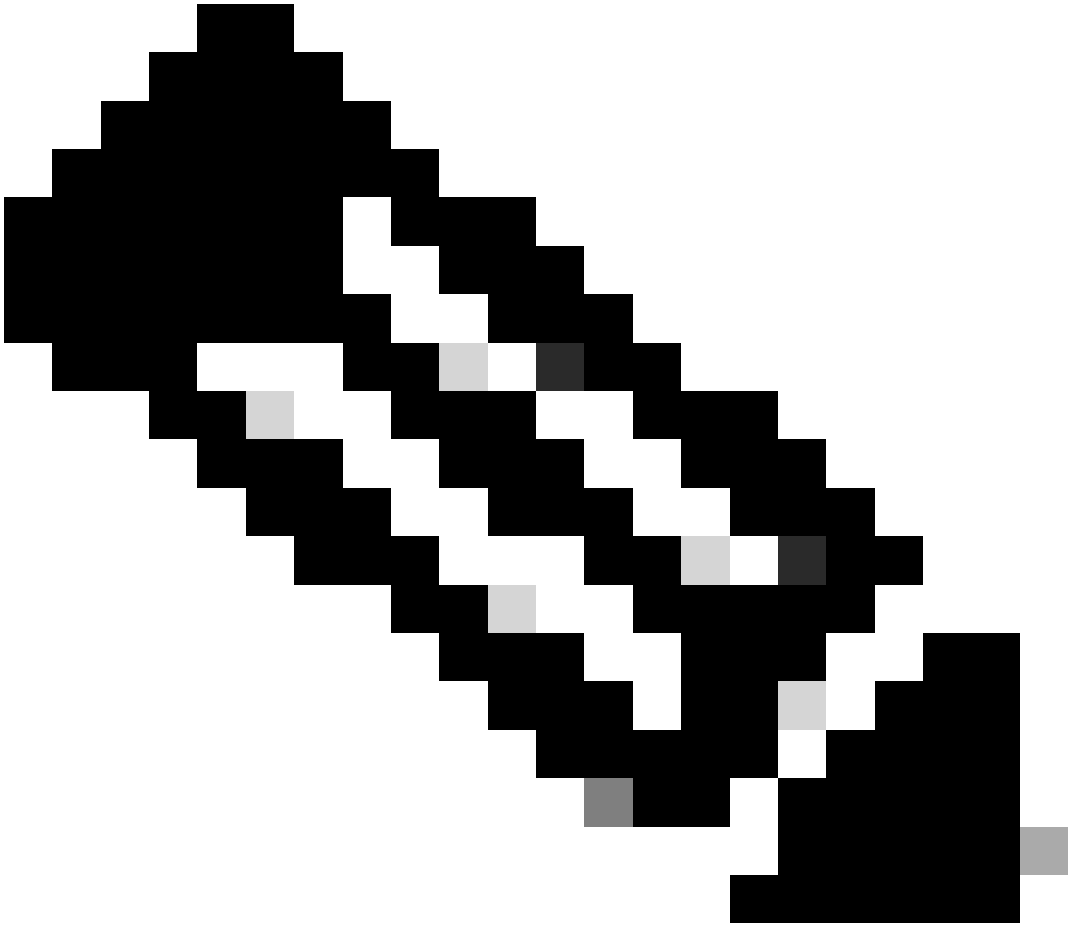
Problema 27. O erro 'Post Quantum key cannot be empty' é mostrado no ASDM

O erro 'Post Quantum key cannot be empty' é mostrado ao editar a seção Advanced em ASDM > Configuration > Remote Access VPN > Network (Client) Access > IPsec (IKEv2) Connection Profiles':



Solução de problemas - Ações recomendadas

Consulte o bug da Cisco ID do software CSCwe58266 "Configuração ASDM IKev2 - Mensagem de erro Post Quantum Key cannot be empty".



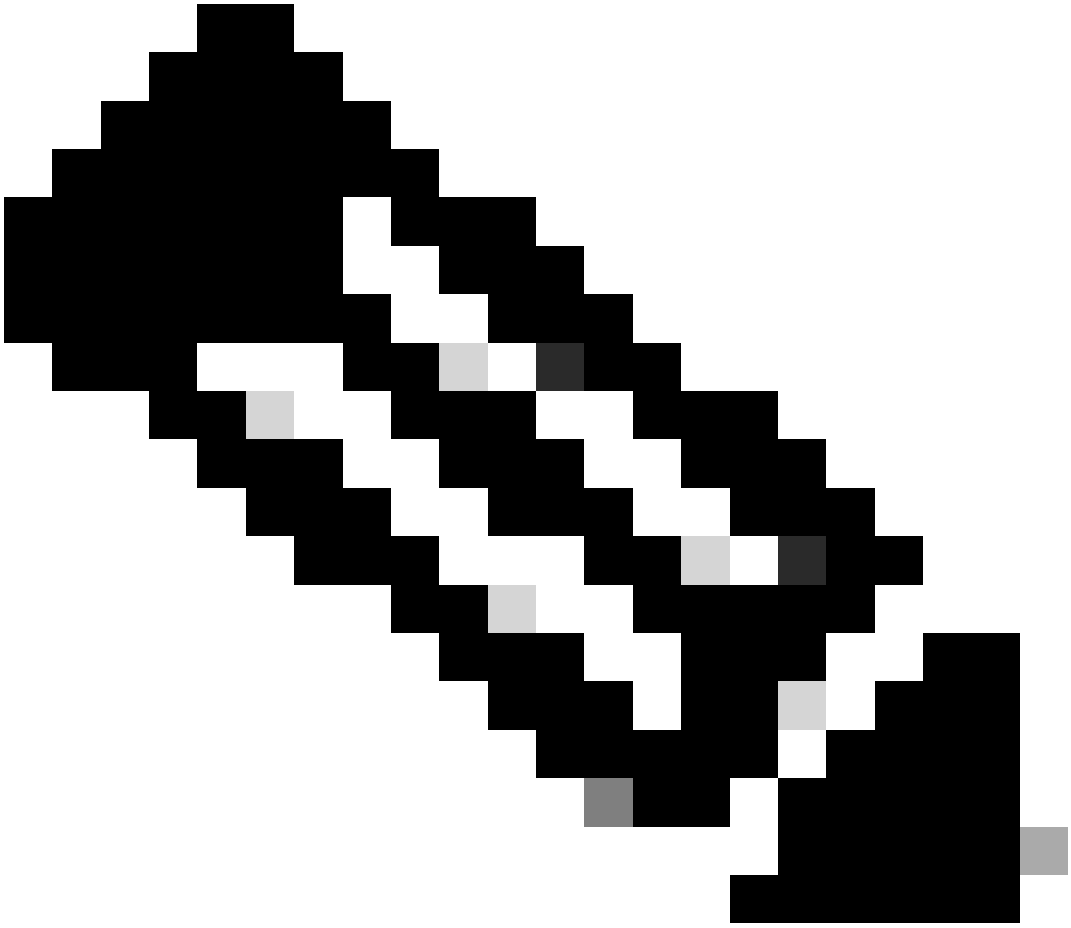
Note: Esse defeito foi corrigido em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

Problema 28. O ASDM não exibe nenhum resultado ao usar a opção "onde usado"

O ASDM não exibe nenhum resultado ao usar a opção "onde usado" encontrada ao navegar para Configuração > Firewall > Objetos > Objetos de rede/Grupos e clicar com o botão direito do mouse em um Objeto.

Solução de problemas - Ações recomendadas

Consulte o bug do software Cisco ID CSCwd98702 opção "Onde usado" em ASDM não está funcionando.



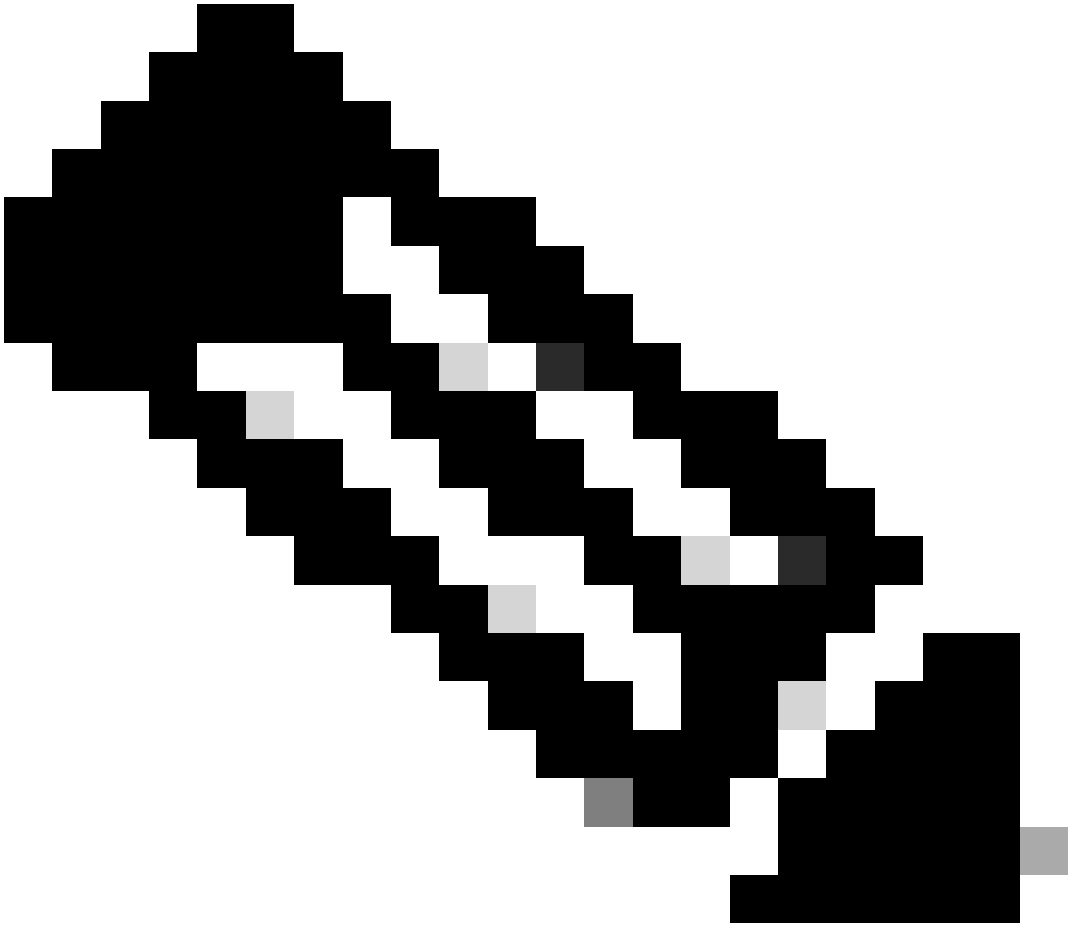
Note: Esse defeito foi corrigido em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

Problema 29. Mensagem de aviso "[Network Object] cannot be deleted porque it is used in the following" ao excluir um objeto de rede

O ASDM não exibe a mensagem de aviso "[Network Object] cannot be deleted because it is used in the following" when deleting a network object that is referenced in a network group in Configuration > Firewall > Objects > Network Objects/Groups.

Solução de problemas - Ações recomendadas

Consulte o bug da Cisco ID de software CSCwe67056 "[Network Object] cannot be deleted because it is used in the following" warning not appear" (O [objeto de rede] não pode ser excluído porque é usado no seguinte aviso).



Note: Esse defeito foi corrigido em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

Problema 30. Problemas de usabilidade com a guia Network Objects/Group no ASDM

Um ou mais destes sintomas são observados:

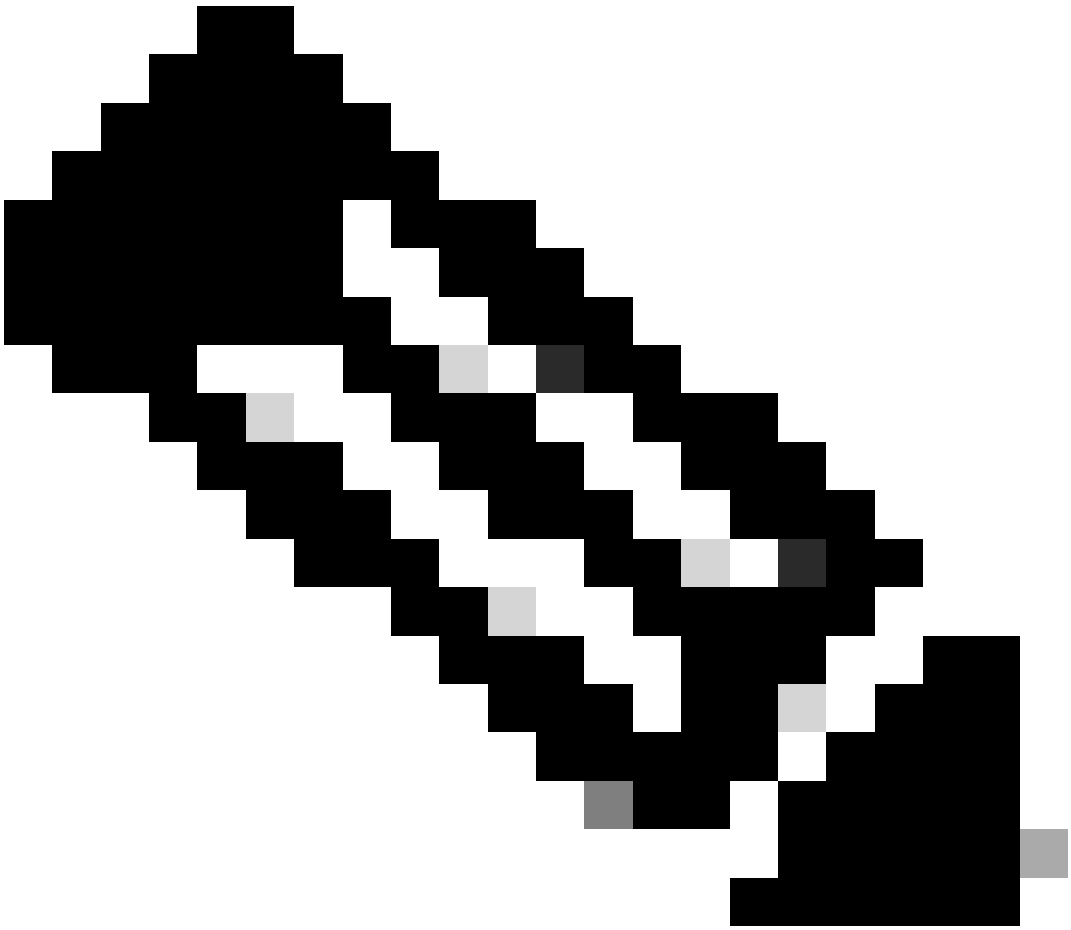
- A entrada de texto "Name" na seção "Create new Object Member" das janelas "Add/Edit Object Group" é marcada como "optional". No entanto, o botão "Adicionar**>>**" para criar e adicionar o objeto fica desativado, a menos que um nome seja inserido.
- A guia "Usos" que é aberta quando um usuário clica no botão "Onde usado..." o menu de contexto lista apenas as entidades (ACLs, mapas de rotas, grupos de objetos) que fazem referência direta ao objeto. Ele também deve listar recursivamente segundo, terceiro e assim por diante. as referências de ordem (ou seja, uma ACL que usa um grupo de objetos que contém um objeto também devem ser listadas como "uso" do Objeto).

- A operação "Excluir" disponível no menu de contexto também exibe esse comportamento. Exclui automaticamente qualquer entidade que faça referência direta ao objeto (se a entidade ficar vazia quando o objeto for excluído). Ela não funciona dessa maneira quando há um segundo, um terceiro, e assim por diante. a referência de ordem ficaria vazia devido à exclusão do objeto e da primeira referência de ordem.

O usuário pode ser levado a acreditar que o ASDM evita entidades que ficariam vazias devido à exclusão do objeto do restante na configuração. No entanto, não é necessariamente o caso.

Solução de problemas - Ações recomendadas

Consulte o bug do software Cisco ID CSCwe86257 "Usability of Network Objects/Group Tab in ASDM".

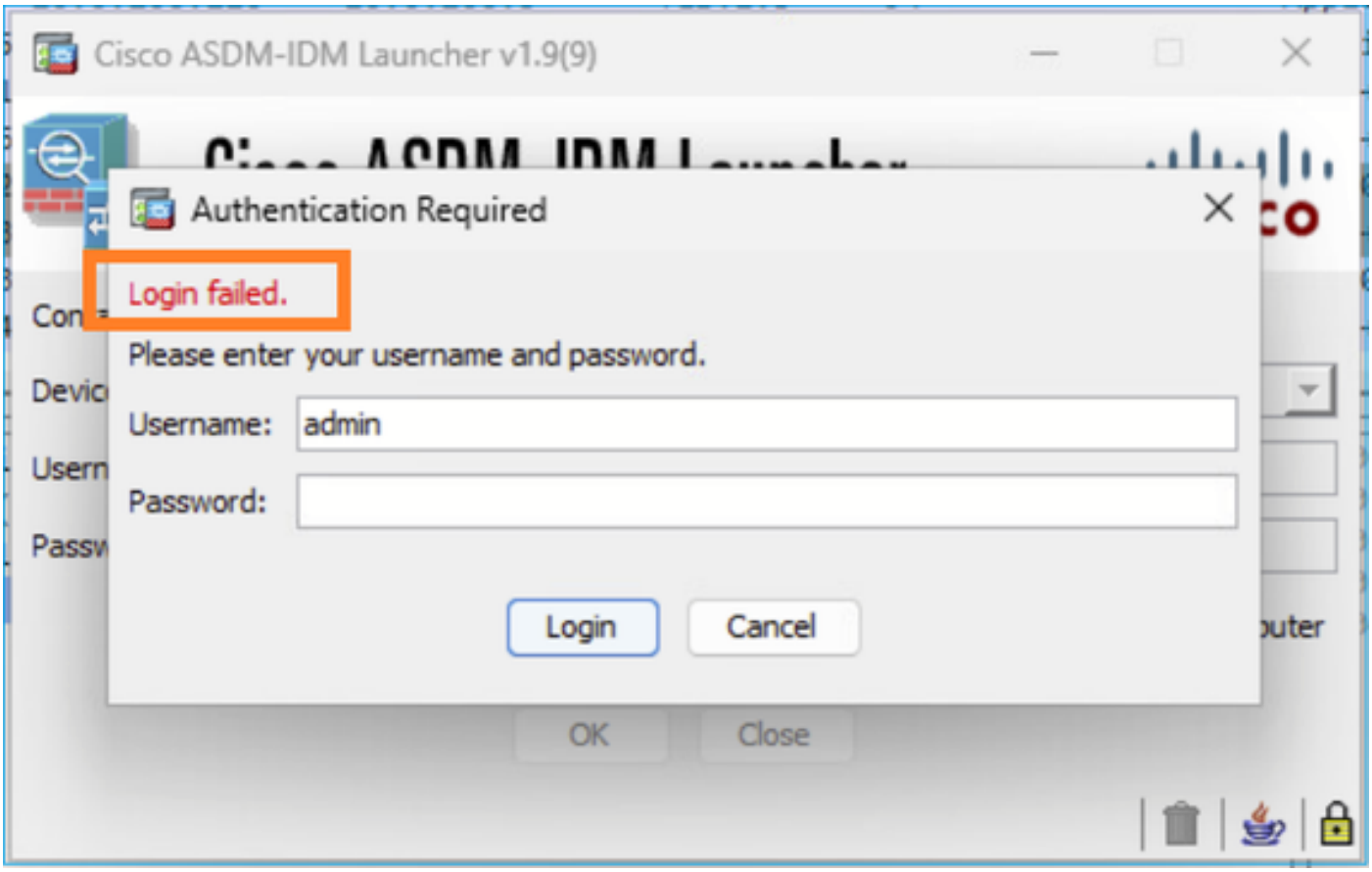


Note: Esse defeito foi corrigido em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

Identificar e Solucionar Problemas de Autenticação do ASDM

Problema 1. Falha no Login no ASDM

O erro mostrado na interface do usuário do ASDM é:



Solução de problemas - Ações recomendadas

Esse erro pode ser visto quando você tem o HTTP e o WebVPN Cisco Secure Client (AnyConnect) habilitados na mesma interface. Assim, todas as condições devem ser atendidas:

1. O AnyConnect/Cisco Secure Client está ativado em uma interface
2. O servidor HTTP é ativado na mesma interface e na mesma porta que o AnyConnect/Cisco Secure Client

Exemplo:

<#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
```

Dica de solução de problemas: Habilite 'debug http 255' e você poderá ver o conflito entre ASDM e Webvpn:

```
<#root>
ciscoasa#
debug http 255

debug http enabled at level 255.
ciscoasa# ewaURLHookVCARedirect
...addr: 192.0.2.5
ewaURLHookHTTPRedirect: url = /+webvpn+/index.html
HTTP: ASDM request detected [ASDM/] for [/+webvpn+/index.html]   <--------

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

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

Como observação adicional, apesar da falha de login, os syslogs ASA mostram que a autenticação é bem-sucedida:

```
<#root>
asa#
```

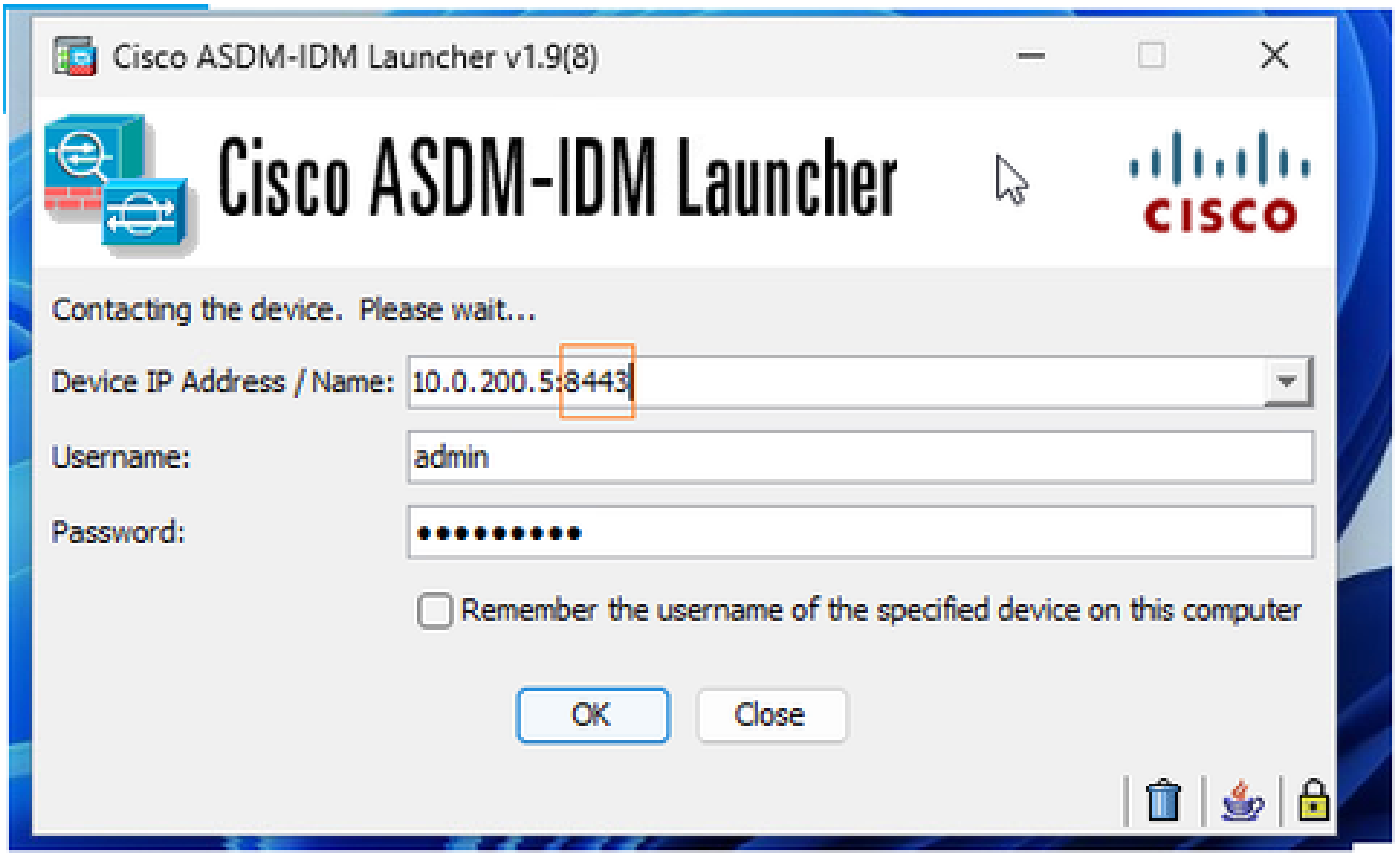
```
show logging

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
```

Soluções

Solução 1

Altere a porta TCP do servidor ASA HTTP, por exemplo:

```
<#root>

ciscoasa#

configure terminal


ciscoasa(config)#

http server enable 8443
```



Solução 2

Altere a porta TCP para o AnyConnect/Cisco Secure Client, por exemplo:

<#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
```

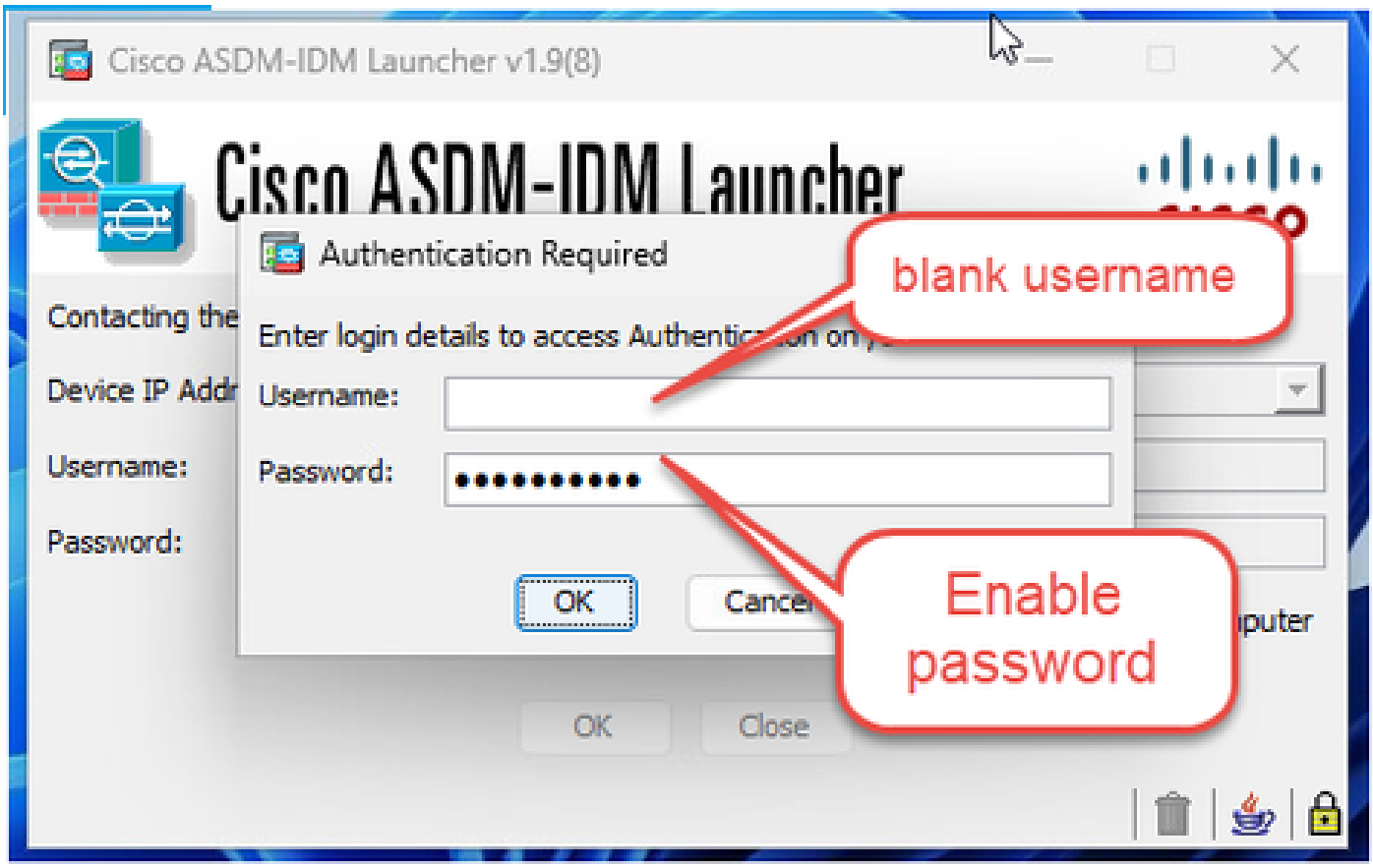
Solução 3

Uma solução alternativa é remover a configuração "aaa authentication http console":

<#root>

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

Nesse caso, você pode fazer login no ASDM usando apenas a senha de ativação:



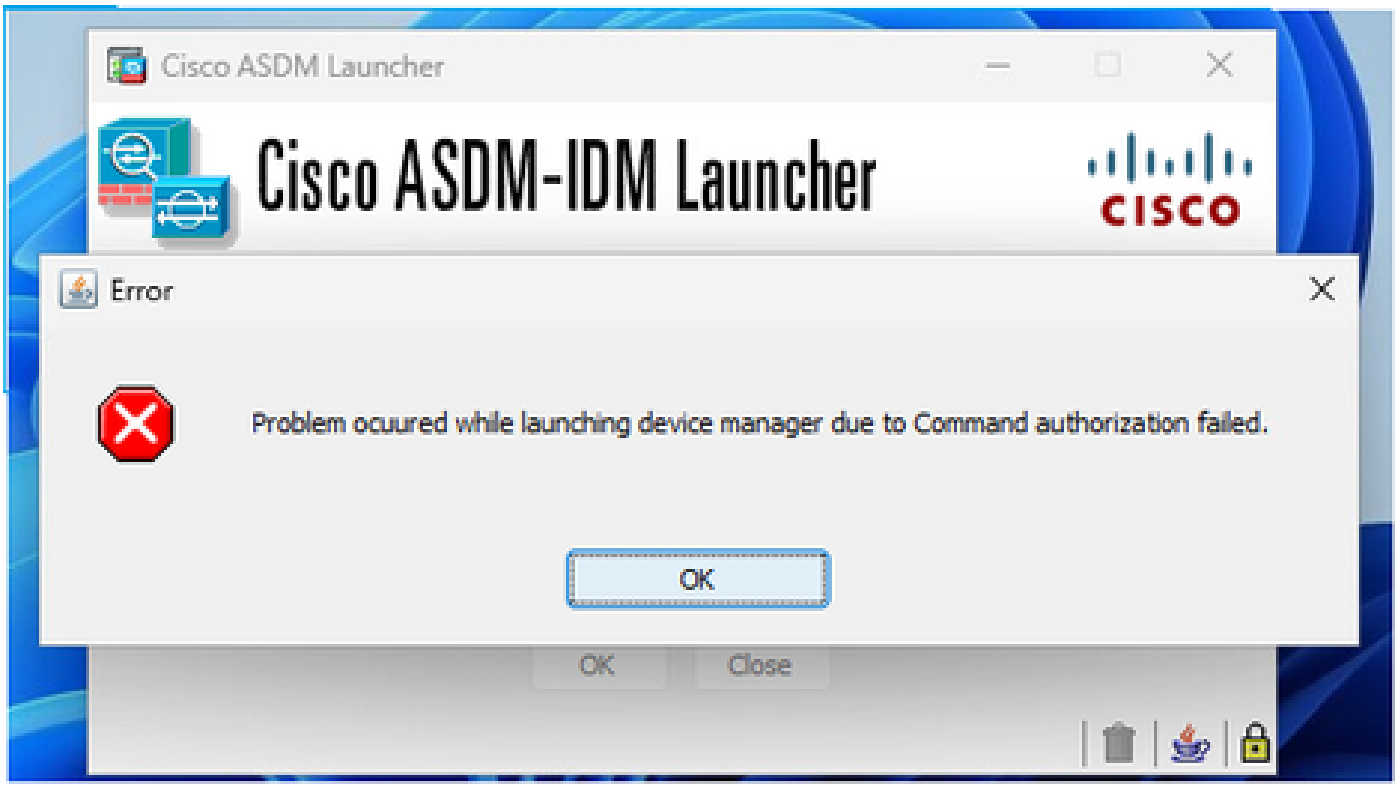
Defeito relacionado

ID de bug da Cisco CSCwb67583

Adicionar aviso quando webvpn e ASDM estiverem habilitados na mesma interface

Problema 2. Falha na autorização do Comando ASDM

O erro mostrado na interface do usuário do ASDM é:



Solução de problemas - Etapas recomendadas

Verifique sua configuração AAA no ASA e certifique-se de que:

- Você também tem a autenticação aaa configurada.
- Se você usar um servidor de autenticação remoto, ele estará acessível e autorizará os comandos.

Referência

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

Problema 3. Configurar o acesso somente leitura do ASDM

Às vezes, você deseja fornecer acesso somente leitura aos usuários do ASDM.

Solução de problemas - Etapas recomendadas

Crie um novo usuário com um nível de privilégio personalizado (5), por exemplo:

<#root>

```
asa(config)#
```

username [username] password [password] privilege 5

Esse comando cria um usuário com um nível de privilégio 5, que é o nível "somente monitoramento". Substitua `[username]` e `[password]` pelo nome de usuário e senha desejados.

Detalhes

A autorização de comandos locais permite atribuir comandos a um dos 16 níveis de privilégio (0 a 15). Por default, cada comando é atribuído ao nível de privilégio 0 ou 15. Você pode definir cada usuário para estar em um nível de privilégio específico, e cada usuário pode inserir qualquer comando no nível de privilégio atribuído ou menos. O ASA suporta níveis de privilégio de usuário definidos no banco de dados local, um servidor RADIUS ou um servidor LDAP (se você mapear atributos LDAP para atributos RADIUS).

Procedimento

Passo 1	Selecione Configuration > Device Management > Users/AAA > AAA Access > Authorization.
Passo 2	Marque a caixa de seleção Enable authorization for ASA command access > Enable.
Etapa 3	Escolha LOCAL na lista suspensa Grupo de servidores.
Passo 4	Ao habilitar a autorização de comando local, você tem a opção de atribuir manualmente níveis de privilégio a comandos individuais ou grupos de comandos ou habilitar os privilégios de conta de usuário predefinidos. · Clique em Definir Funções de Usuário Definidas pelo ASDM para usar privilégios de conta de usuário predefinidos. A caixa de diálogo Configuração de Funções de Usuário Definidas pelo ASDM é exibida. Clique em Sim para usar os privilégios de conta de usuário predefinidos: Admin (nível de privilégio 15, com acesso total a todos os comandos CLI; Somente Leitura (nível de privilégio 5, com acesso somente leitura); e Monitor Only (nível de privilégio 3, com acesso apenas à seção Monitoring). · Clique em Configurar privilégios de comando para configurar manualmente os níveis de comando. A caixa de diálogo Command Privileges Setup é exibida. Você pode visualizar todos os comandos escolhendo Todos os modos na lista suspensa Modo de comando ou pode escolher um modo de configuração para visualizar os comandos disponíveis nesse modo. Por exemplo, se você escolher contexto, poderá exibir todos os comandos disponíveis no modo de configuração de contexto. Se um comando puder ser inserido no modo EXEC do usuário ou no modo EXEC privilegiado, bem como no modo de configuração, e o comando executar ações diferentes em cada modo, você poderá

	definir o nível de privilégio para esses modos separadamente. A coluna Variant exibe show, clear ou cmd. Você pode definir o privilégio apenas para a forma show, clear ou configure do comando. A forma de configuração do comando é geralmente a forma que causa uma alteração de configuração, seja como o comando não modificado (sem o prefixo show ou clear) ou como a forma no. Para alterar o nível de um comando, clique duas vezes nele ou clique em Editar. Você pode definir o nível entre 0 e 15. Você só pode configurar o nível de privilégio do comando principal. Por exemplo, você pode configurar o nível de todos os comandos aaa, mas não o nível dos comandos aaa authentication e aaa authorization separadamente. Para alterar o nível de todos os comandos exibidos, clique em Selecionar tudo e em Editar. Clique em OK para aceitar suas alterações.
Etapa 5	Clique em Apply. As configurações de autorização são atribuídas e as alterações são salvas na configuração atual.

Referência

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

Problema 4. Autenticação Multifator (MFA) ASDM

Solução de problemas - Etapas recomendadas

No momento em que este documento foi escrito, o ASDM não suporta MFA (ou 2FA). Essa limitação inclui MFA com soluções como PingID e assim por diante.

Referência

ID de bug Cisco CSCvs85995

ENH: Acesso ASDM com autenticação de dois fatores ou MFA

Problema 5. Configuração da autenticação externa do ASDM

Solução de problemas - Etapas recomendadas

Você pode usar LDAP, RADIUS, RSA SecurID ou TACACS+ para configurar a autenticação externa no ASDM.

Referências

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

Problema 6. Falha na autenticação LOCAL do ASDM

Solução de problemas - Etapas recomendadas

Caso você use a autenticação externa e a autenticação LOCAL como um fallback, a autenticação local funcionará somente se o servidor externo estiver inativo ou não estiver funcionando. Somente nesse cenário a autenticação LOCAL assume o controle e você pode se conectar com os usuários LOCAL.

Isso ocorre porque a autenticação externa tem precedência sobre a autenticação LOCAL.

Exemplo:

<#root>

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

Referência

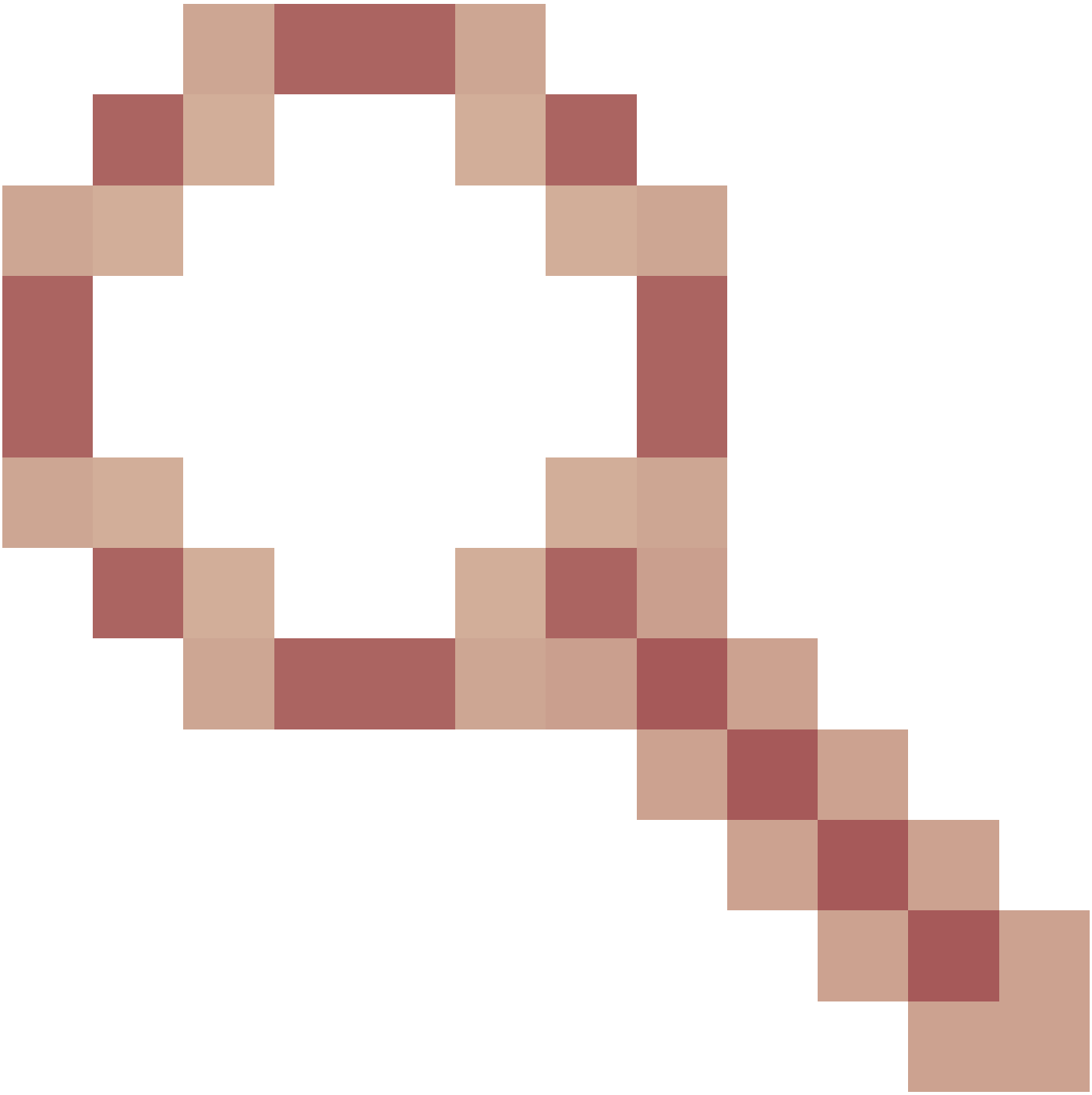
- https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/A-H/asa-command-ref-A-H/aa-ac-commands.html#wp6184732320

Problema 7. Senha de Uso Único do ASDM

Solução de problemas - Etapas recomendadas

- O suporte à autenticação ASDM OTP (senha única) foi adicionado no ASA versão 8.x - 9.x e somente no modo roteado único.
- A autenticação OTP do ASDM para o modo transparente e/ou o modo multicontexto do Firewall ASA não entra nesta categoria.

Consulte a ID de bug da Cisco CSCtf23419



ENH: Suporte à autenticação OTP do ASDM em modos multicontexto e transparente

Problema 8. O Perfil de Conexão não mostra todos os métodos

O problema nesse caso é uma incompatibilidade entre a configuração da CLI do ASA e a interface do usuário do ASDM.

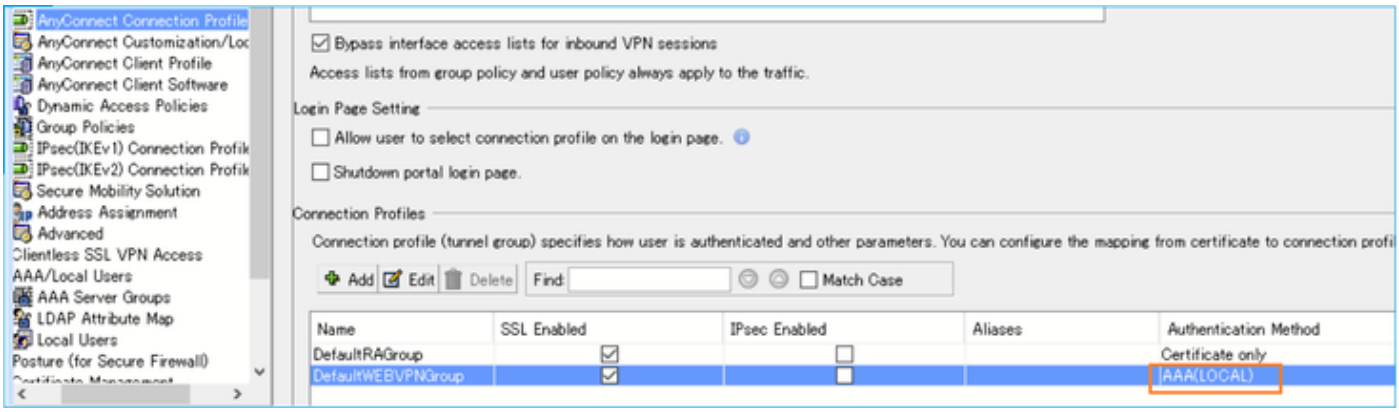
Especificamente, o CLI tem:

<#root>

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

```
 authentication aaa certificate
```

Embora a interface do usuário do ASDM não mencione o método de certificado:



Solução de problemas - Etapas recomendadas

Isso é considerado um problema de aparência. O método não está aparecendo no ASDM, mas a autenticação de certificado é usada.

Problema 9. A Sessão ASDM não Expira

O sintoma é que o timeout de sessão da GUI do ASDM não é levado em conta.

Solução de problemas - Etapas recomendadas

Isso ocorre quando o comando "aaa authentication http console LOCAL" não é definido no ASA gerenciado.

Consulte a ID de bug da Cisco CSCwj70826

ENH: adicionar um aviso: definir o tempo limite da sessão, requer "aaa authentication http console LOCAL"

Solução

Configure o comando "aaa authentication http console LOCAL" no ASA gerenciado.

Problema 10. Falha na autenticação LDAP do ASDM

Solução de problemas - Etapas recomendadas

Passo 1

Certifique-se de que a configuração esteja em vigor, por exemplo:

<#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

Passo 2

Verifique o status do servidor LDAP:

<#root>

```
asa#
```

show aaa-server

Bom cenário:

<#root>

```
Server status:
```

ACTIVE

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

Cenário ruim:

<#root>

```
Server status:
```

FAILED

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

Etapa 3

Verifique se a autenticação LOCAL funciona corretamente, desabilitando temporariamente a autenticação LDAP.

Passo 4

No ASA, execute depurações LDAP e tente autenticar o usuário:

<#root>

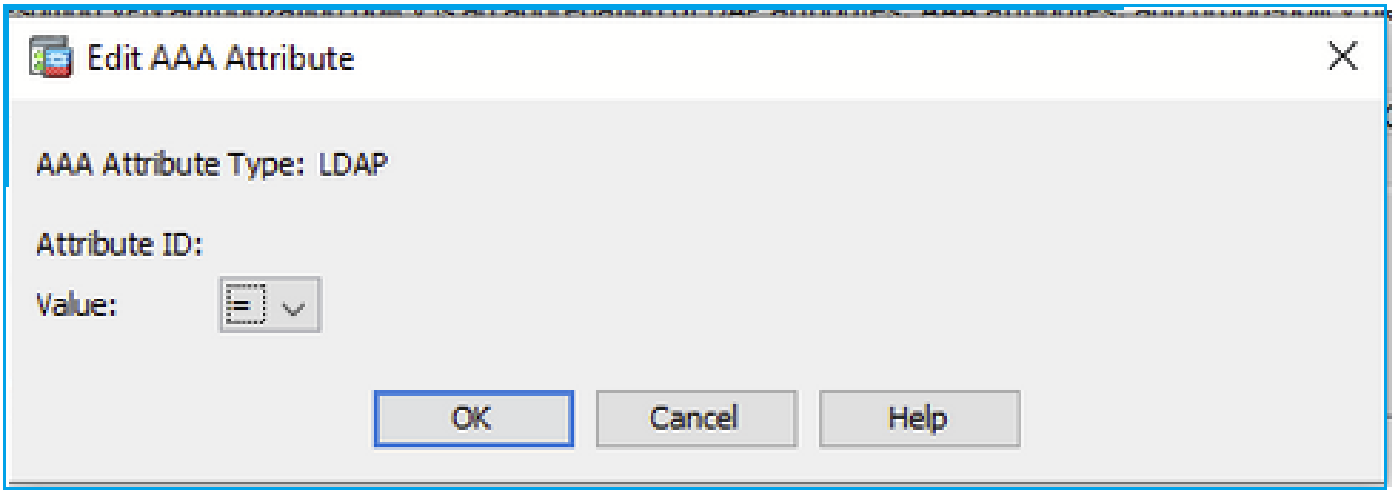
```
#
```

debug ldap 255

Nas depurações, procure linhas que contenham dicas como "Com falha".

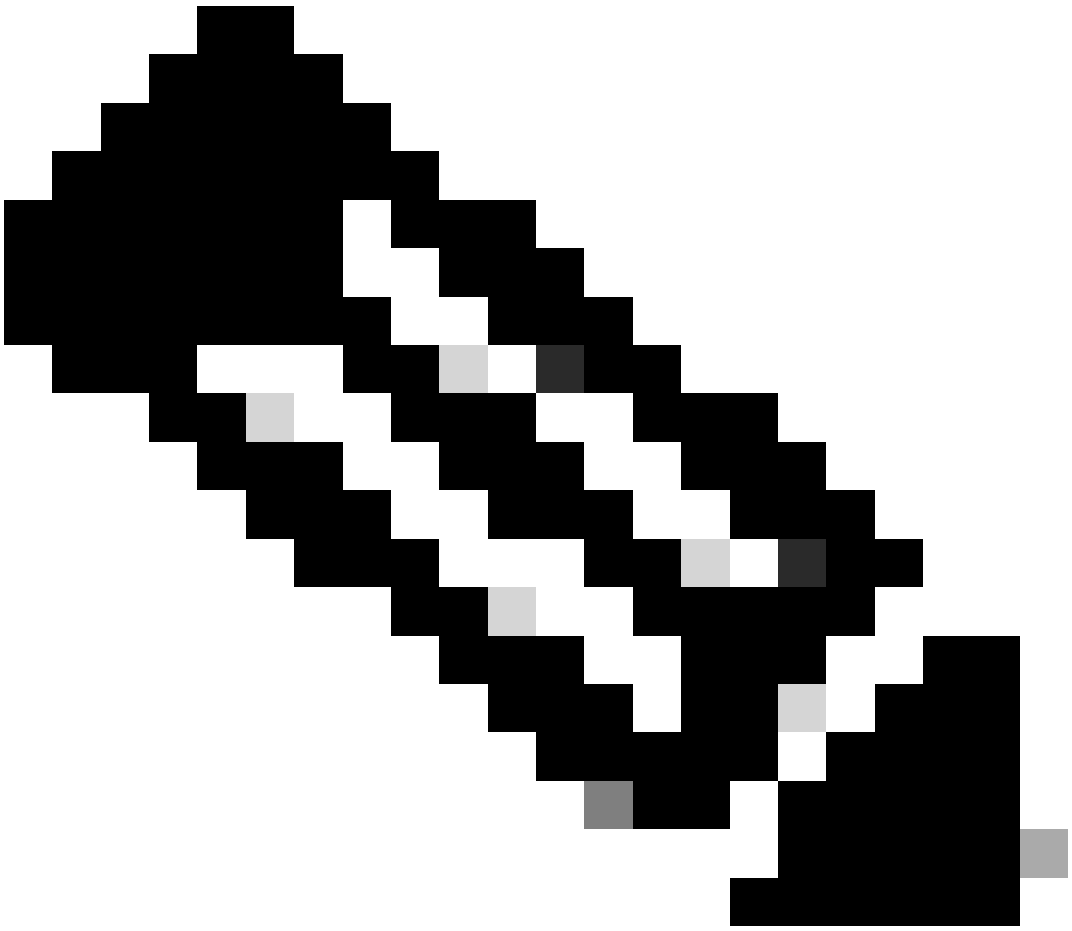
Problema 11. A configuração do LDAP WebVPN do ASDM está ausente

Em DAP configuration on ASDM AAA Attributes type (Radius/LDAP) are not visible only seeing = and != on dropdown:



Solução de problemas - Etapas recomendadas

Este é um defeito de software rastreado pela ID de bug Cisco CSCwa99370
ASDM:configuração DAP com tipo de Atributos AAA ausente (Radius/LDAP)

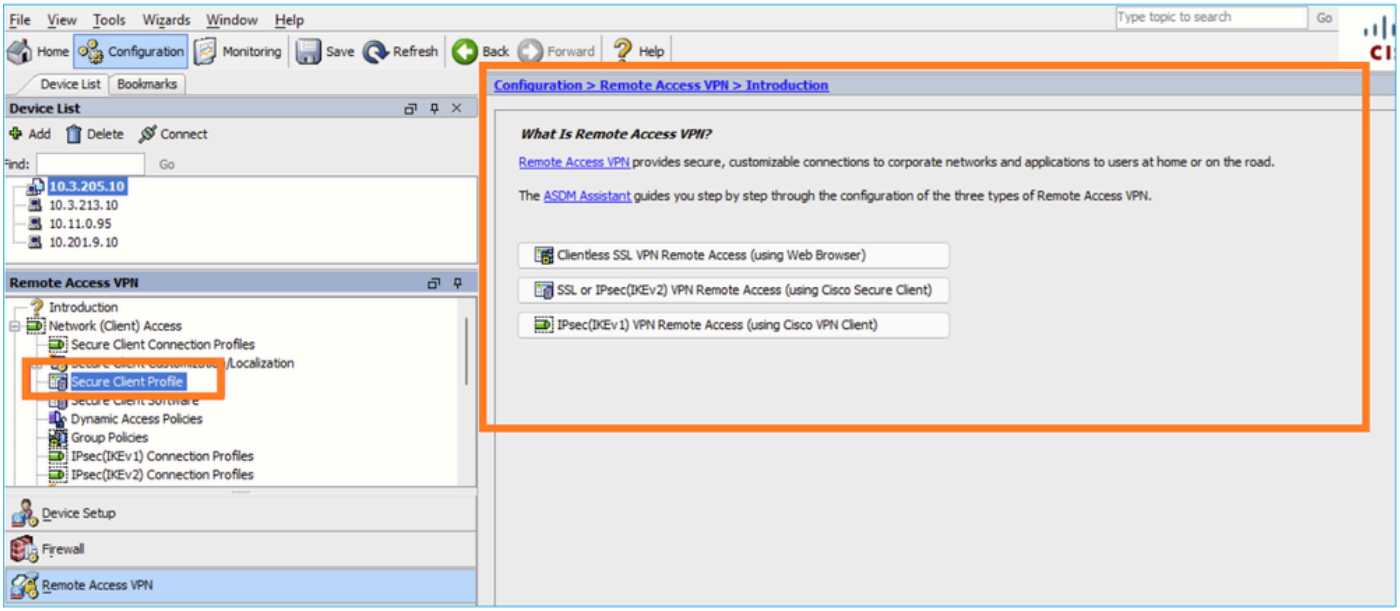


Note: Esse defeito foi corrigido em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

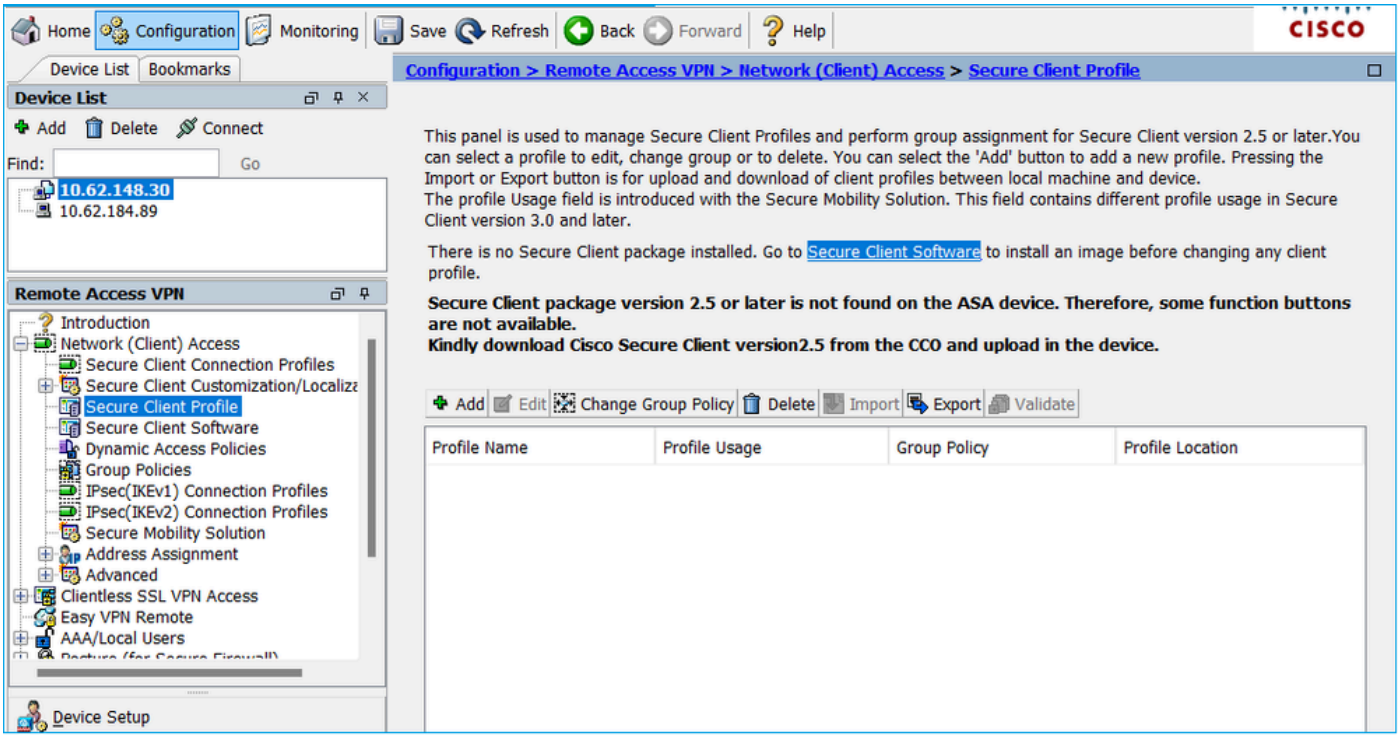
Identificar e Solucionar Outros Problemas do ASDM

Problema 1. Não é possível acessar o Secure Client Profile no ASDM

A IU do ASDM mostra isto:



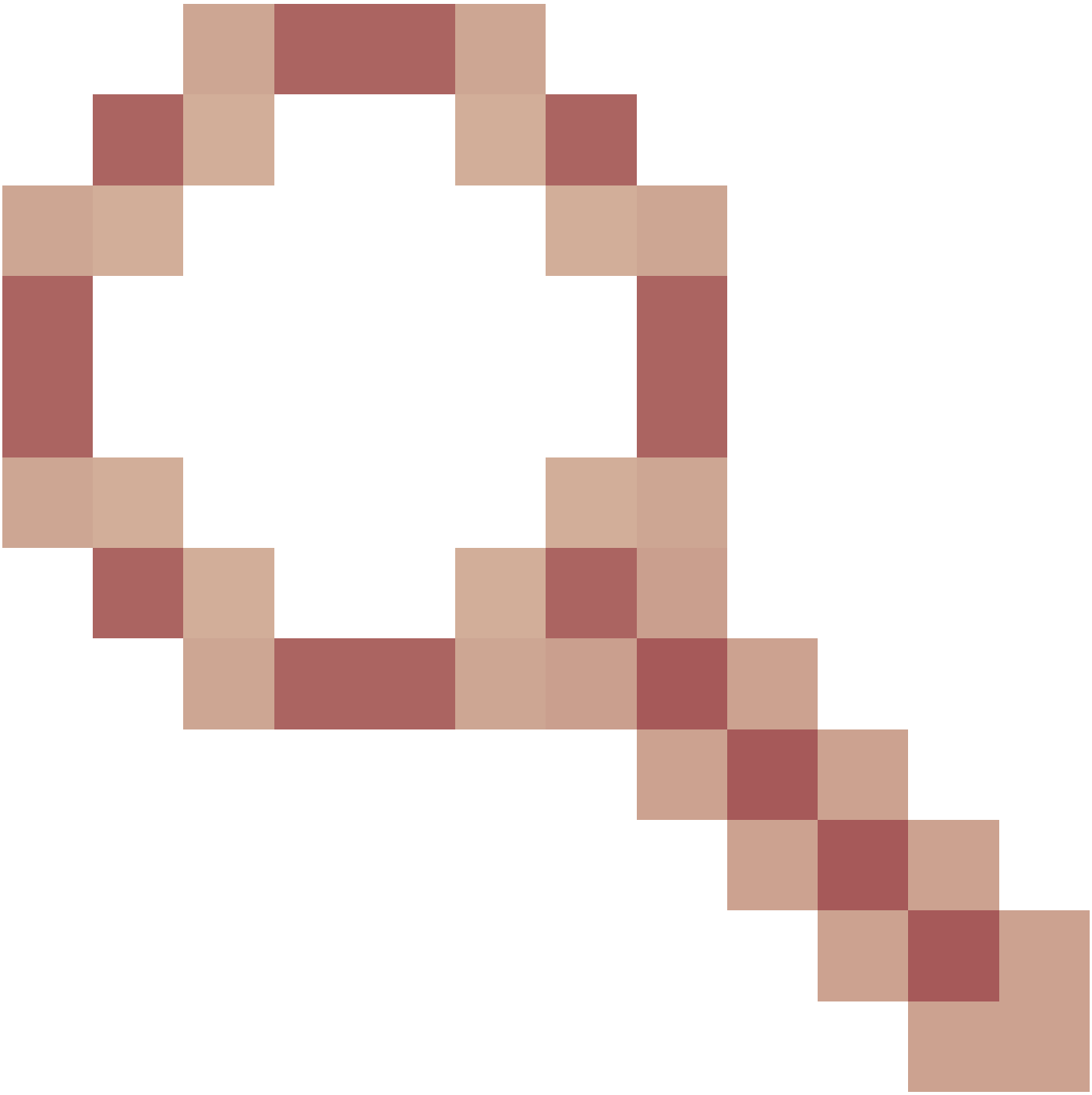
Enquanto a saída de IU esperada é:



Solução de problemas - Etapas recomendadas

Este é um defeito conhecido:

ID de bug Cisco CSCwi56155



Não é possível acessar o Secure Client Profile no ASDM

Soluções:

Fazer downgrade do AnyConnect

or

Atualizar o ASDM para a versão 7.20.2

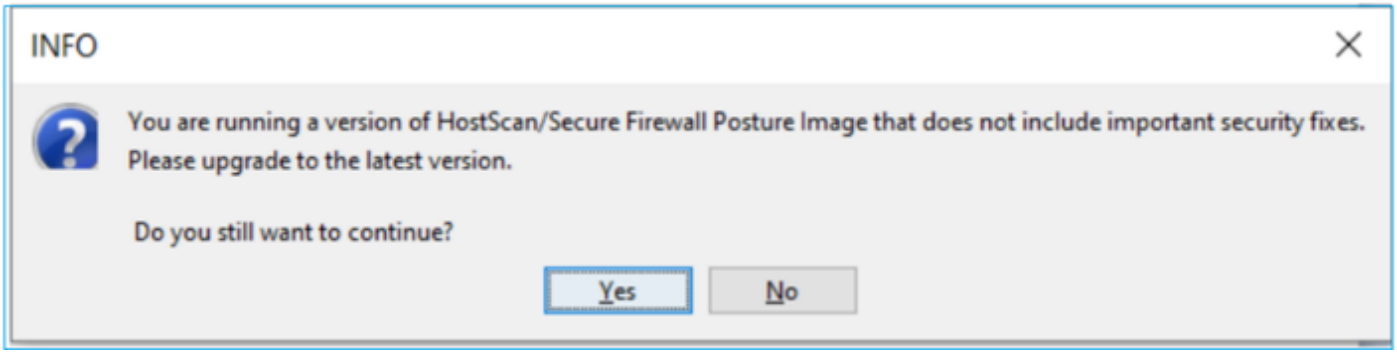
Verifique as notas de defeito para obter mais detalhes. Além disso, você pode se inscrever no defeito para receber uma notificação sobre suas atualizações.

Problema 2. O ASDM mostra um pop-up para o hostscan - a imagem não inclui

correções de segurança importantes

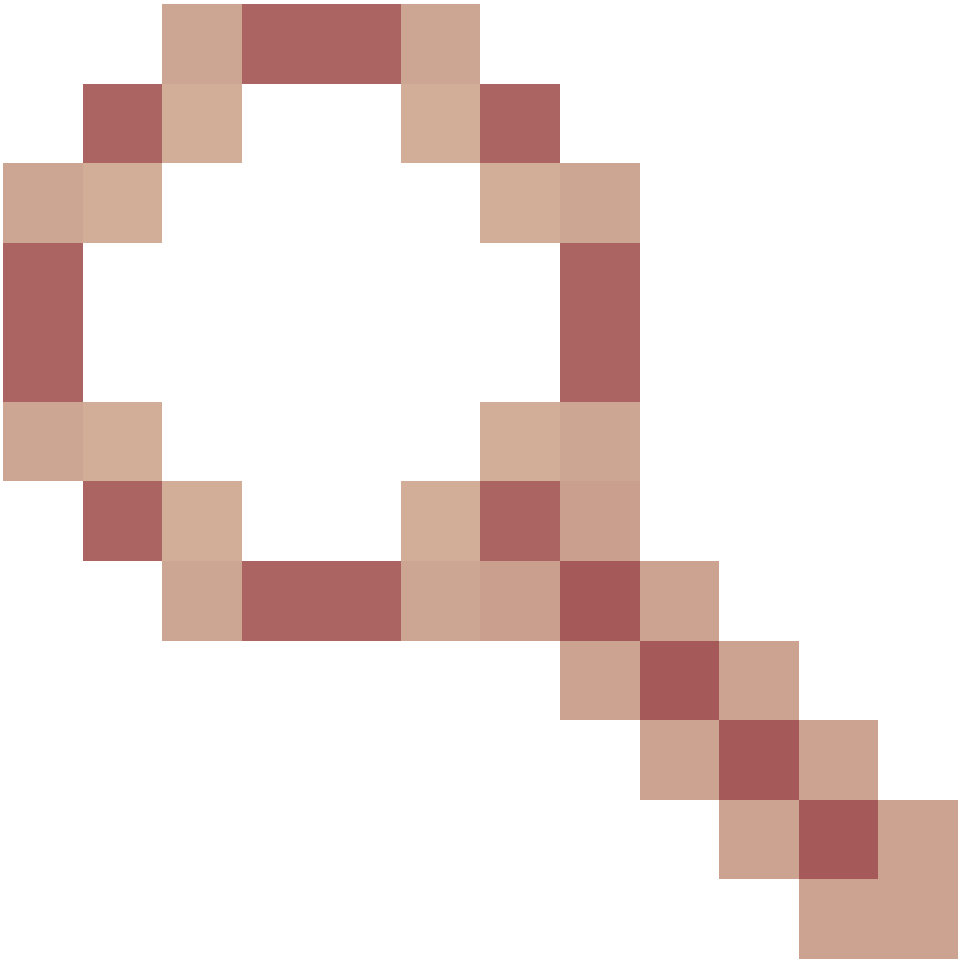
A IU do ASDM mostra:

"Você está executando uma versão da imagem de postura do HostScan/SecureFirewall que não inclui correções de segurança importantes. Atualize para a versão mais recente. Ainda deseja continuar?"

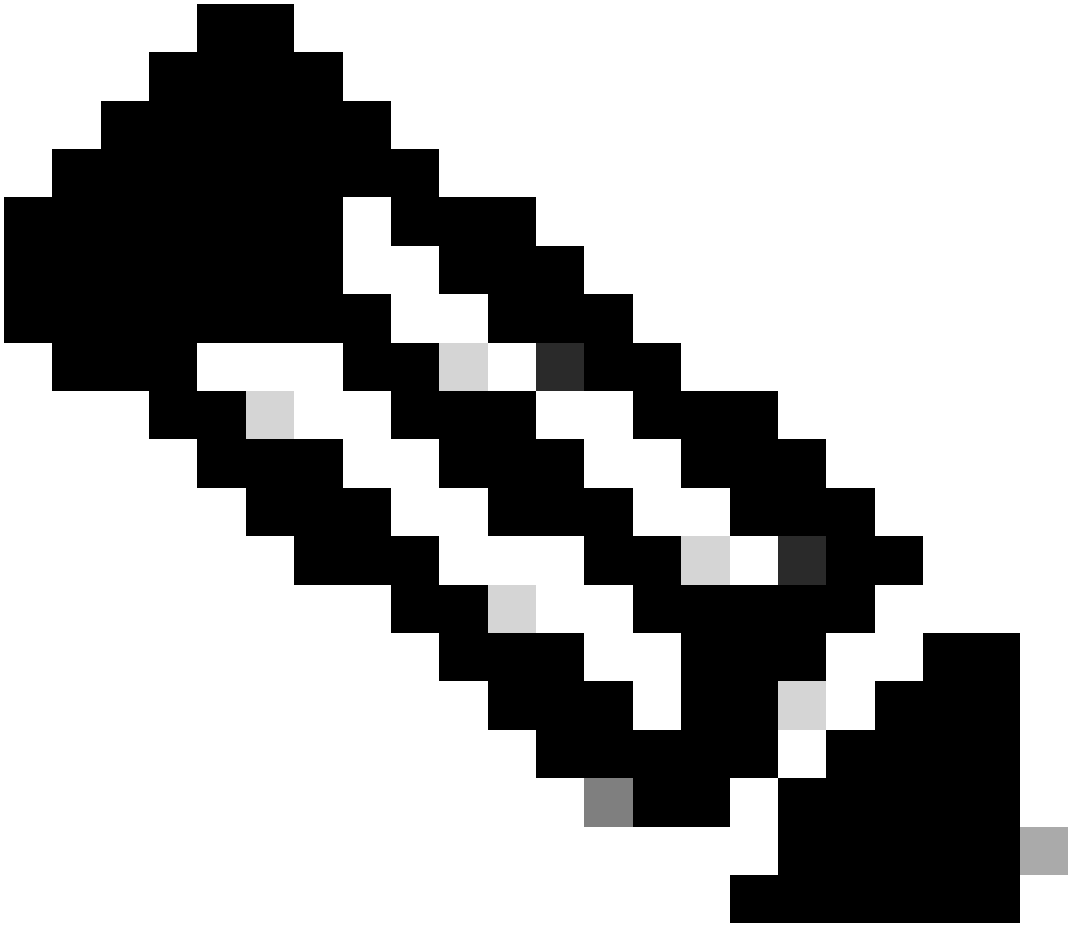


Solução de problemas - Etapas recomendadas

Este é um defeito conhecido:



ID de bug Cisco CSCwc62461
Ao fazer login no ASDM pop-up para hostscan - a imagem não inclui correções de segurança importantes



Note: Esse defeito foi corrigido em versões recentes do software ASDM. Verifique os detalhes do defeito para obter mais informações.

Solução:

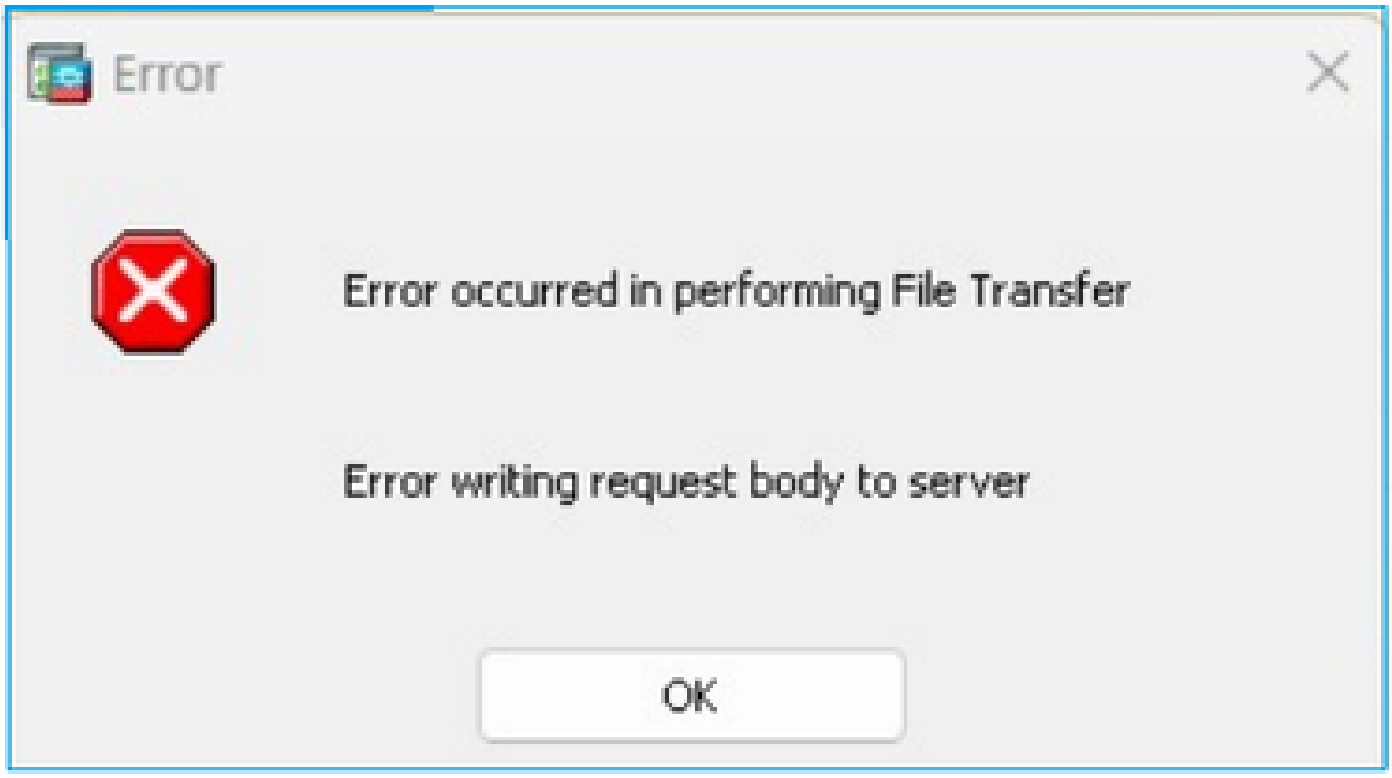
Clique em 'Sim' na caixa de mensagem pop-up para continuar.

Problema 3. ASDM "Erro ao gravar o corpo da solicitação no servidor" ao copiar uma imagem no ASDM

A IU do ASDM mostra:

Ocorreu um erro ao executar a transferência de arquivos

Erro ao gravar o corpo da solicitação no servidor



Solução de problemas - Ações recomendadas

Este é um defeito conhecido monitorado por:

ID de bug Cisco CSCtf74236
ASDM "Erro ao gravar corpo da solicitação no servidor" ao copiar imagem

Solução

Use SCP/TFTP para transferir o arquivo.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.