排除ASDM配置、身份验证和其他问题

目录

简介

背景

排除ASDM配置问题

- 问题1. ASDM不显示应用于接口的任何访问控制列表(ACL)
- 问题2. ASA CLI和ASDM UI之间的命中计数不一致
- 问题3. “错误：%在“^”标记处检测到无效输入。" 在ASDM中编辑ACL时出现错误消息
- 问题4. “错误：ACL与路由映射关联，不支持非活动，在特定情况下应删除acl错误消息
- 问题5. ASDM实时日志查看器中没有隐式拒绝连接的日志
- 问题6. ASDM在尝试修改任何网络对象或对象组时冻结
- 问题7. ASDM可以为不同接口显示额外的访问控制列表规则
- 问题8.实时日志在实时日志查看器中不可用
- 问题9. “实时日志查看器”的“日期”和“时间”列为空。疑难解答 — 建议操作
- 问题10.在多情景ASA中切换到其他情景后，登录ASDM可能会失败
- 问题11.在不同情景之间切换时，ASDM会话突然终止
- 问题12. ASDM随机退出/终止，并显示消息“ASDM从ASA设备收到要断开的消息”。ASDM现在将退出。”
- 问题13. ASDM负载挂起，并显示消息“Authentication FirePOWER login”
- 问题14. ASDM不显示Firepower模块管理/配置
- 问题15.在ASDM上无法访问安全客户端配置文件
- 问题16.无法在ASDM上编辑安全客户端配置文件XML配置文件
- 问题17.配置更改后缺少安全客户端映像
- 问题18. http server session-timeout和http server idle-timeout命令无效
- 问题19. ASDM上的Dap.xml复制失败
- 问题20.ASDM上看不到IKE策略和IPSEC提议
- 问题21. ASDM显示消息“The enable password not set.请立即设置。”
- 问题22.刷新ASDM UI后，ASDN对象消失
- 问题23.无法为低于4.5的版本编辑AnyConnect客户端配置文件
- 问题24.无法导航到Edit Service Policy > Rule Actions > ASA FirePOWER Inspection选项卡
- 问题25. ASDM上的AnyConnect映像5.1版和AnyConnect配置文件编辑器
- 问题26. AAA属性类型(Radius/LDAP)在ASDM中不可见
- 问题27. ASDM上显示“Post Quantum key cannot be empty”错误
- 问题28.使用“使用情况”选项时，ASDM不会显示任何结果
- 问题29.删除网络对象时，无法删除警告消息“[网络对象]，因为它用于以下内容”
- 问题30.ASDM中“网络对象/组”选项卡的可用性问题

排除ASDM身份验证问题

- 问题1. ASDM登录失败
- 问题2. ASDM命令授权失败
- 问题3.配置ASDM只读访问
- 问题4. ASDM多重身份验证(MFA)

问题5. ASDM外部身份验证配置
问题6. ASDM本地身份验证失败
问题7. ASDM一次性密码
问题8.连接配置文件未显示所有方法
问题9. ASDM会话不超时
问题10. ASDM LDAP身份验证失败
问题11.缺少ASDM Webvpn DAP配置
排除ASDM其他问题
问题1.无法访问ASDM上的安全客户端配置文件
问题2. ASDM显示hostscan的弹出窗口 — 映像不包括重要的安全修复
问题3.通过ASDM复制映像时，ASDM“将请求正文写入服务器时出错”

简介

本文档介绍自适应安全设备管理器(ASDM)配置、身份验证和其他问题的故障排除过程。

背景

本文档是ASDM故障排除系列的一部分，包括以下文档：

链路1<>

链路2<>

链路3<>

排除ASDM配置问题

问题1. ASDM不显示应用于接口的任何访问控制列表(ACL)

ASDM不会显示应用于接口的任何访问控制列表(ACL)，即使有应用于相关接口的有效访问组也是如此。消息改为显示“0传入规则”。 观察到以下症状：在接口的访问组配置中配置了L3和L2 ACL:

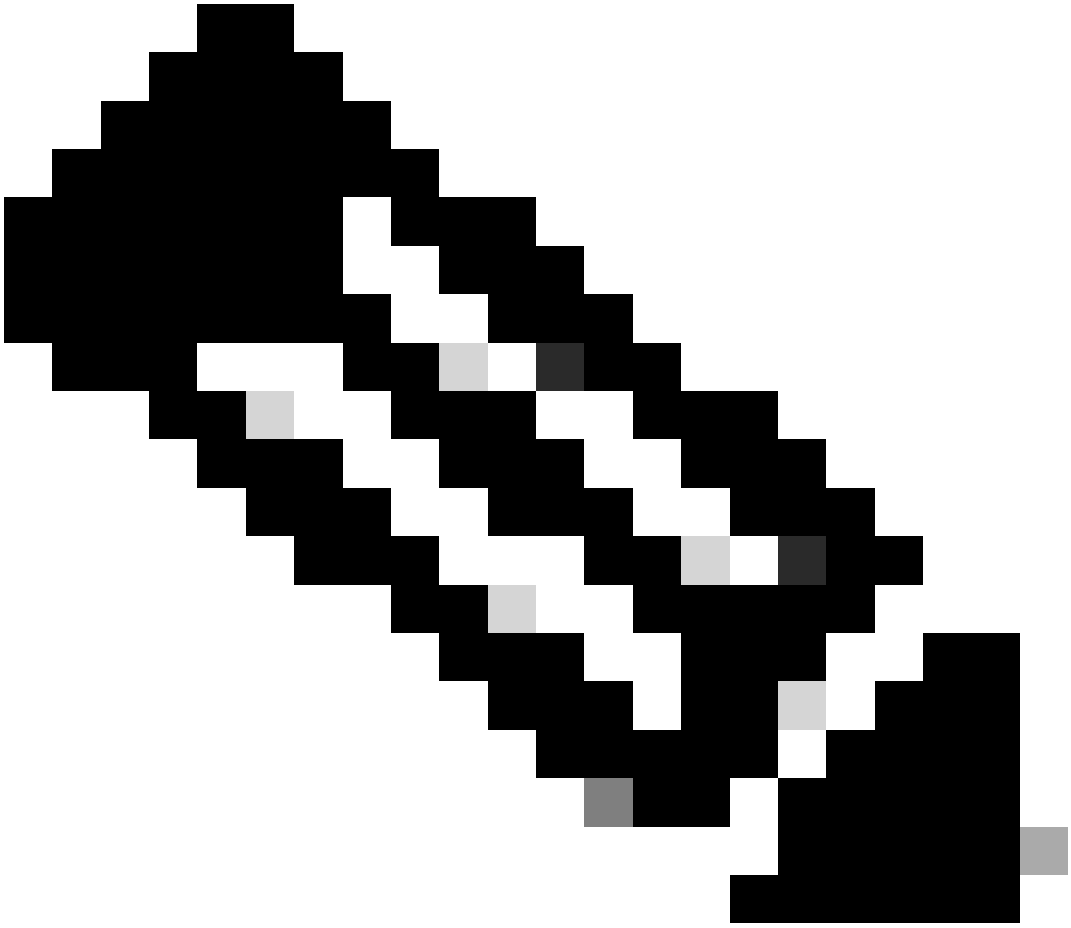
<#root>

```
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
```

故障排除 — 建议的操作

请参阅软件Cisco Bug ID CSCwj14147 “如果L2和L3 acl混合，ASDM无法加载访问组配置。”



注意：此缺陷在最新的ASDM软件版本中已修复。有关详细信息，请查看缺陷详细信息。

问题2. ASA CLI和ASDM UI之间的命中计数不一致

ASDM中的命中计数条目与防火墙输出上的show access-list命令所报告的访问列表命中计数不一致。

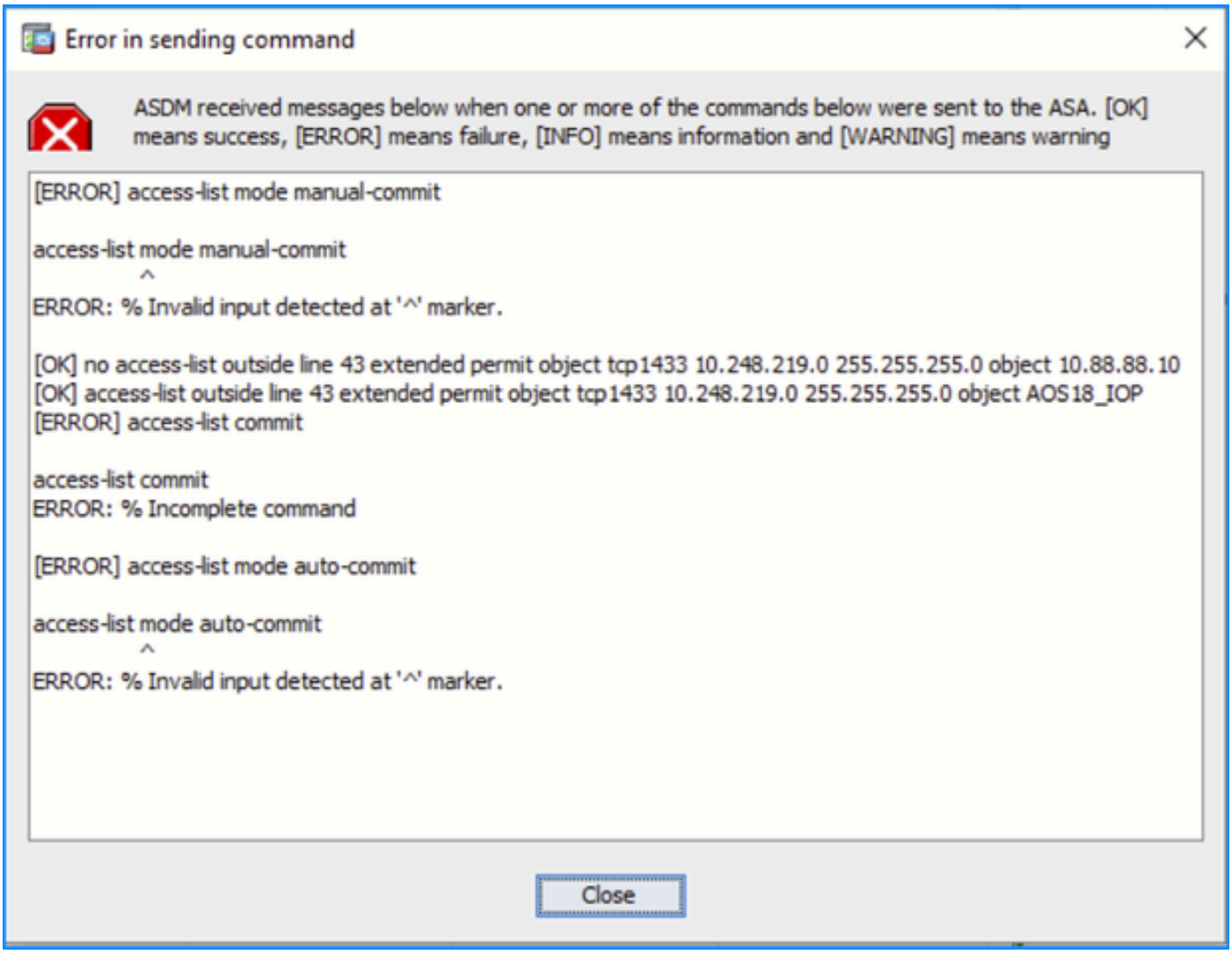
故障排除 — 建议的操作

请参阅软件Cisco Bug ID CSCtq38377“ENH:ASDM应在ASA上使用ACL散列计算，而不是本地计算”和Cisco Bug ID CSCtq38405“ENH:ASA需要向ASD提供ACL哈希信息的机制”

问题3. “错误：%在“^”标记处检测到无效输入。" 在ASDM中编辑ACL时出现错误消息

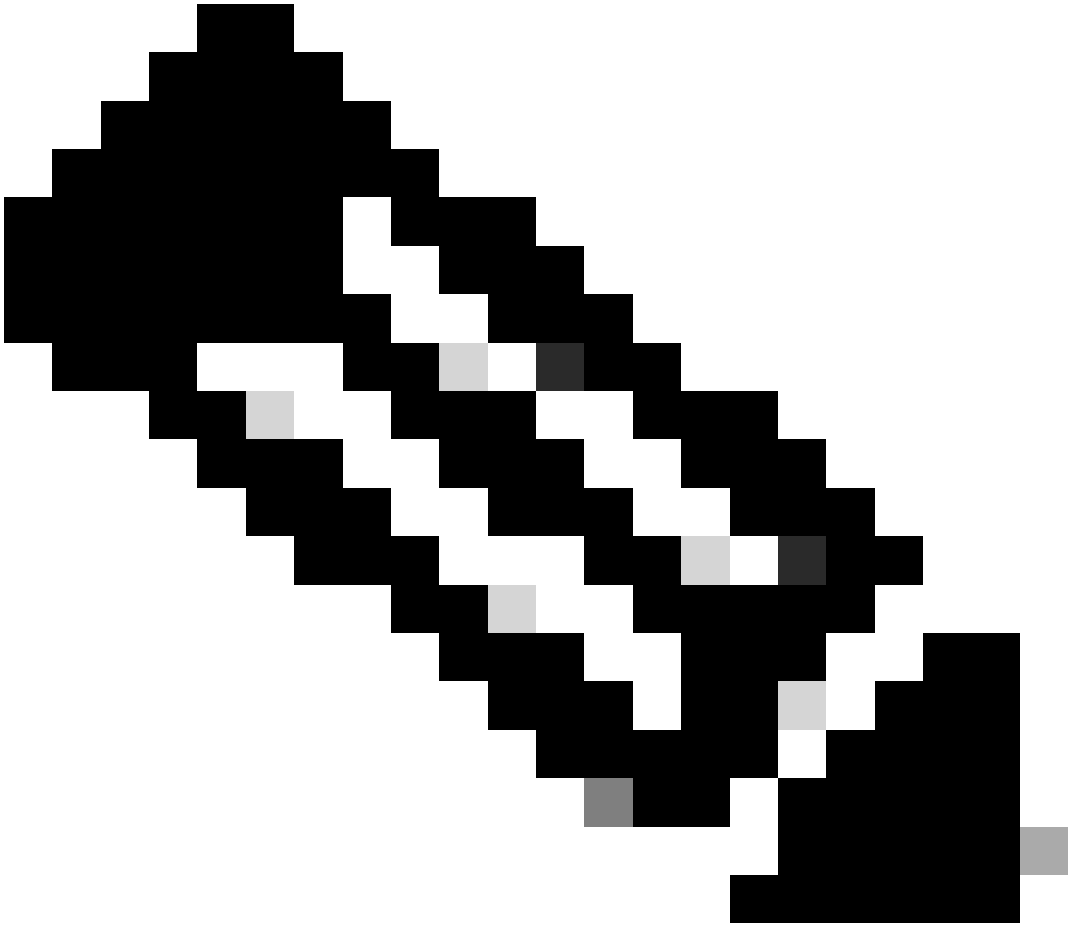
“错误：%在“^”标记处检测到无效输入。" 在ASDM中编辑ACL时会显示错误消息：

```
[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.
```



故障排除 — 建议的操作

请参阅软件Cisco Bug ID CSCvq05064“Edit an entry(ACL) from ASDM gives an error.将ASDM与OpenJRE/Oracle配合使用时 — 版本7.12.2”和Cisco Bug ID CSCvp88926“Sending additional commands while deleting access-list”。



注意：这些缺陷在最新的ASDM软件版本中已修复。有关详细信息，请查看缺陷详细信息。

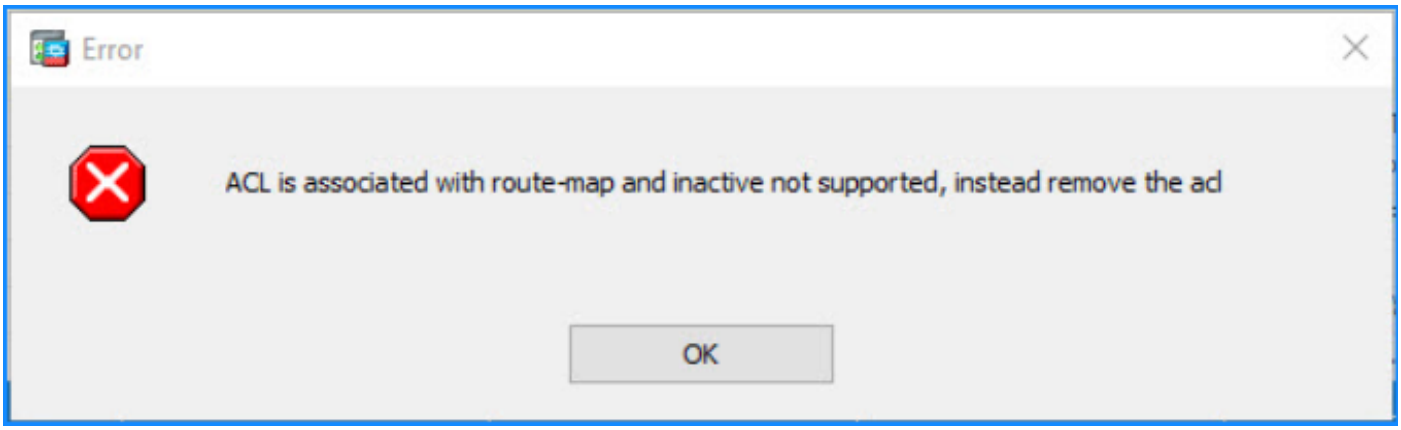
问题 4. “错误：ACL与路由映射关联，不支持非活动，在特定情况下应删除acl错误消息

“错误：ACL与路由映射关联，不支持非活动，请改为删除acl错误消息，如以下情况之一所示：

1. 在基于策略的路由配置中使用的ASDM中编辑ACL:

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

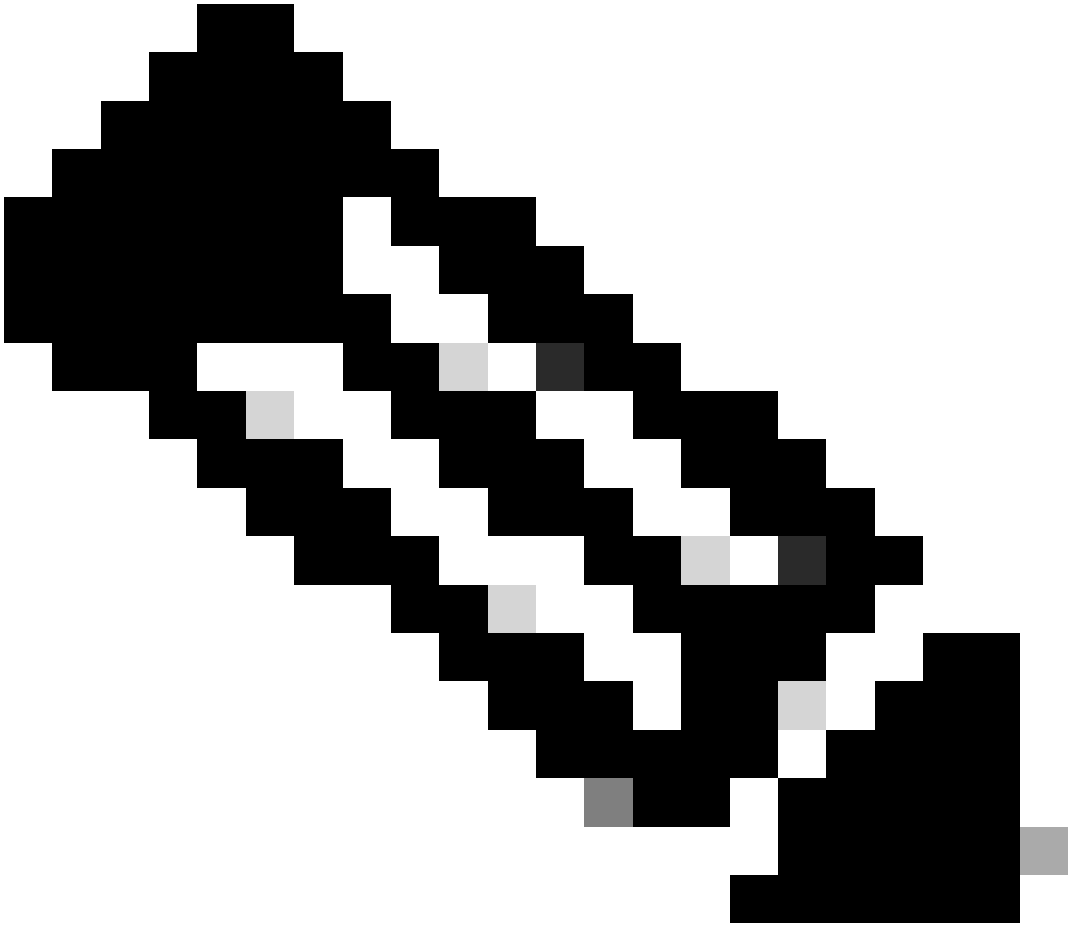
错误：ACL与路由映射关联，不支持非活动状态，请删除acl



2.编辑ACL ASDM > Configuration -> Remote Access VPN -> Network(Client)Access > Dynamic Access策略

故障排除 — 建议的操作

1. 请参阅软件Cisco Bug ID CSCwb57615“Configuring pbr access-list with line number failed.”。 解决方法是从配置中排除“line”参数。
2. 请参阅软件Cisco Bug ID CSCwe34665“Unable to Edit the ACL objects if it is already in use， get the exception”。



注意：这些缺陷已在最近的ASA软件版本中得到修复。有关详细信息，请查看缺陷详细信息。

问题5. ASDM实时日志查看器中没有隐式拒绝连接的日志

ASDM实时日志查看器不显示隐式拒绝连接的日志。

故障排除 — 建议的操作

访问列表末尾的隐式deny不会生成系统日志。如果希望所有被拒绝的流量生成系统日志，请在ACL末尾添加带有log关键字的规则。

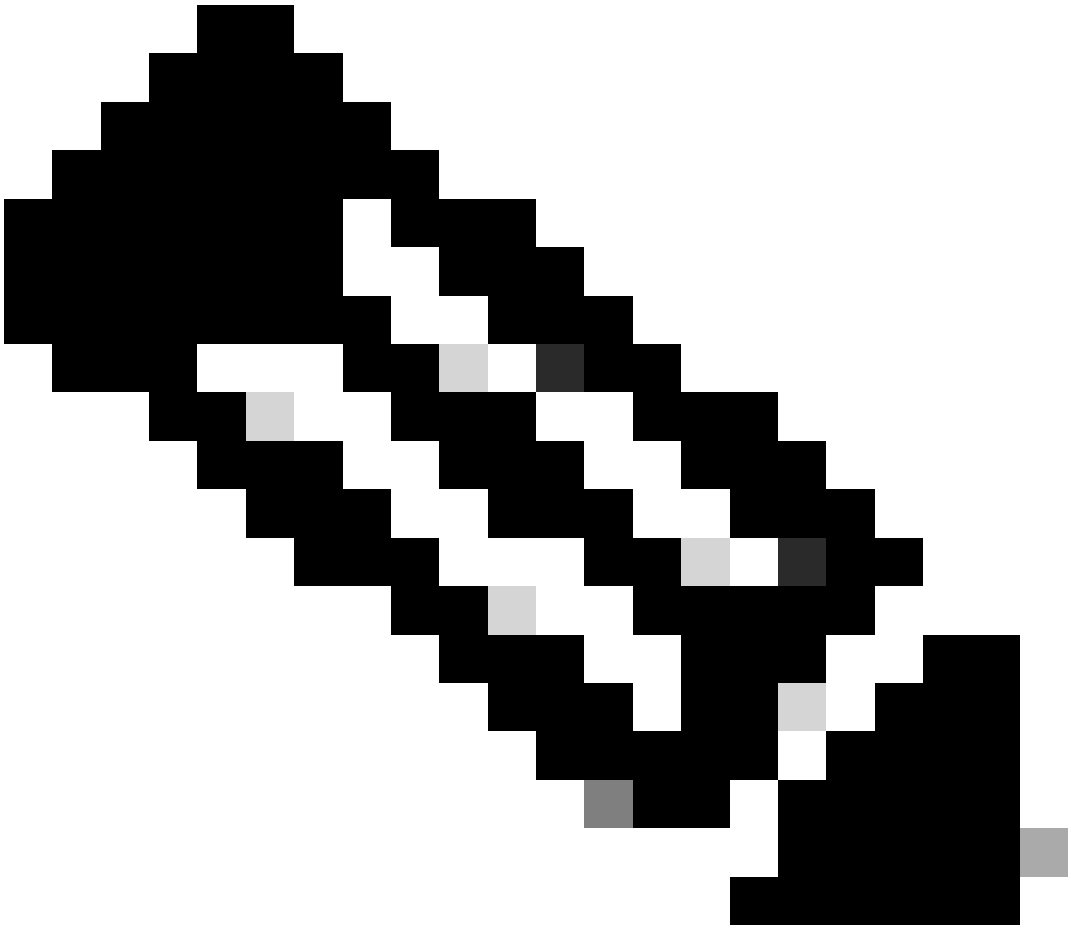
问题6. ASDM在尝试修改任何网络对象或对象组时冻结

尝试从Addresses选项卡下的Configuration > Firewall > Access Rules页面修改任何网络对象或对象组时，ASDM将冻结。遇到此问题时，用户无法编辑网络对象窗口中的任何参数。

故障排除 — 建议的操作

请参阅软件Cisco Bug ID CSCwj1250“ASDM freezes when editing network objects or network object-groups”。 解决方法是禁用topN主机统计信息收集：

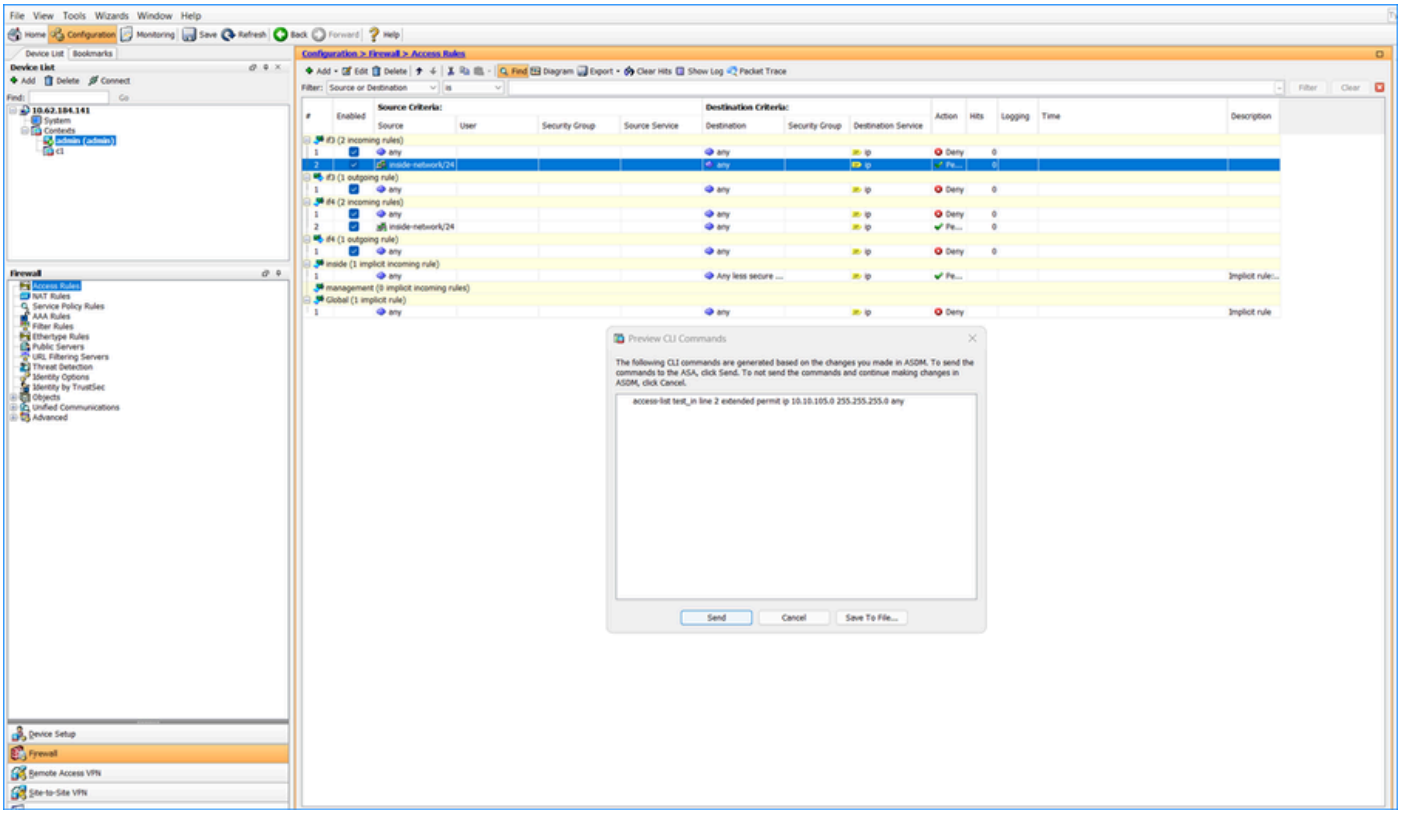
```
<#root>

ASA(config)#

no hpm topN enable
```



注意：此缺陷在最新的ASDM软件版本中已修复。有关详细信息，请查看缺陷详细信息。

问题7. ASDM可以为不同的接口显示额外的访问控制列表规则

如果修改了接口级访问控制列表，ASDM可以显示不同接口的其他访问控制列表规则。在本示例中，传入规则#2已添加到接口if3 ACL。ASDM还显示#2口的if4，而此规则不是由用户配置的。命令预览正确显示了一个待决更改。这是用户界面显示问题。



故障排除 — 建议的操作

请参阅软件Cisco Bug ID CSCwm71434“ASDM可能显示重复的接口访问列表条目”。

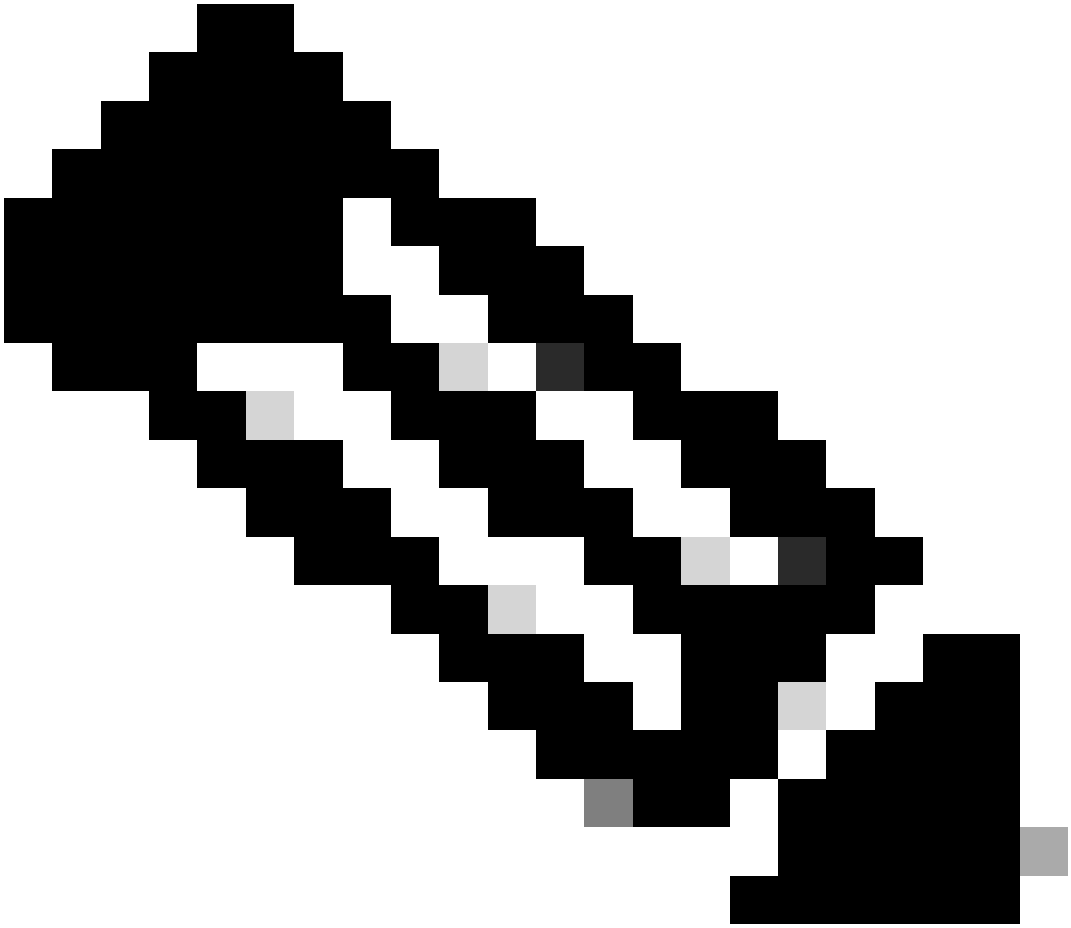
问题8.实时日志查看器中没有实时日志

实时日志查看器中未显示日志

故障排除 — 建议的操作

1. 确保已配置日志记录。请参阅ASDM手册1:Cisco ASA系列常规操作ASDM配置指南，7.22，章节：日志记录.

2. 请参阅软件Cisco Bug ID CSCvf82966“ASDM - Logging:无法查看实时日志”。

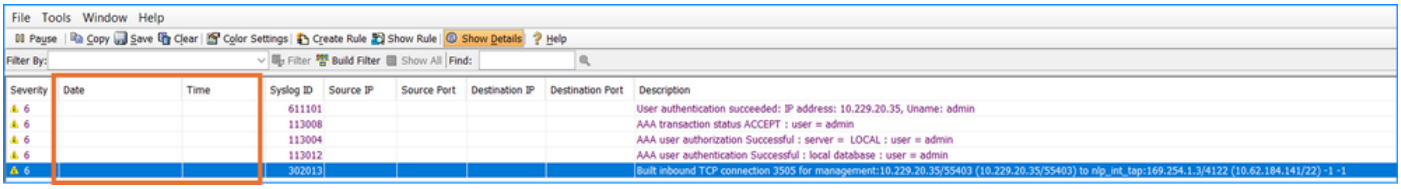


注意：此缺陷在最新的ASDM软件版本中已修复。有关详细信息，请查看缺陷详细信息。

参考

- ASDM第1册：Cisco ASA系列常规操作ASDM配置指南，7.22，章节：日志记录.

问题9.实时日志查看器中的“日期”和“时间”列为空



故障排除 — 建议的操作

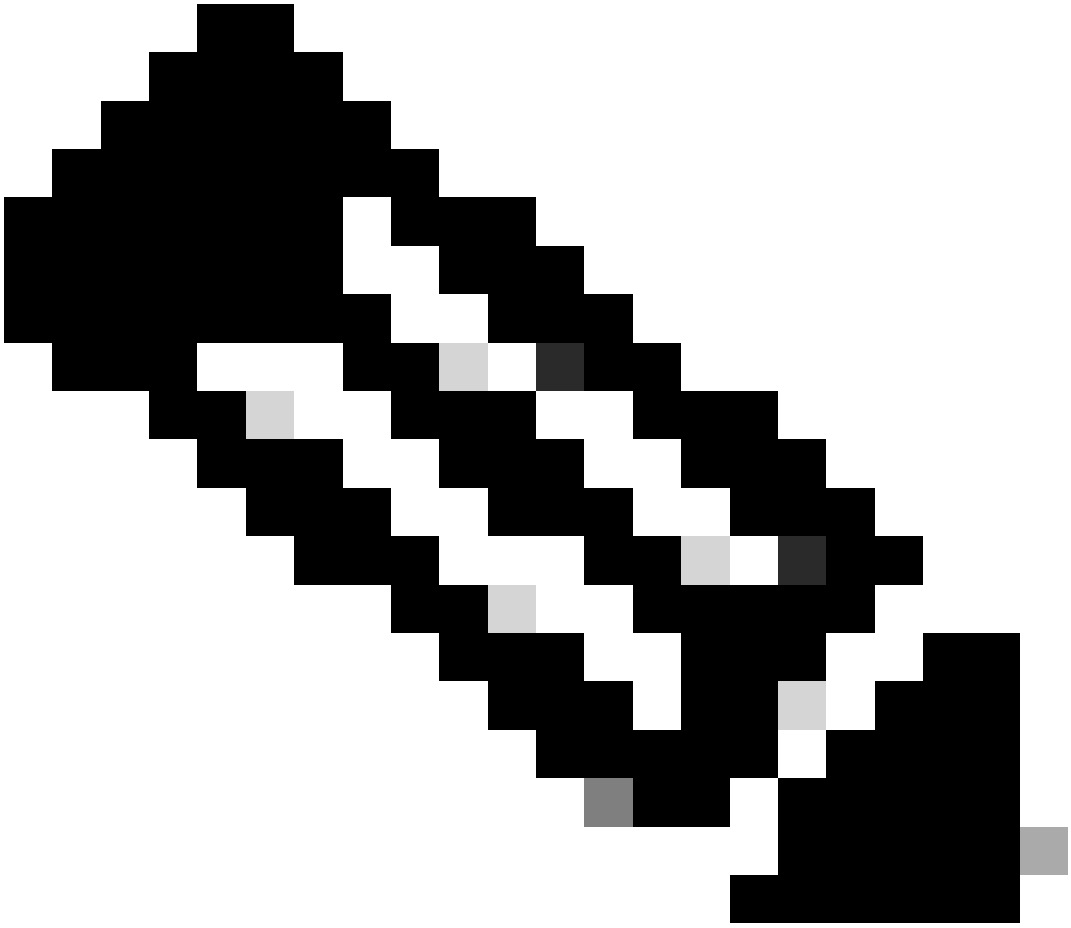
1. 检查是否使用了RFC5424日志记录时间戳格式：

```
<#root>

#

show run logging


logging enable

logging timestamp rfc5424
```

2. 如果使用RFC5424日志记录时间戳格式，请参阅软件Cisco bug ID CSCvs5212 "ASDM ENH:事件日志查看器能够使用rfc5424时间戳格式显示ASA系统日志”。解决方法是避免使用RFC5424格式：

```
<#root>

firewall(config)#

no logging timestamp rfc5424


firewall(config)#

logging timestamp
```

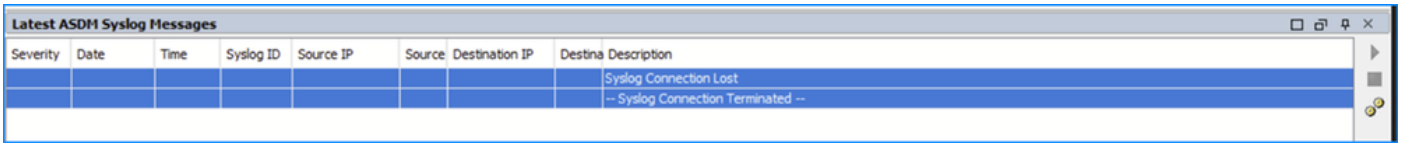
3. 此外，请参阅软件缺陷Cisco Bug ID CSCwh70323“Timestamp entry missing for some syslog messages sent to syslog server”。



注意：此缺陷在最新的ASDM软件版本中已修复。有关详细信息，请查看缺陷详细信息。

问题 10. 在多情景ASA中切换到其他情景后，登录到ASDM可能会失败

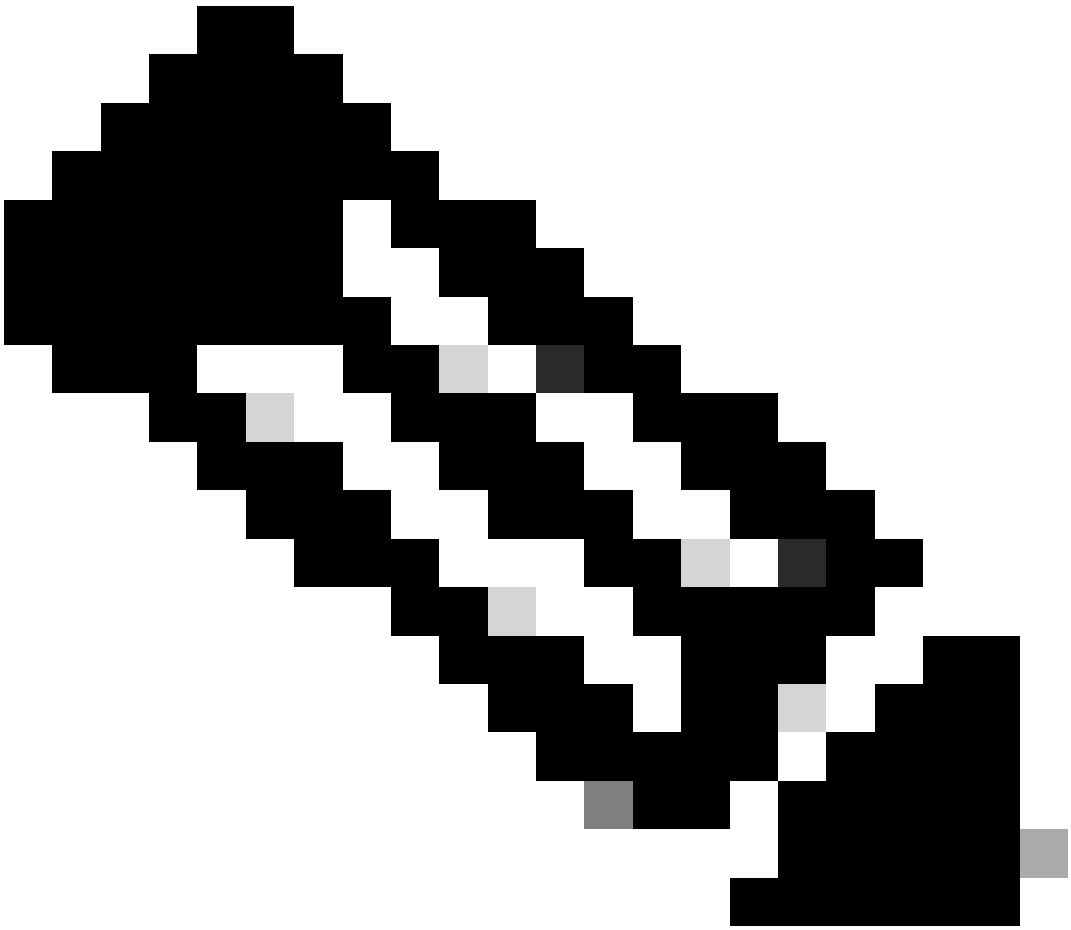
Home页中的Latest ASDM Syslog Messages选项卡显示“Syslog Connection Lost”和“Syslog Connection Terminated”消息：



故障排除 — 建议的操作

确保已配置日志记录。请参阅软件Cisco Bug ID CSCvz15404“ASA:多情景模式：ASDM日志记录在

切换到其他情景时停止。”



注意：此缺陷在最新的ASDM软件版本中已修复。有关详细信息，请查看缺陷详细信息。

问题 11. 在不同情景之间切换时，ASDM会话突然终止

当在不同情景之间切换时，ASDM会话突然终止，并显示错误消息“The maximum number of management sessions for protocol http or user already exists”。请稍后重试”。系统日志消息中显示以下日志：

```
%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
```

故障排除 — 建议的操作

1. 检查当前ASDM资源使用率是否已达到Limit。在本例中，Denied计数器增加：

<#root>

firewall #

show resource usage resource ASDM

Resource Current Peak Limit Denied Context
ASDM

5

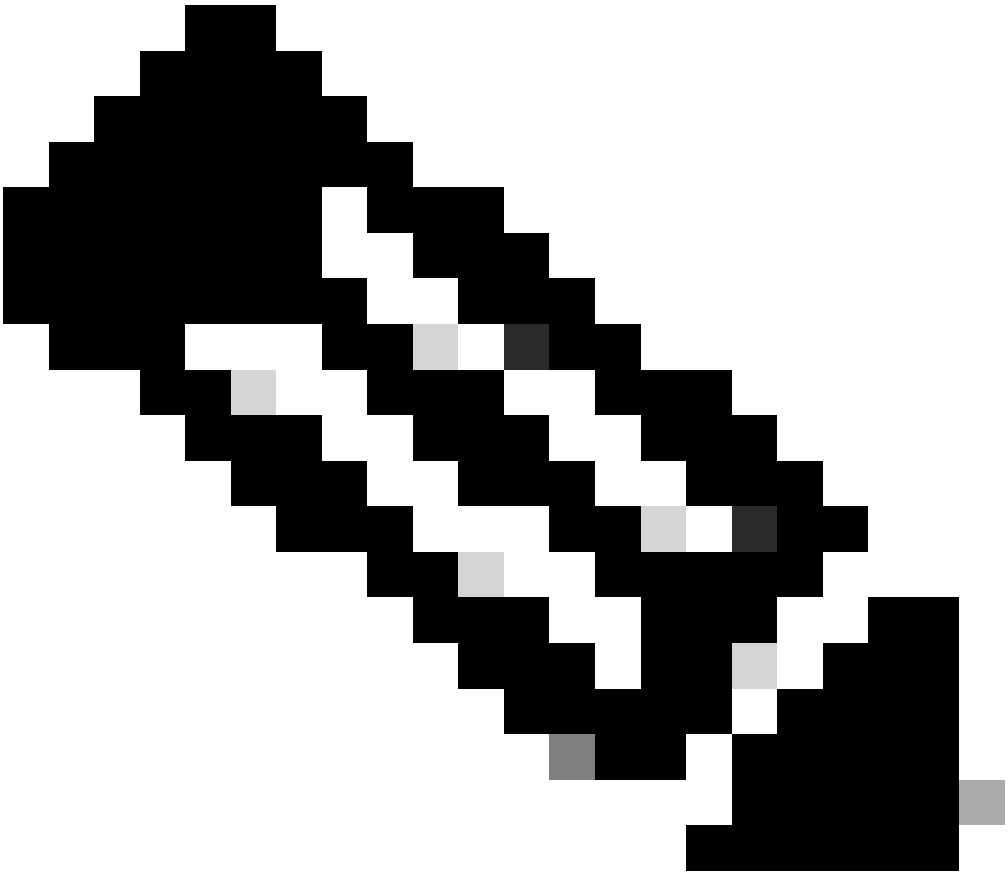
5

5

10

admin

2. 请参阅软件Cisco Bug ID CSCvs72378“ASDM会话在不同情景之间切换时突然终止”。



注意：此缺陷已在最近的ASA软件版本中得到修复。有关详细信息，请查看缺陷详细信息。

3. 如果软件版本具有Cisco Bug ID CSCvs72378的修复程序，并且当前资源已达到限制，请断开一些现有ASDM会话。您可以关闭ASDM，或者清除运行ASDM的主机IP地址的HTTPS连接。在本示例中，假设ASDM上的HTTP服务器在默认HTTPS端口443上运行：

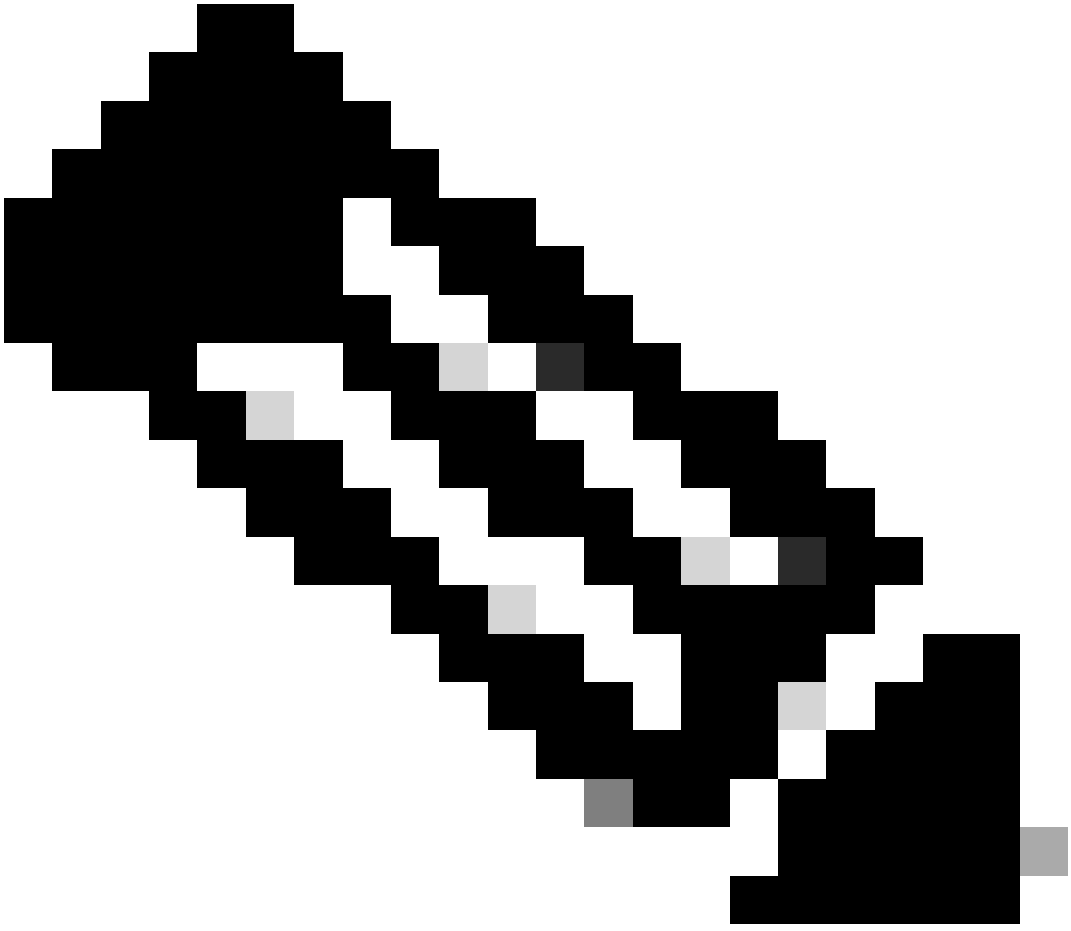
```
<#root>

#

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
```

问题12. ASDM随机退出/终止，并显示消息“ASDM从ASA设备收到要断开连接的消息”。ASDM现在将退出。”

在多情景ASA上，ASDM随机退出/终止，并显示消息“ASDM从ASA设备收到要断开的消息。ASDM现在将退出。”

故障排除 — 建议的操作

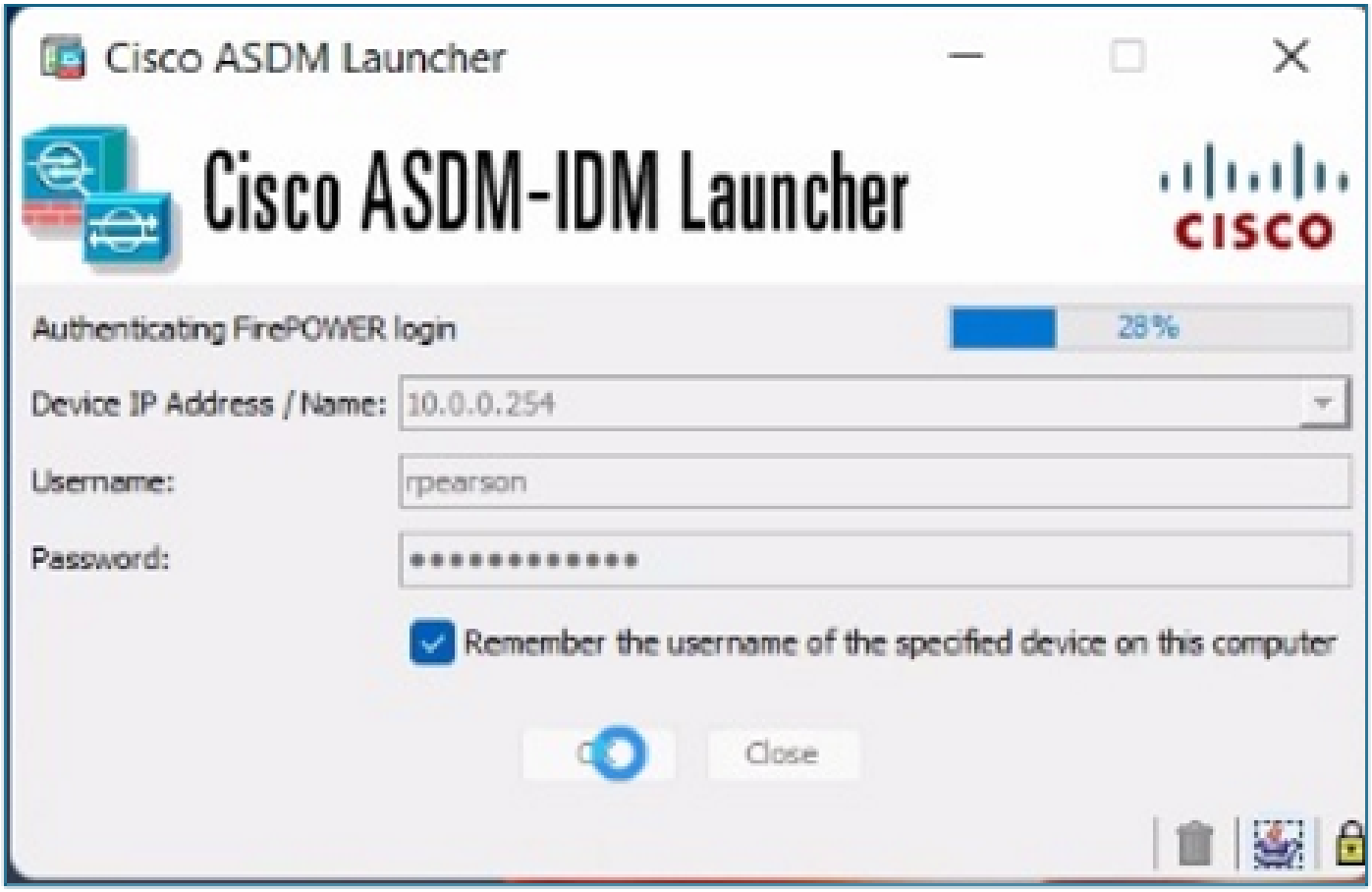
请参阅软件缺陷Cisco Bug ID CSCwh04395“ASDM应用程序随机退出/终止，并显示有关多情景设置的警报消息”。



注意：此缺陷已在最近的ASA软件版本中得到修复。有关详细信息，请查看缺陷详细信息。

问题13.ASDM负载挂起，并显示消息“Authentication FirePOWER login”

ASDM负载挂起，并显示消息“Authentication FirePOWER login”：

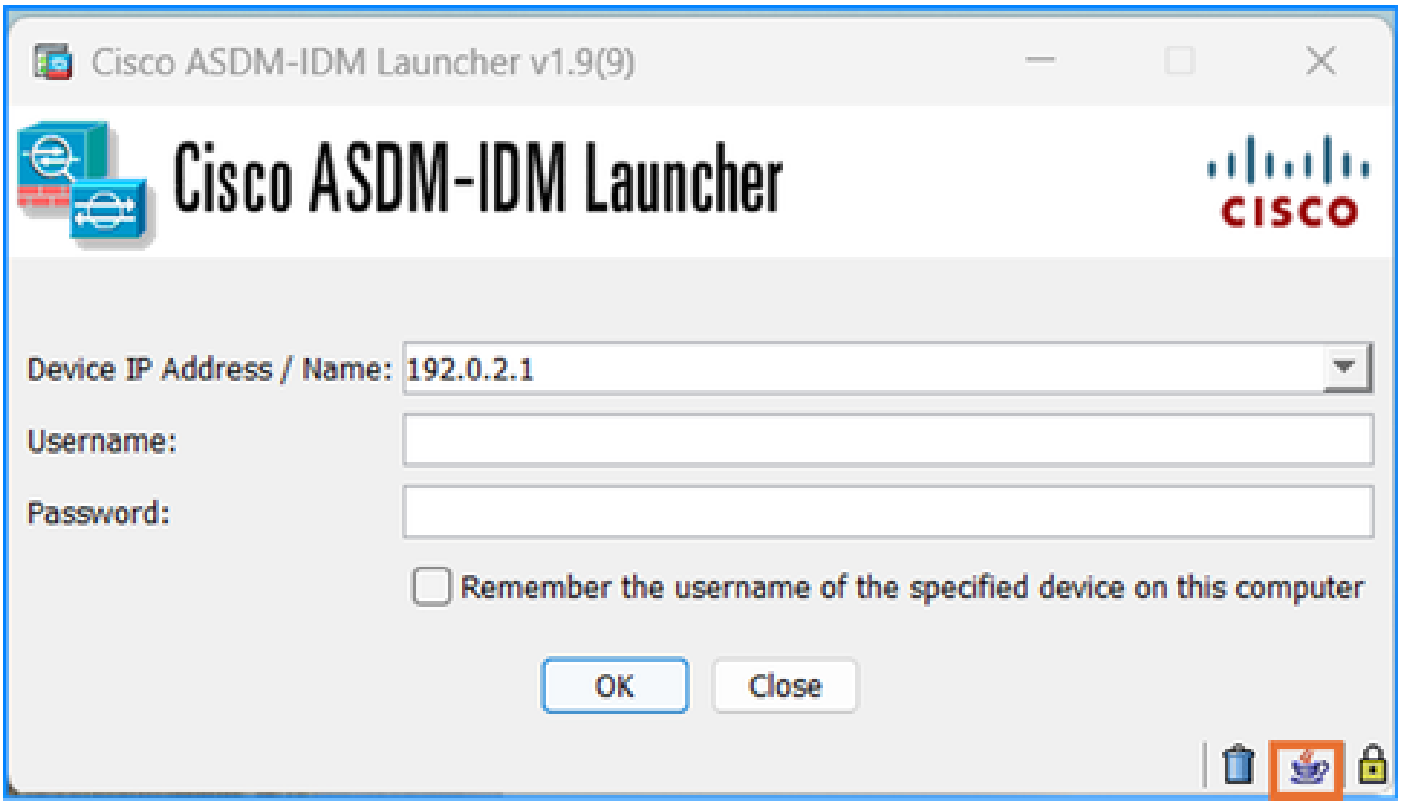


Java控制台日志显示“Failed to connect to FirePower， continuing without it”消息：

<#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)
```

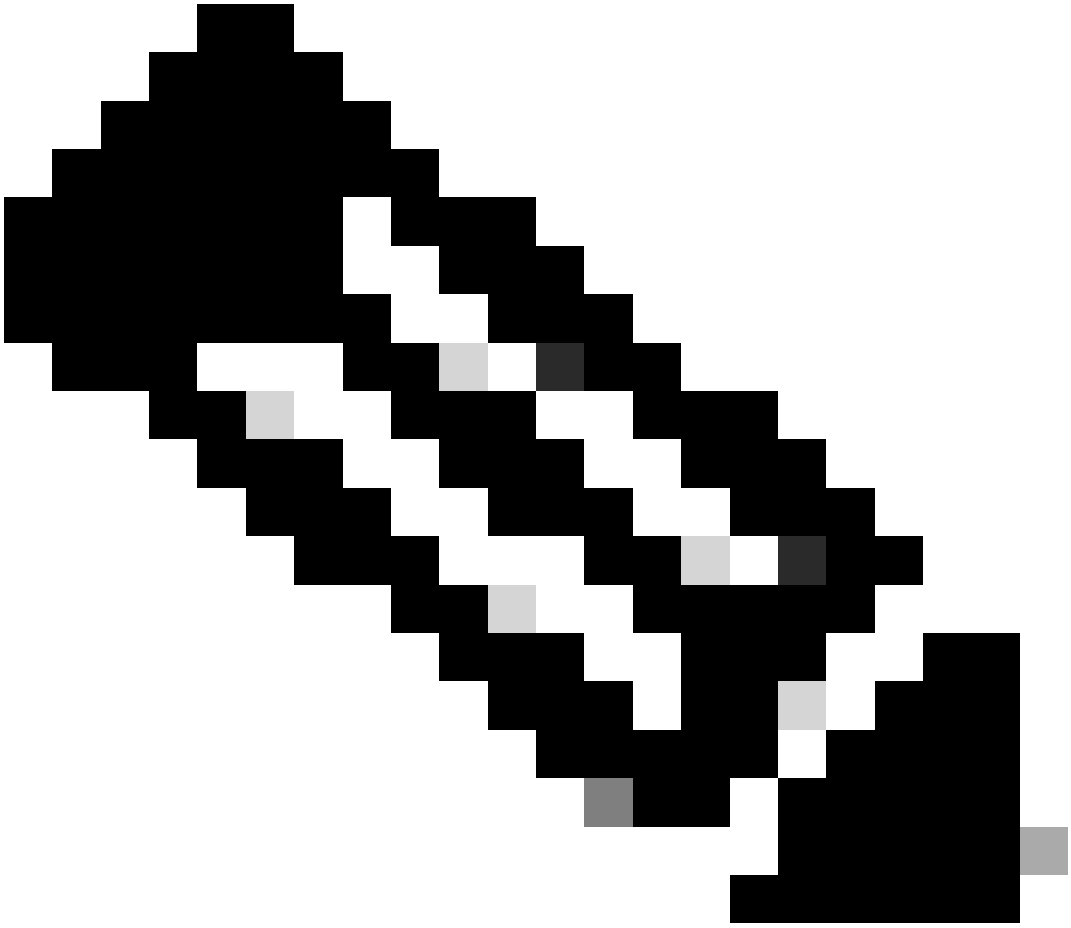
要验证此症状，请启用Java控制台日志：



故障排除 — 建议的操作

请参阅软件Cisco Bug ID CSCwe15164“ASA:ASDM无法显示SFR选项卡，直到通过其CLI“唤醒”。
解决方法步骤：

1. 关闭ASDM管理器。
2. 获取对SFR的SSH访问，并将用户切换到root(sudo su)。
3. 执行上述步骤后，再次重新启动ASDM，ASDM可以加载Firepower(SFR)选项卡。



注意：此缺陷在最新的Firepower软件版本中已修复。有关详细信息，请查看缺陷详细信息。

问题14. ASDM不显示Firepower模块管理/配置

Firepower模块配置在ASDM上不可用。

故障排除 — 建议的操作

1. 确保ASA、ASDM、Firepower模块和操作系统版本兼容。 请参阅Cisco安全防火墙ASA版本说明、Cisco安全防火墙ASDM版本说明、Cisco安全防火墙ASA兼容性:

- ASA 9.14/ASDM 7.14/Firepower 6.6是ASA 5525-X、5545-X和5555-X上ASA FirePOWER模块的最终版本。
- ASA 9.12/ASDM 7.12/Firepower 6.4.0是ASA 5515-X和5585-X上ASA FirePOWER模块的最

终版本。

- ASA 9.9/ASDM 7.9(2)/Firepower 6.2.3是ASA 5506-X系列和5512-X上ASA FirePOWER模块的最终版本。
- 除非另有说明，否则ASDM版本与所有以前的ASA版本向后兼容。例如，ASDM 7.13(1)可以管理ASA 9.10(1)上的ASA 5516-X。
- 使用ASA 9.8(4.45)+、9.12(4.50)+、9.14(4.14)+和9.16(3.19)+的FirePOWER模块管理不支持ASDM;您必须使用FMC来管理这些版本的模块。这些ASA版本需要ASDM 7.18(1.152)或更高版本，但对ASA FirePOWER模块的ASDM支持以7.16结束。
- ASDM 7.13(1)和ASDM 7.14(1)不支持ASA 5512-X、5515-X、5585-X和ASASM;必须升级到ASDM 7.13(1.101)或7.14(1.48)才能恢复ASDM支持。

2. 如果版本兼容，请检查模块是否启动并正在运行：

<#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
```

如果模块关闭，则可以使用sw-module module reset命令重置模块，然后重新加载模块软件。

参考

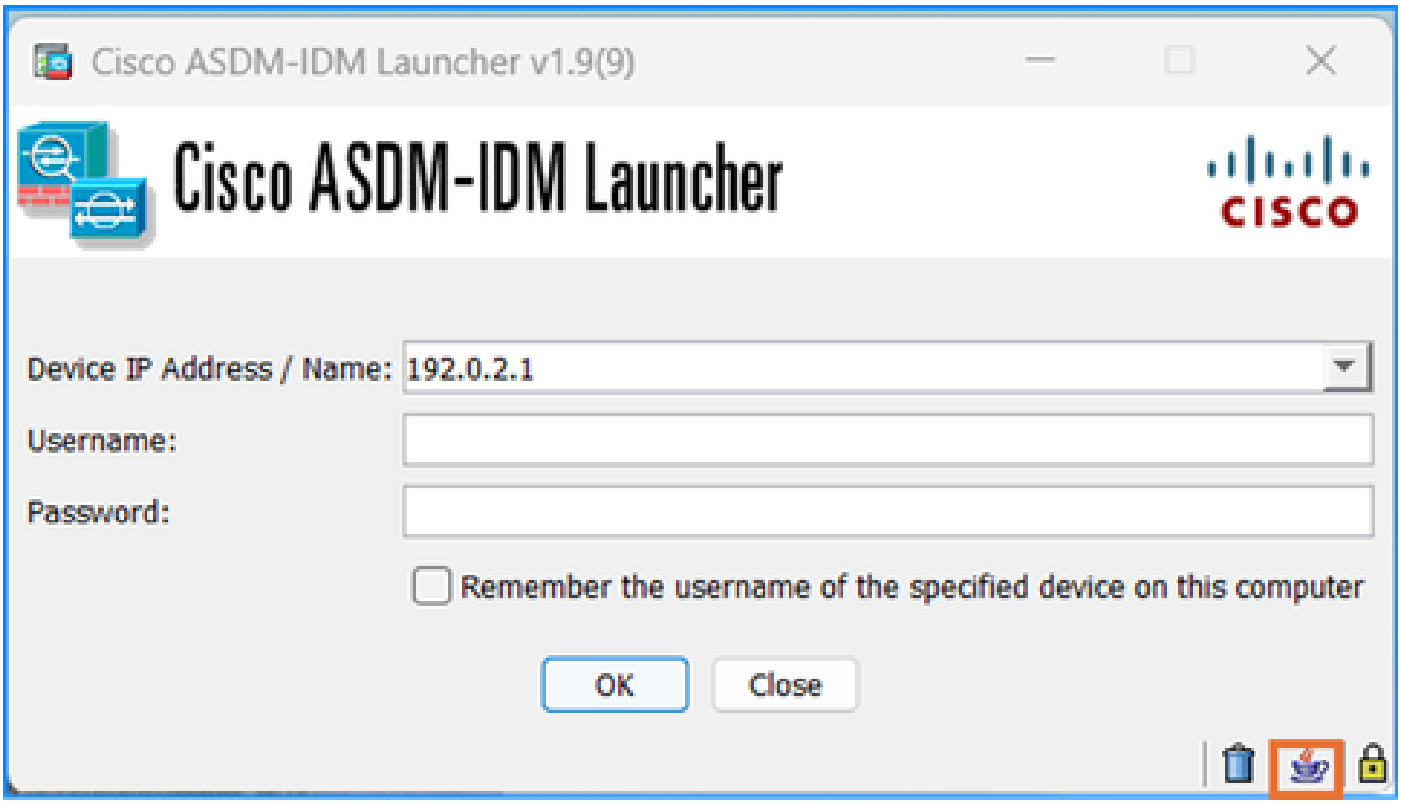
- 思科安全防火墙ASA版本说明
- 思科安全防火墙ASDM版本说明
- 思科安全防火墙ASA兼容性

问题15.在ASDM上无法访问安全客户端配置文件

Java控制台日志显示“java.lang.ArrayIndexOutOfBoundsException:3”错误消息：

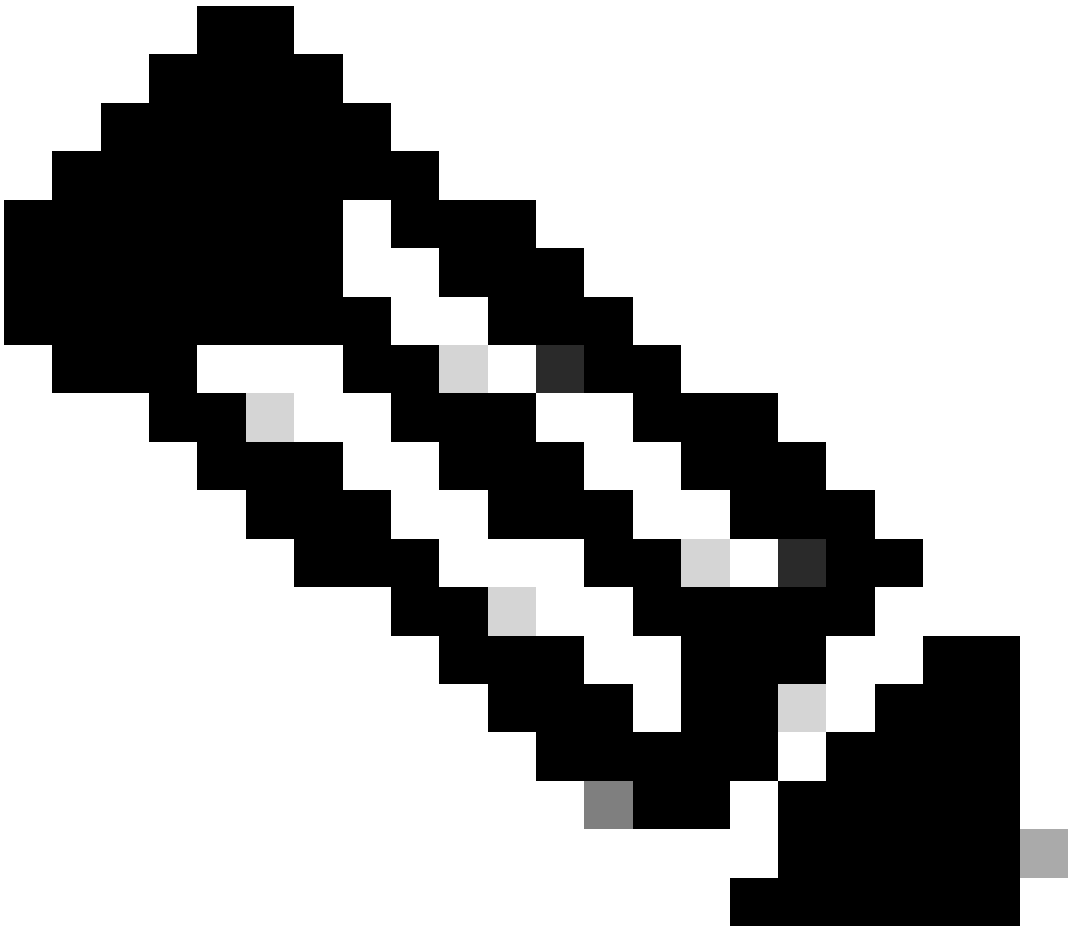
```
<#root>

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)
```

要验证此症状，请启用Java控制台日志：



故障排除 — 建议的操作

请参阅软件Cisco Bug ID CSCwi56155“Unable to access Secure Client Profile on ASDM”。



注意：此缺陷在最新的ASDM软件版本中已修复。有关详细信息，请查看缺陷详细信息。

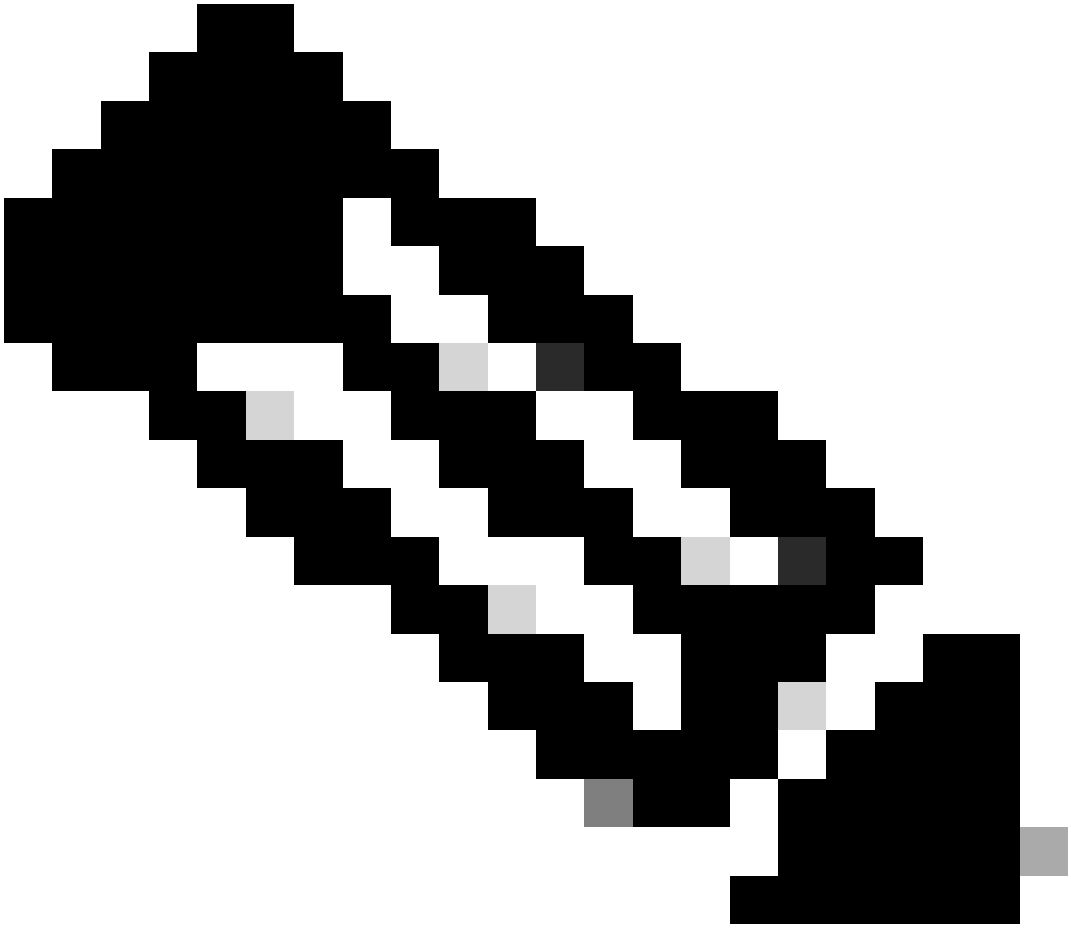
问题16.无法在ASDM上编辑安全客户端配置文件XML配置文件

如果ASA设备上存在AnyConnect映像的版本低于4.8版本，则无法在ASA设备上编辑ASDM Configuration > Remote Access VPN > Network(Client)Access中的安全客户端配置文件XML配置文件。

错误消息“设备上的安全客户端映像中没有配置文件编辑器插件。请转至“网络（客户端）访问”>“安全客户端软件”，安装安全客户端映像2.5版或更高版本，然后重试”。

故障排除 — 建议的操作

请参阅软件Cisco Bug ID CSCwk64399“ASDM — 无法编辑安全客户端配置文件”。解决方法是设置另一个优先级较低的AnyConnect映像。



注意：此缺陷在最新的ASDM软件版本中已修复。有关详细信息，请查看缺陷详细信息。

问题17.配置更改后安全客户端映像丢失

在ASDM Configuration > Network(Client)Access > Secure Client Profile中进行更改后，Configuration > Network(Client)Access > Secure Client Software中的映像丢失。

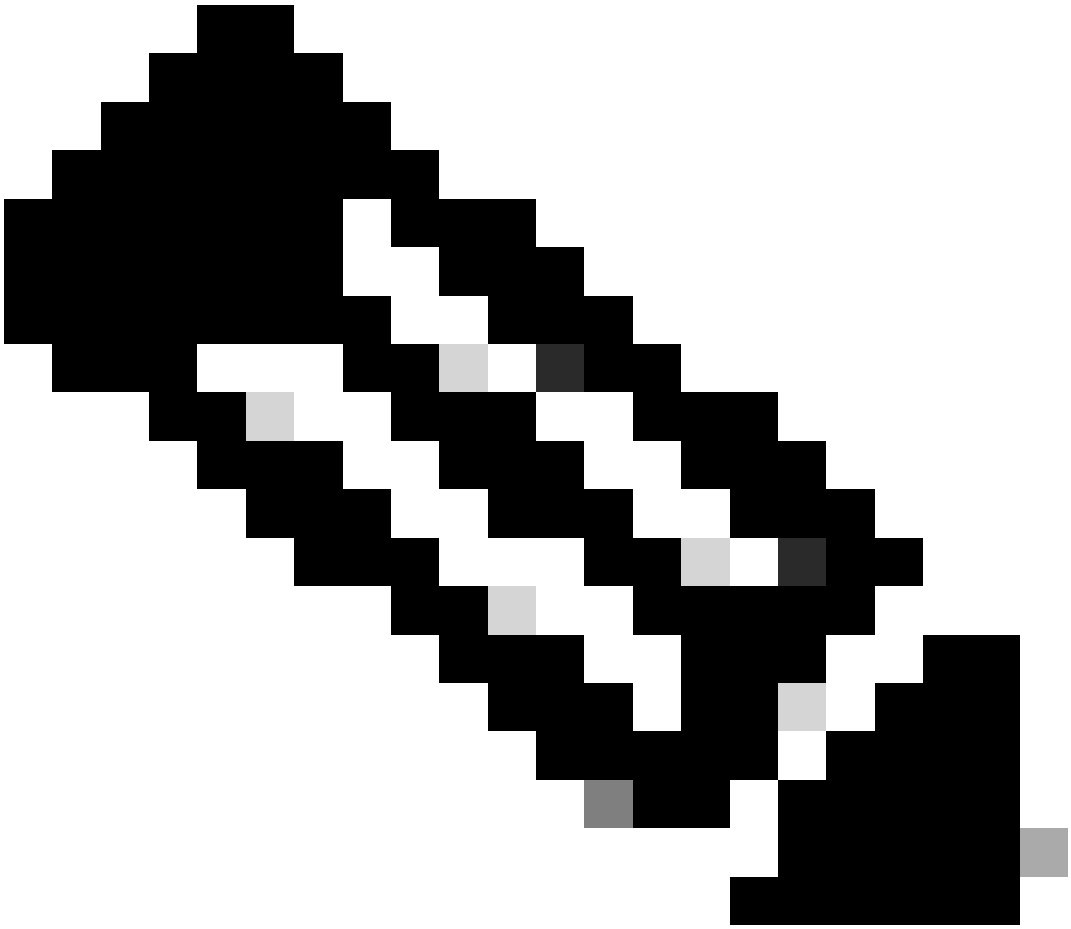
故障排除 — 建议的操作

请参阅软件Cisco Bug ID CSCwf23826 “Secure Client Software is not displayed after modifying the Secure Client Profile Editor in ASDM”。解决方法选项：

- 点击ASDM中的刷新图标

或者

- 关闭并重新打开ASDM



注意：此缺陷在最新的ASDM软件版本中已修复。有关详细信息，请查看缺陷详细信息。

问题 18. http server session-timeout和http server idle-timeout命令无效

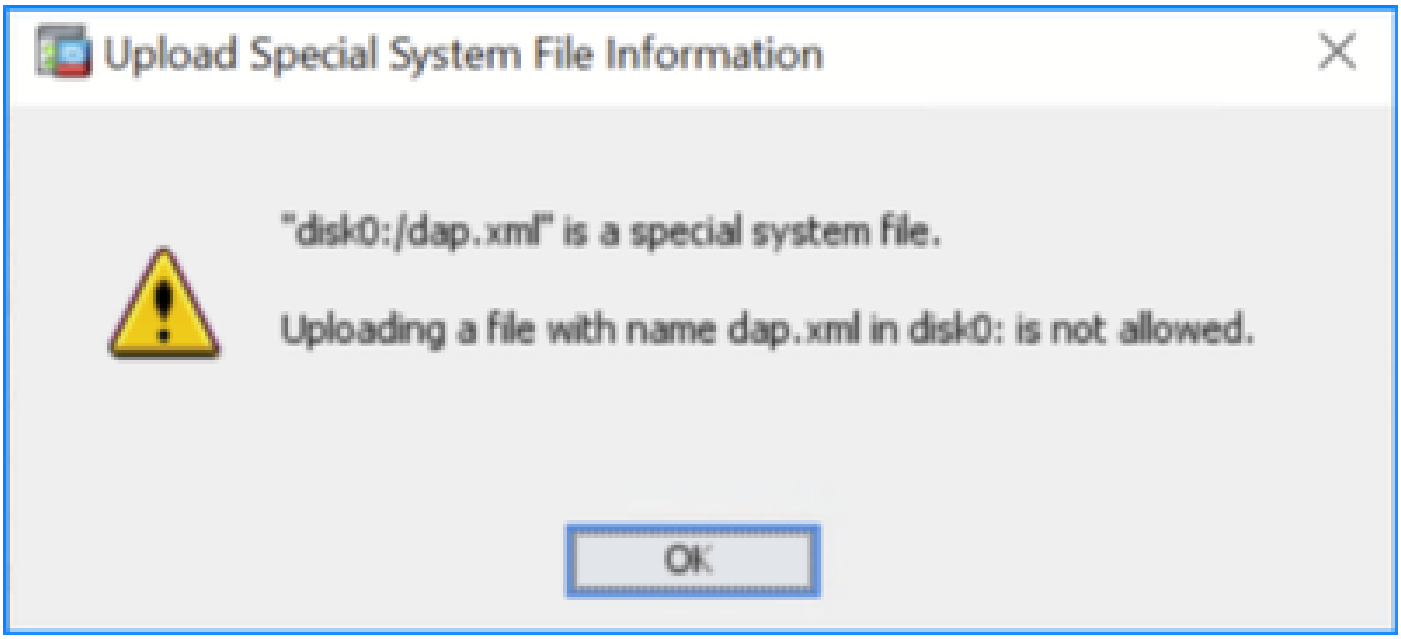
http server session-timeout和http server idle-timeout命令在多情景模式ASA中无效。

故障排除 — 建议的操作

请参阅软件Cisco Bug ID CSCtx41707“在多情景模式下支持http server timeout命令”。命令是可配置的，但值不起作用。

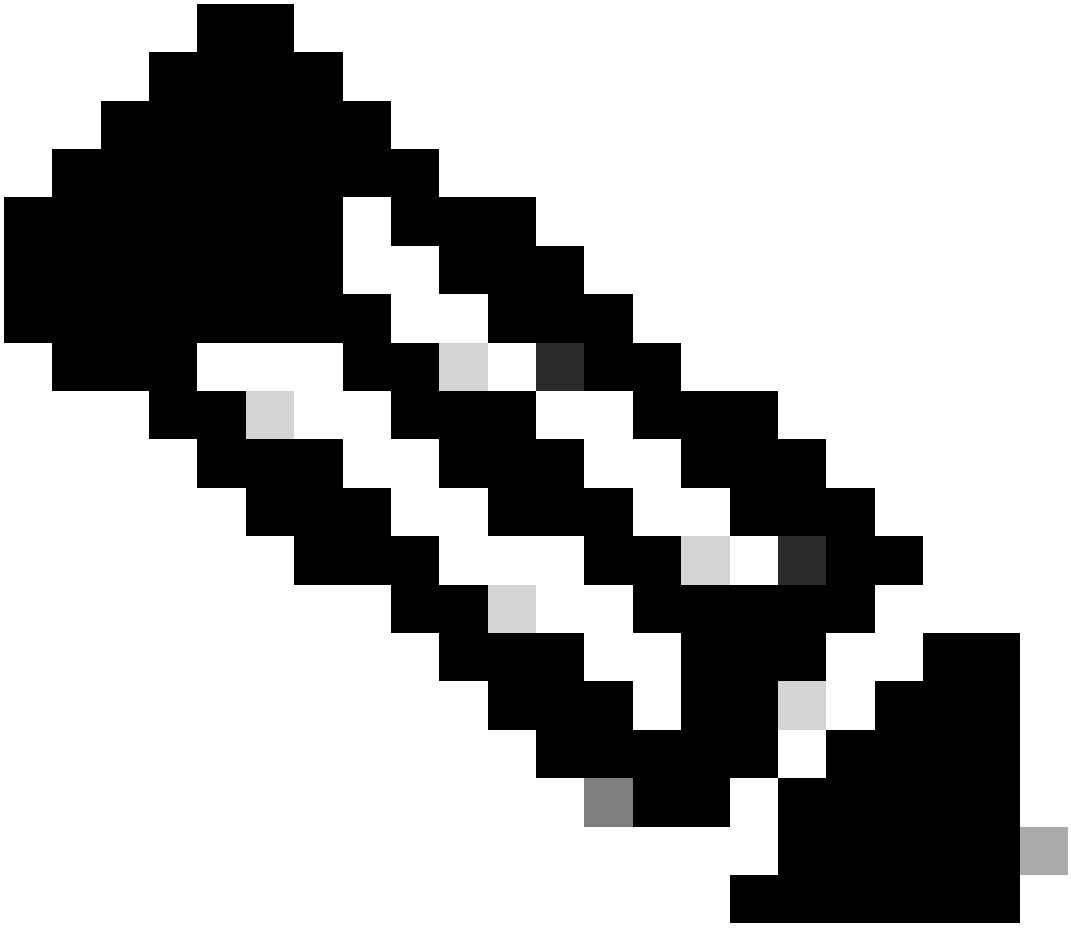
问题 19. ASDM上的Dap.xml复制失败

通过ASDM中的File Management窗口将dap.xml复制到ASA失败，错误为“disk0:/dap.xml is an special system file”。在disk0中上传名为dap.xml的文件：不允许”：



故障排除 — 建议的操作

请参阅软件Cisco Bug ID CSCvt62162“Cannot copy dap.xml using File Management in ASDM 7.13.1”。解决方法是使用FTP或TFTP等协议将文件直接复制到ASA。



注意：此缺陷在最新的ASDM软件版本中已修复。有关详细信息，请查看缺陷详细信息。

问题20.ASDM上看不到IKE策略和IPSEC提议

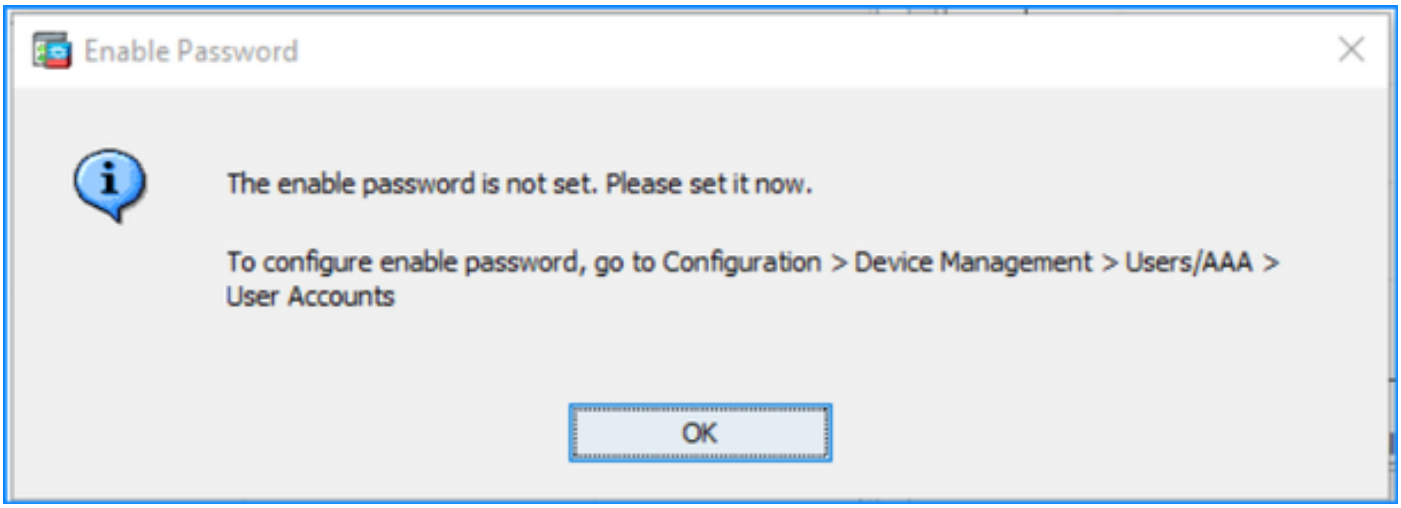
ASDM不会在配置 > 站点到站点VPN窗口中显示IKE策略和IPSEC提议。

故障排除 — 建议的操作

请参阅软件Cisco Bug ID CSCwm42701“ASDM display blank in IKE policies and IPSEC proposals（IKE策略和IPSEC建议选项卡）”。

问题21. ASDM显示消息“The enable password not set.请立即设置。”

ASDM显示消息“未设置启用密码。请立即设置。” 在命令行中更改启用密码后：



故障排除 — 建议的操作

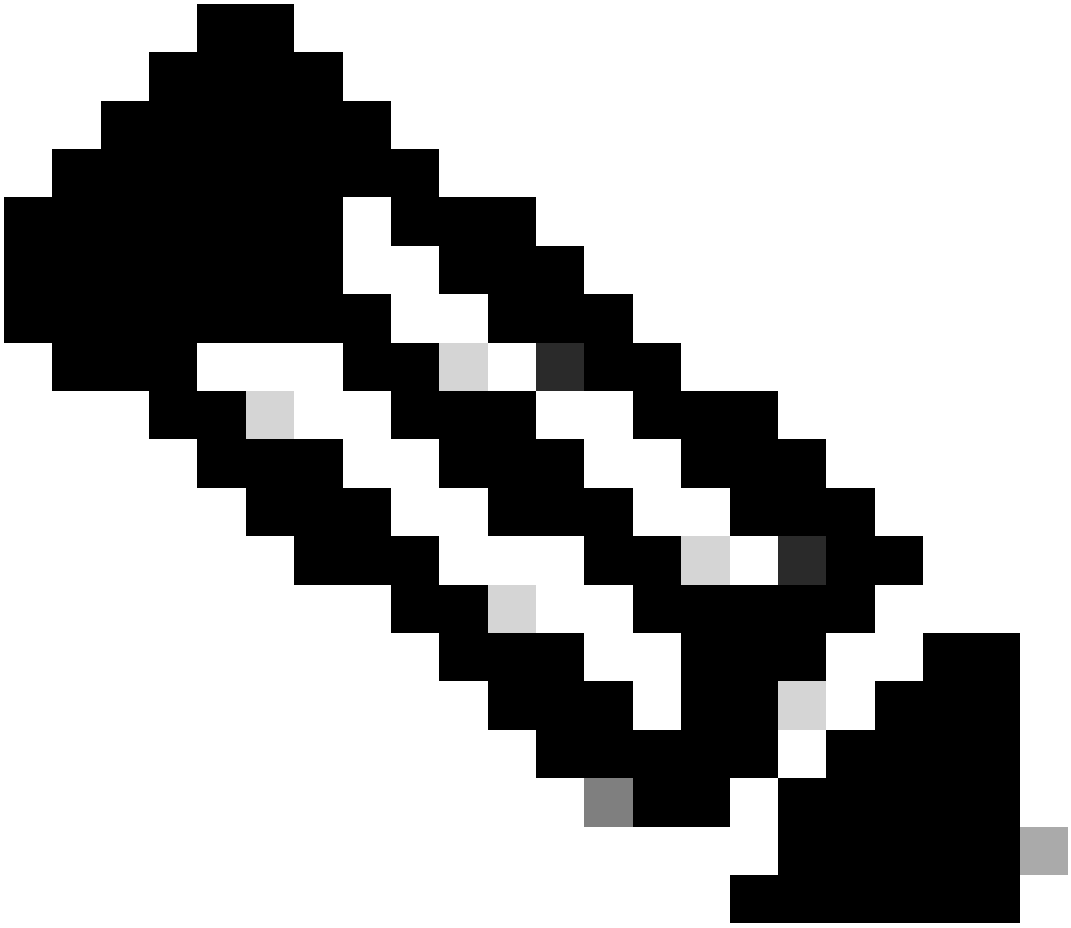
请参阅软件Cisco Bug ID CSCvq42317“ASDM prompts to change enable password after it is set on CLI”。

问题 22. 刷新ASDM UI后，ASDN对象消失

将对象组和对象主机添加到现有对象组时，刷新ASDM后，对象组从ASDM列表中消失。对象名称必须以数字开头，此缺陷才能匹配。

故障排除 — 建议的操作

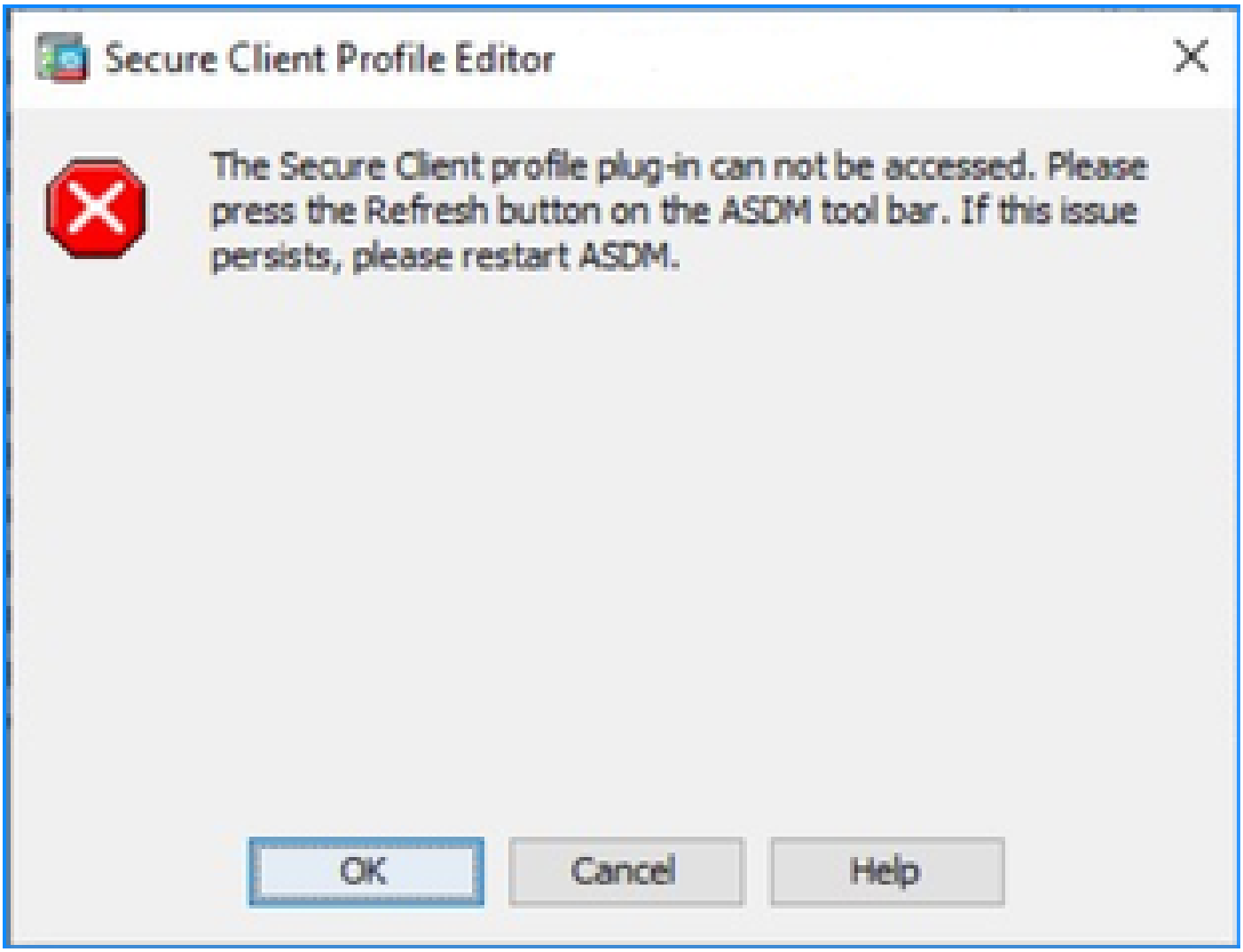
请参阅软件Cisco Bug ID CSCwf71723“ASDM loss configured objects/object groups”。



注意：此缺陷在最新的ASDM软件版本中已修复。有关详细信息，请查看缺陷详细信息。

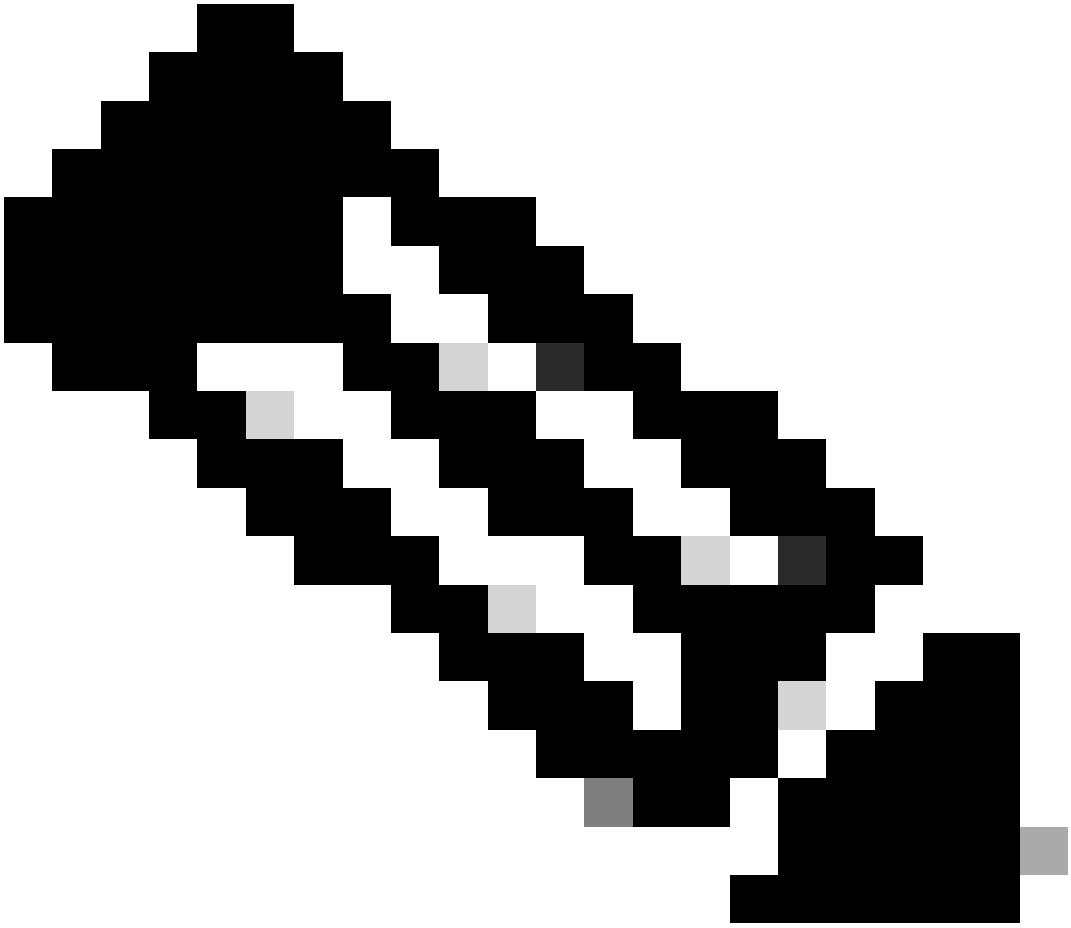
问题23.无法为低于4.5的版本编辑AnyConnect客户端配置文件

无法为4.5版之前的AnyConnect配置文件编辑AnyConnect客户端配置文件。错误消息为“The Secure Client profile plug-in cannot be access.请按ASDM工具栏上的“刷新”按钮。如果此问题仍然存在，请重新启动ASDM。":



故障排除 — 建议的操作

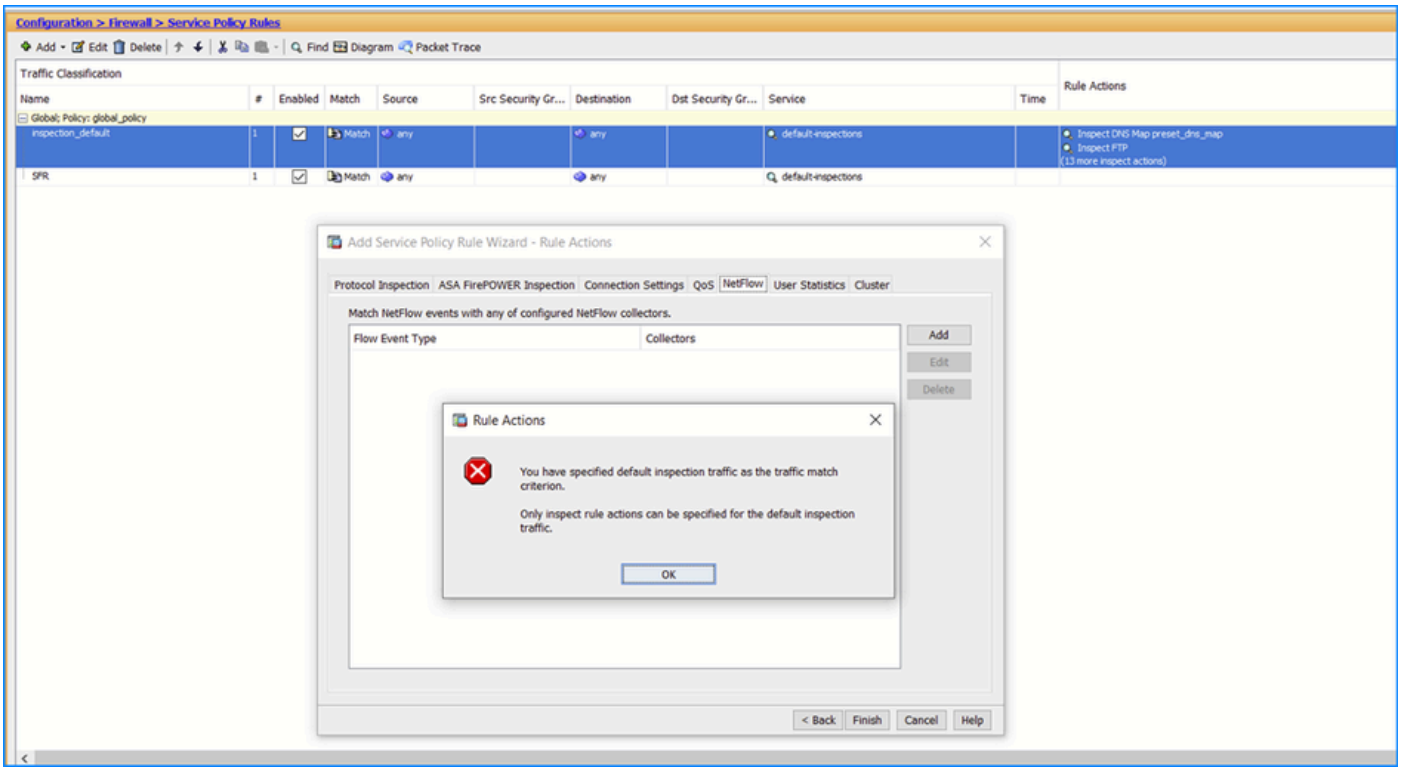
请参阅软件Cisco Bug ID CSCwf16947“ASDM - Unable to load Anyconnect Profile Editor”。



注意：此缺陷在最新的ASDM软件版本中已修复。有关详细信息，请查看缺陷详细信息。

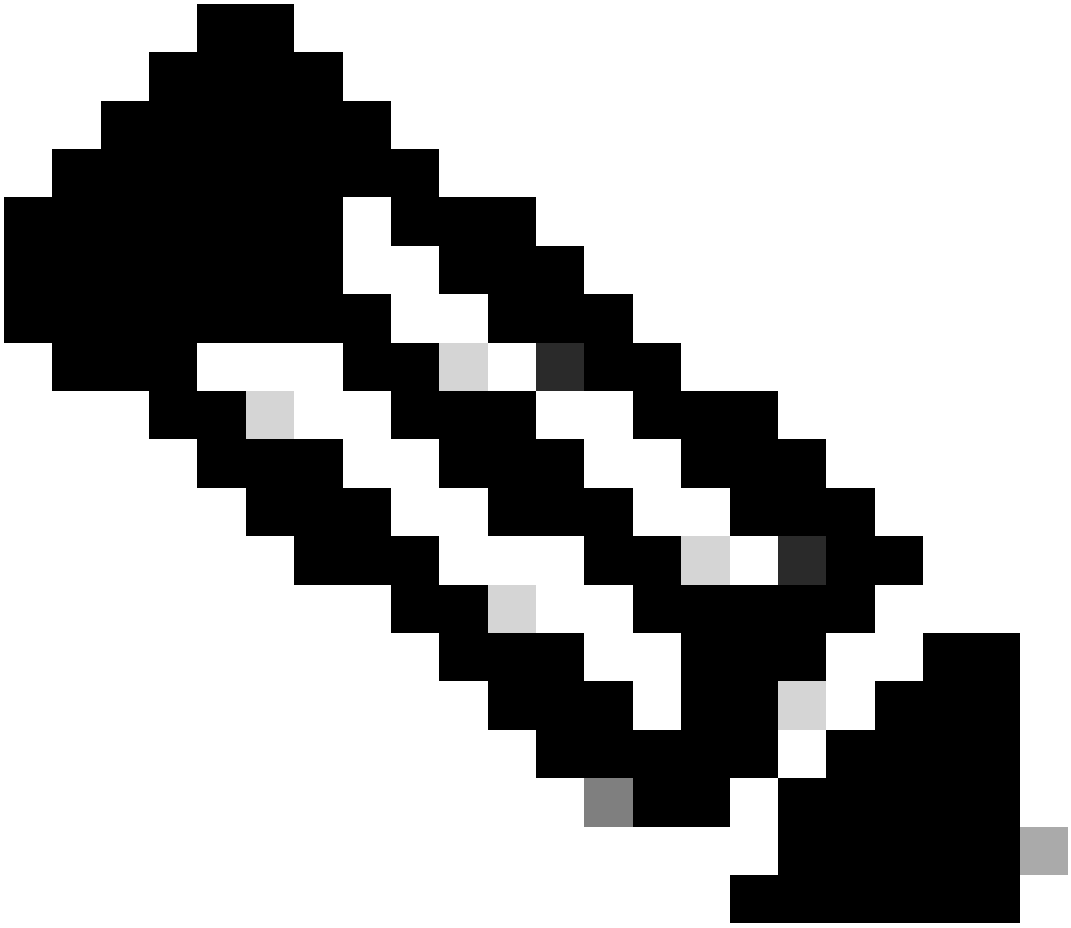
问题24.无法导航到Edit Service Policy > Rule Actions > ASA FirePOWER Inspection选项卡

在ASDM 7.8.2版中，用户无法导航到Edit Service Policy > Rule Actions > ASA FirePOWER Inspection选项卡，并显示以下错误：“您已指定默认检测流量作为流量匹配条件。只能为默认检测流量指定检测规则操作。" 即使选择了用于重定向的ACL，也会出现这种情况：



故障排除 — 建议的操作

请参阅软件Cisco Bug ID CSCvg15782“ASDM — 升级到版本7.8(2)后无法查看修改SFR流量重定向”。解决方法是使用CLI编辑策略映射配置。



注意：此缺陷在最新的ASDM软件版本中已修复。有关详细信息，请查看缺陷详细信息。

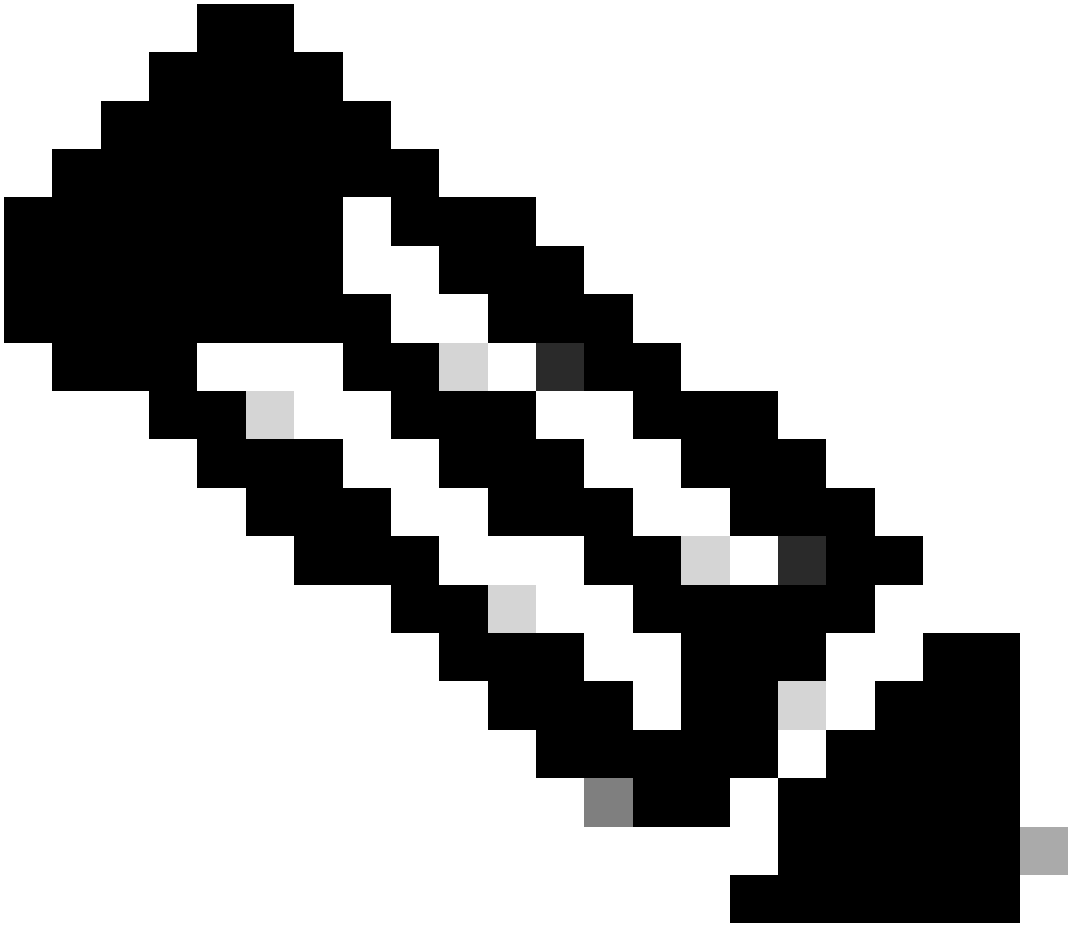
问题25. ASDM上的AnyConnect映像5.1版和AnyConnect配置文件编辑器

在安全客户端软件5.1版中观察到以下症状：

1. 加载Win/Mac/Linux软件包时未列出组策略模块名称
2. ASDM无法打开AnyConnect配置文件编辑器。

故障排除 — 建议的操作

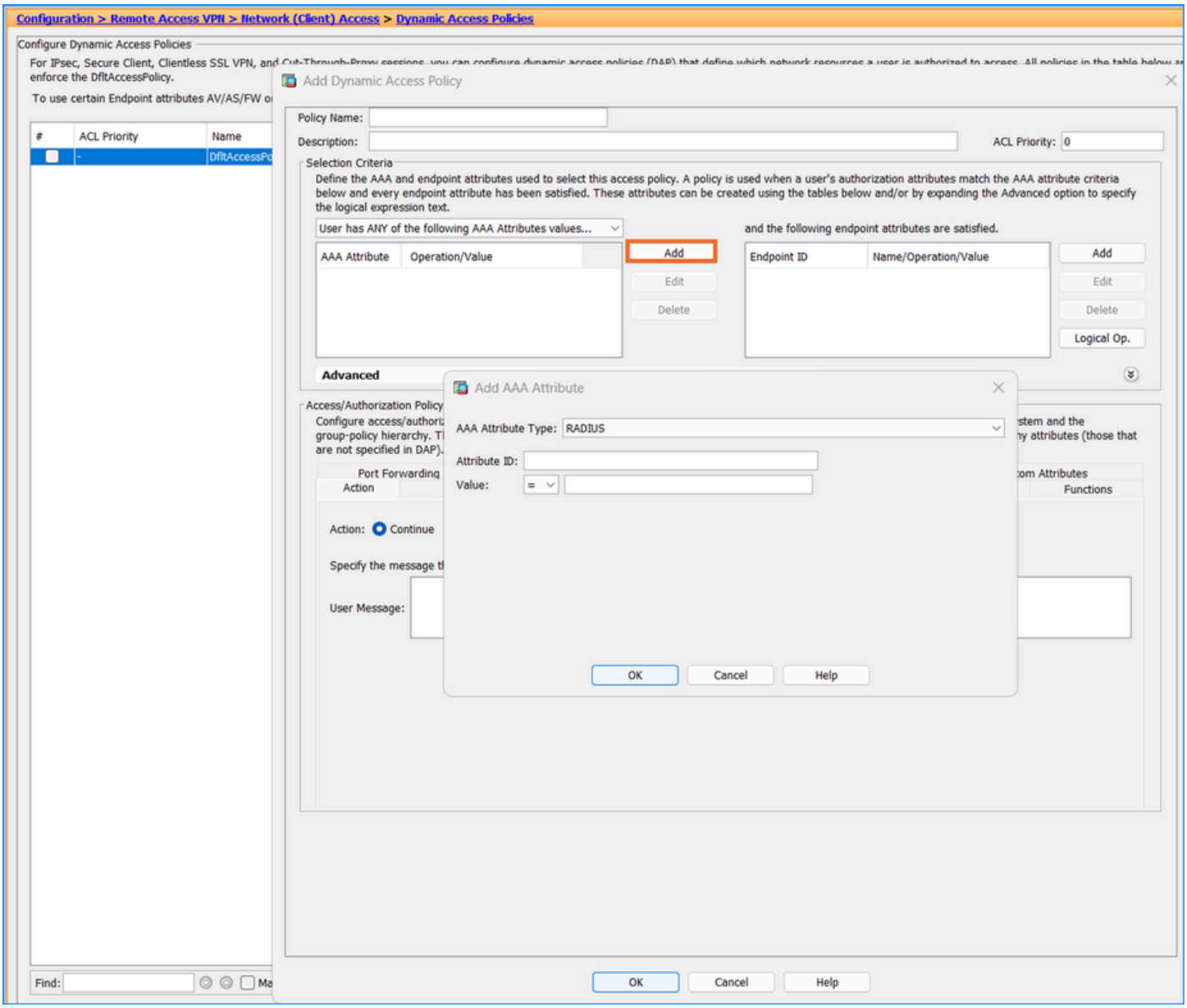
请参阅软件Cisco Bug ID CSCwh74417“ASDM:使用CSC映像5.1时，无法加载AnyConnect配置文件编辑器和组策略。解决方法是使用安全客户端的较低版本。



注意：此缺陷在最新的ASDM软件版本中已修复。有关详细信息，请查看缺陷详细信息。

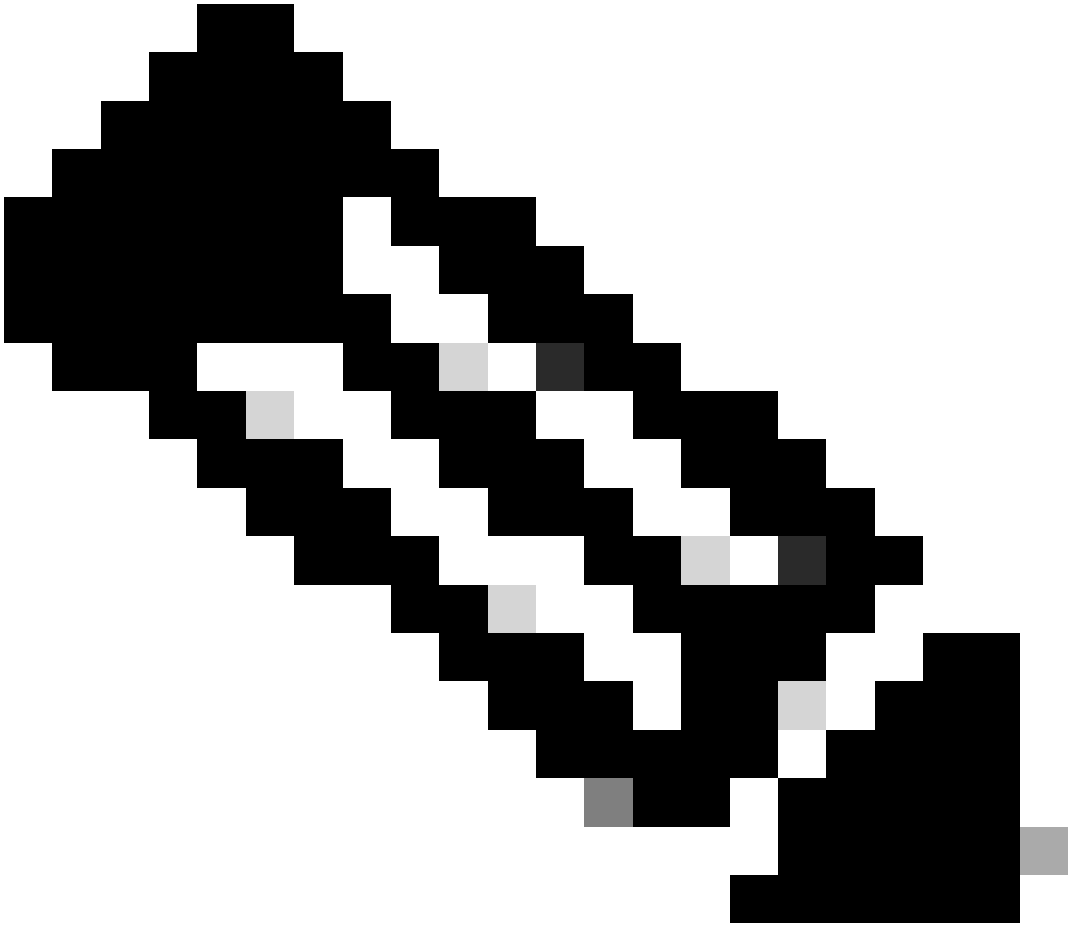
问题 26. AAA属性类型(Radius/LDAP)在ASDM中不可见

AAA属性类型(Radius/LDAP)在ASDM > Configuration > Remote Access VPN > Network(Client)Access > Dynamic Access Policies > Add > On AAA attribute字段>Add >选择Radius或LDAP中不可见：



故障排除 — 建议的操作

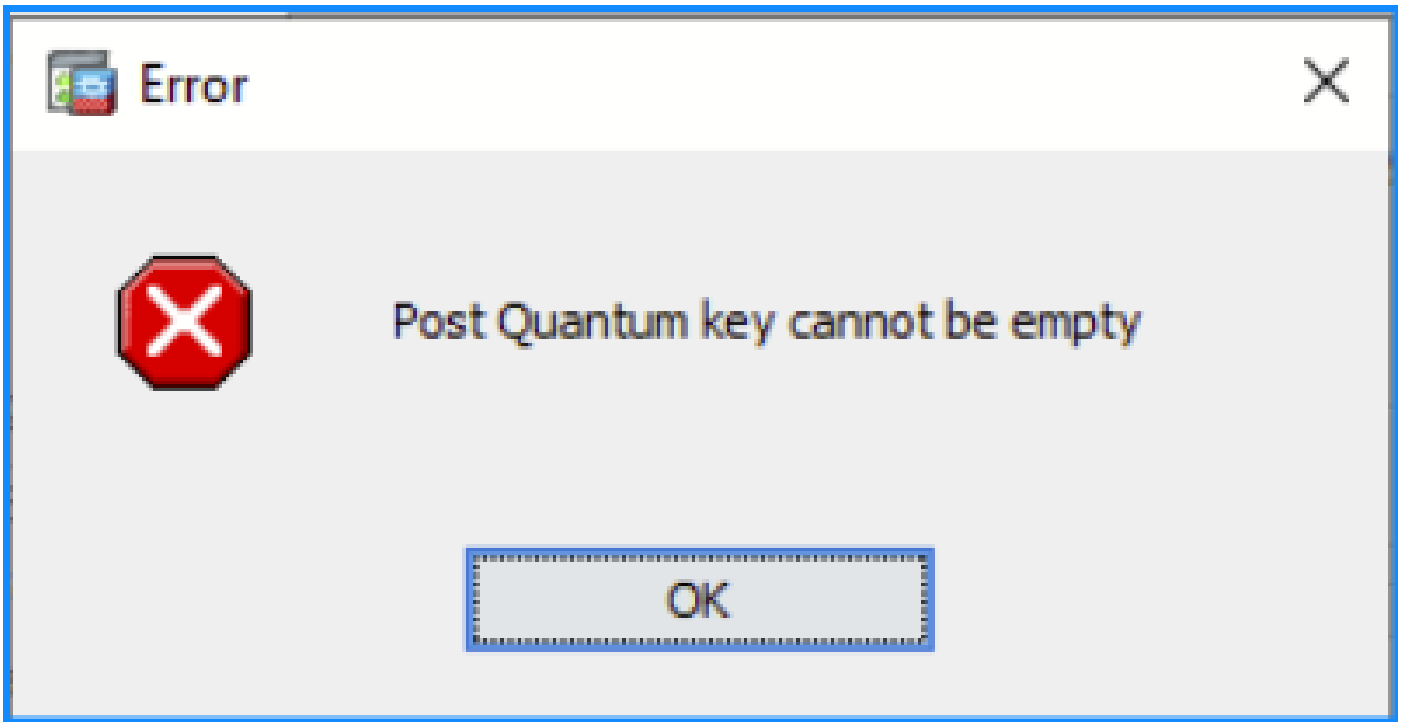
请参阅软件Cisco Bug ID CSCwa99370“ASDM:ASDM:DAP配置缺少AAA属性类型(Radius/LDAP)”和Cisco Bug ID CSCwd16386“ASDM:DAP配置缺少AAA属性类型(Radius/LDAP)”。



注意：这些缺陷在最新的ASDM软件版本中已修复。有关详细信息，请查看缺陷详细信息。

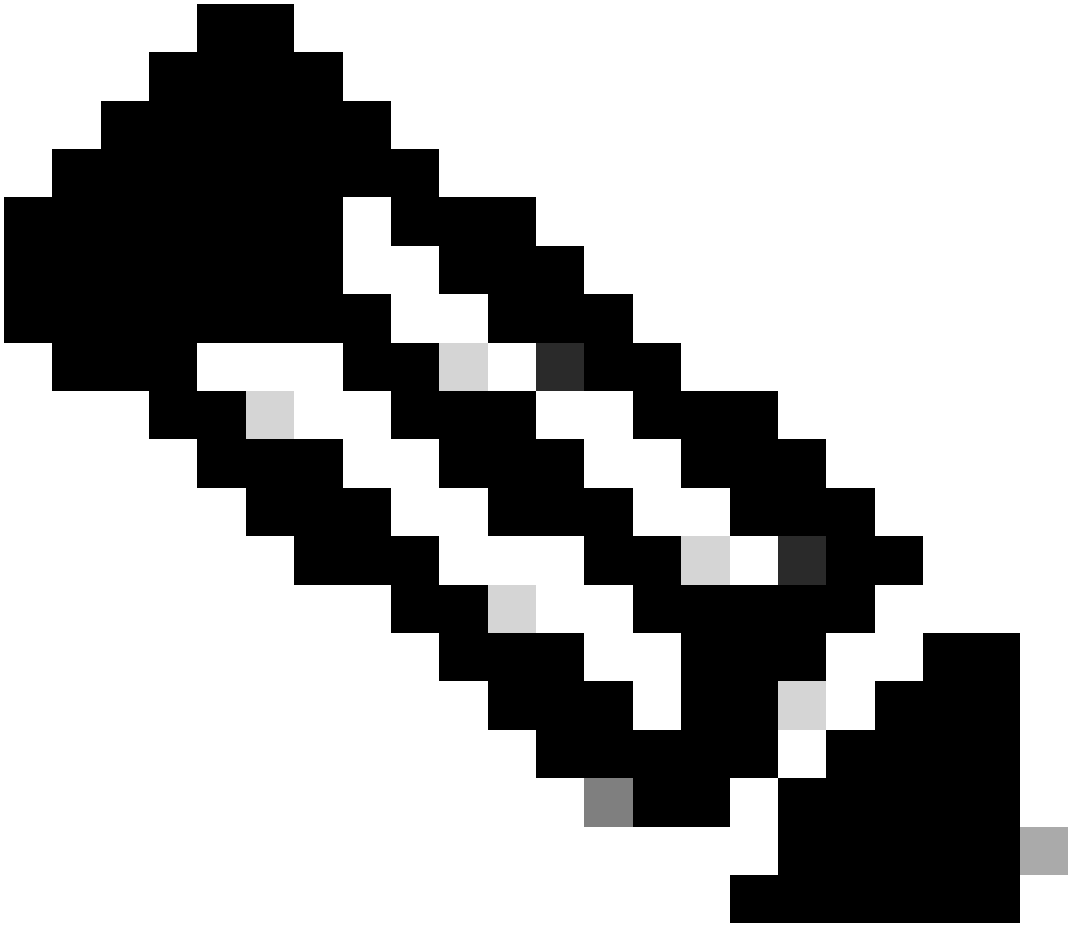
问题 27. ASDM上显示“Post Quantum key cannot be empty”错误

编辑ASDM > Configuration > Remote Access VPN > Network(Client)Access > IPsec(IKEv2)Connection Profiles中的Advanced部分时，显示错误“Post Quantum key cannot be empty”(Post Quantum key cannot be empty):



故障排除 — 建议的操作

请参阅软件Cisco Bug ID CSCwe58266“ASDM IKev2 configuration - Post Quantum Key cannot be empty error message”。



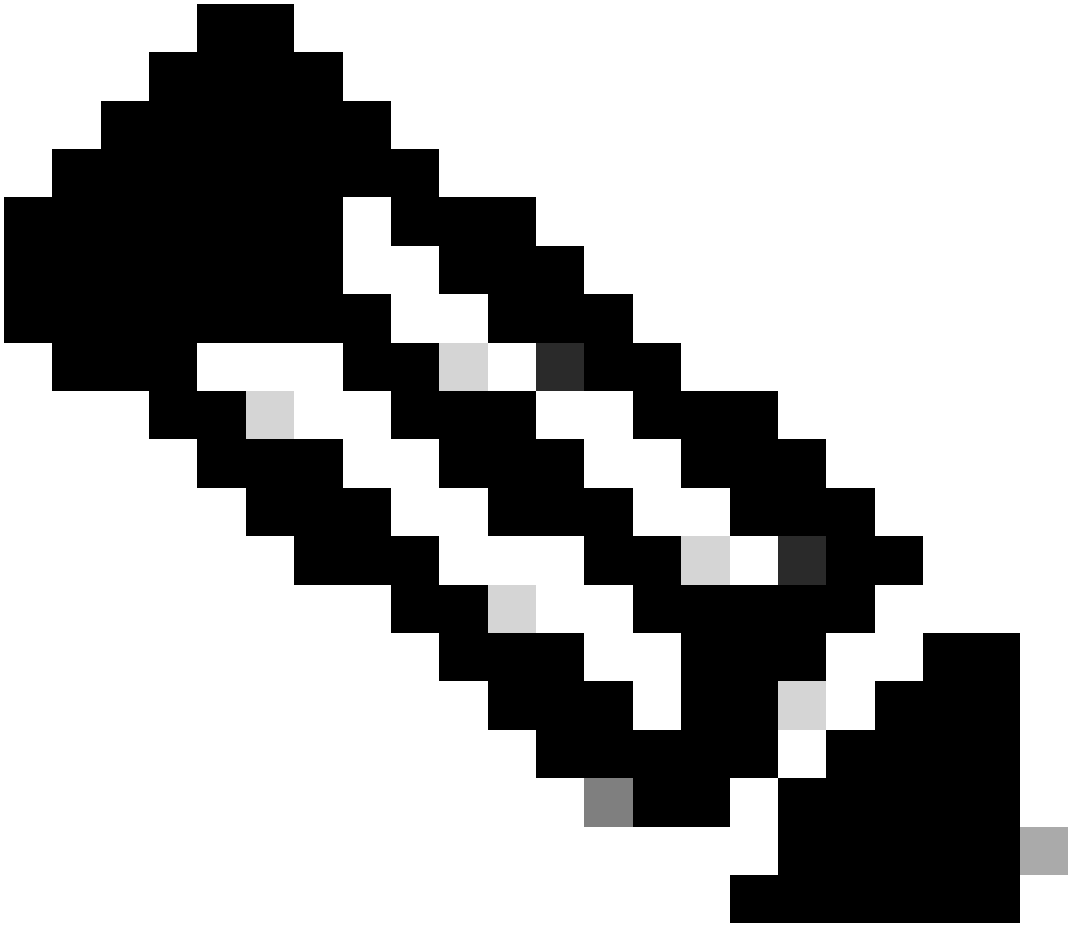
注意：此缺陷在最新的ASDM软件版本中已修复。有关详细信息，请查看缺陷详细信息。

问题 28. ASDM在使用“使用位置”选项时不会显示任何结果

当使用选项“使用位置”找到时，ASDM不会显示任何结果，方法是导航到Configuration > Firewall > Objects > Network Objects/Groups，然后右键点击Object。

故障排除 — 建议的操作

请参阅软件Cisco Bug ID CSCwd98702的“Where used”选项（在ASDM不工作的情况下）。



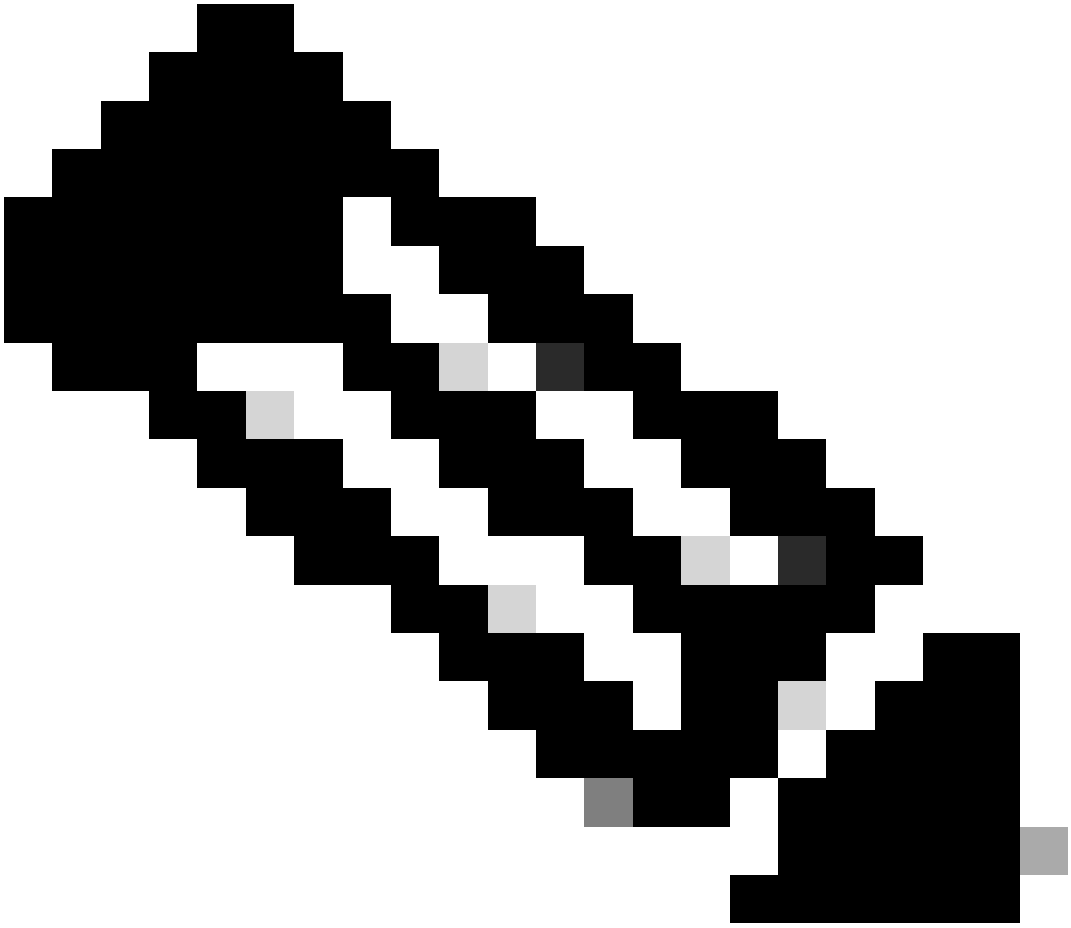
注意：此缺陷在最新的ASDM软件版本中已修复。有关详细信息，请查看缺陷详细信息。

问题 29. 删除网络对象时，无法删除警告消息“[网络对象]，因为它用于以下内容”

在Configuration > Firewall > Objects > NetworkObjects/Groups中删除网络组中引用的网络对象时，ASDM不会显示警告消息“由于以下情况而无法删除网络对象”。

故障排除 — 建议的操作

请参阅软件Cisco Bug ID CSCwe67056 “[网络对象] cannot be deleted because it is used in the following" warning not appearing"（无法删除此软件所使用的网络对象）。



注意：此缺陷在最新的ASDM软件版本中已修复。有关详细信息，请查看缺陷详细信息。

问题 30. ASDM中网络对象/组选项卡的可用性问题

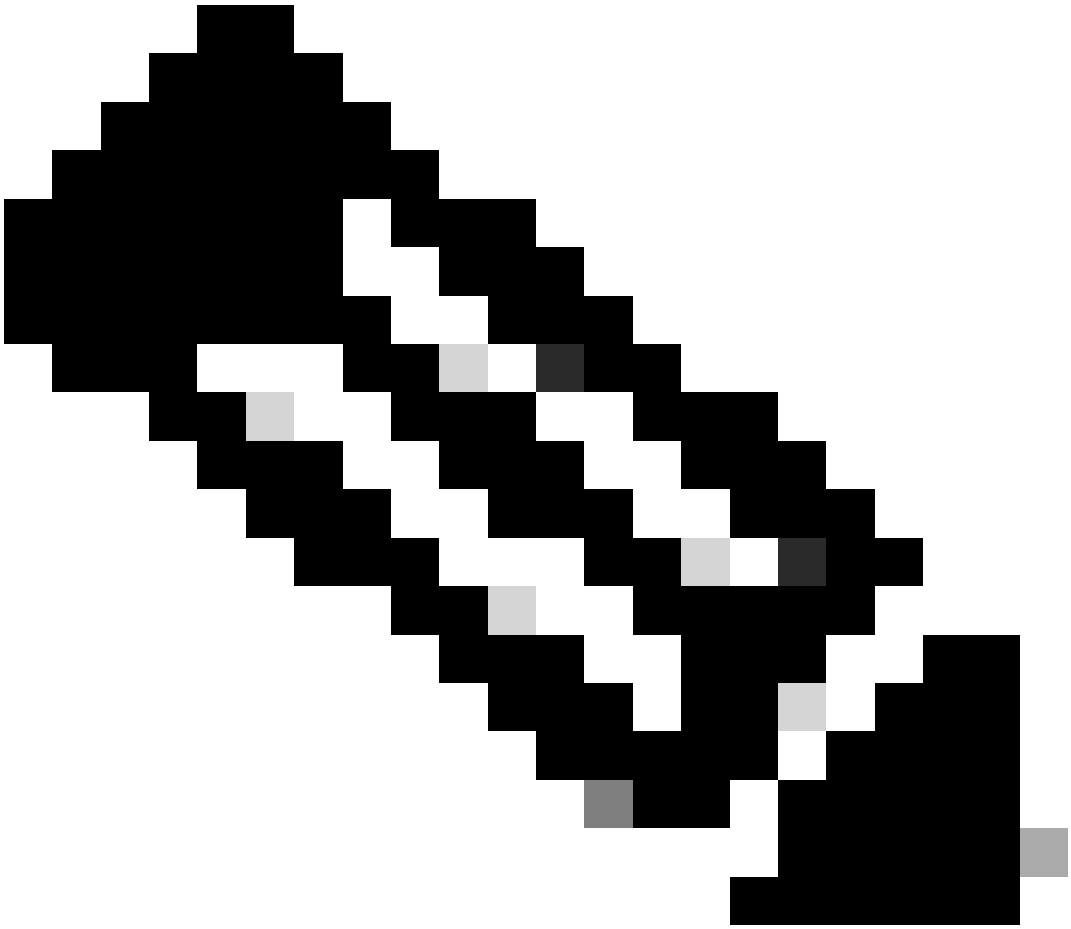
观察到以下一个或多个症状：

- “Add/Edit Object Group Windows”的“Create new Object Member”部分中的“Name”文本输入标记为“optional”。 但是，除非输入名称，否则用于创建和添加对象的“Add>>”按钮将被禁用。
- 当用户点击“使用位置……”时打开的“使用实例”选项卡 上下文菜单仅列出直接引用该对象的实体（ACL、路由映射、对象组）。它还必须递归地列出第二、第三等。顺序引用（即使用包含对象的对象组的ACL也必须列为对象的“用法”）。
- 上下文菜单中的“删除”操作也会显示此行为。它自动删除直接引用该对象的任何实体（如果删除对象时该实体变为空）。 当第二次、第三次等等，它不会以这种方式运行。由于删除了对象和第一个订单引用，订单引用将变为空。

用户可以相信ASDM会阻止由于从其余配置中删除对象而变为空的实体。然而，情况未必如此。

故障排除 — 建议的操作

请参阅软件Cisco Bug ID CSCwe86257“Usability of Network Objects/Group Tab in ASDM”。

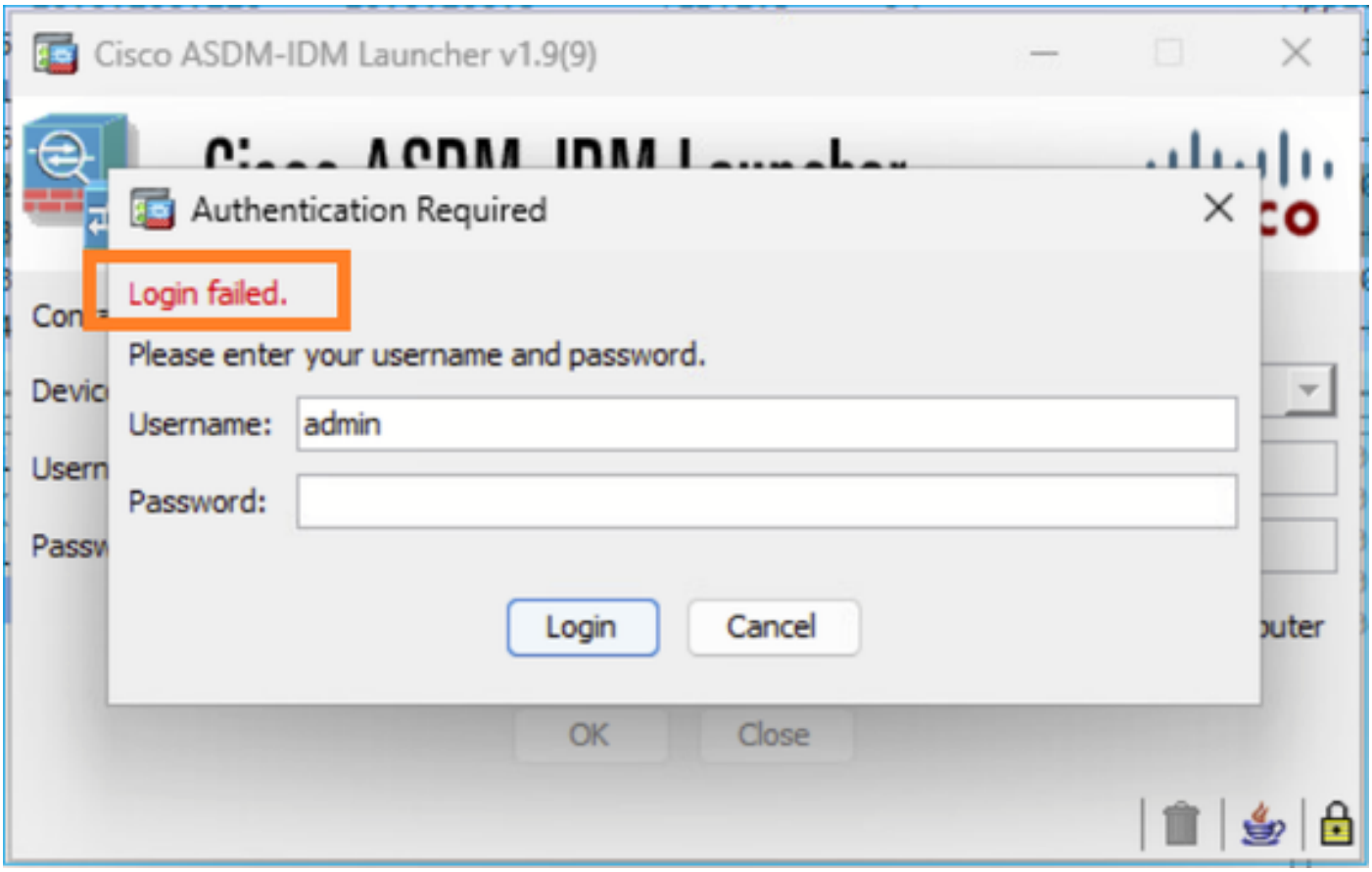


注意：此缺陷在最新的ASDM软件版本中已修复。有关详细信息，请查看缺陷详细信息。

排除ASDM身份验证问题

问题1. ASDM登录失败

ASDM UI上显示的错误为：



故障排除 — 建议的操作

当您在同一接口上同时启用HTTP和Webvpn Cisco安全客户端(AnyConnect)时，可以看到此错误。因此，必须满足以下所有条件：

1. AnyConnect/Cisco安全客户端在接口上启用
2. HTTP服务器在与AnyConnect/Cisco安全客户端相同的接口和端口上启用

示例：

```
<#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
```

故障排除提示：启用“debug http 255”，您可以看到ASDM和Webvpn之间的冲突：

```
<#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
```

请注意，尽管登录失败，但ASA系统日志显示身份验证成功：

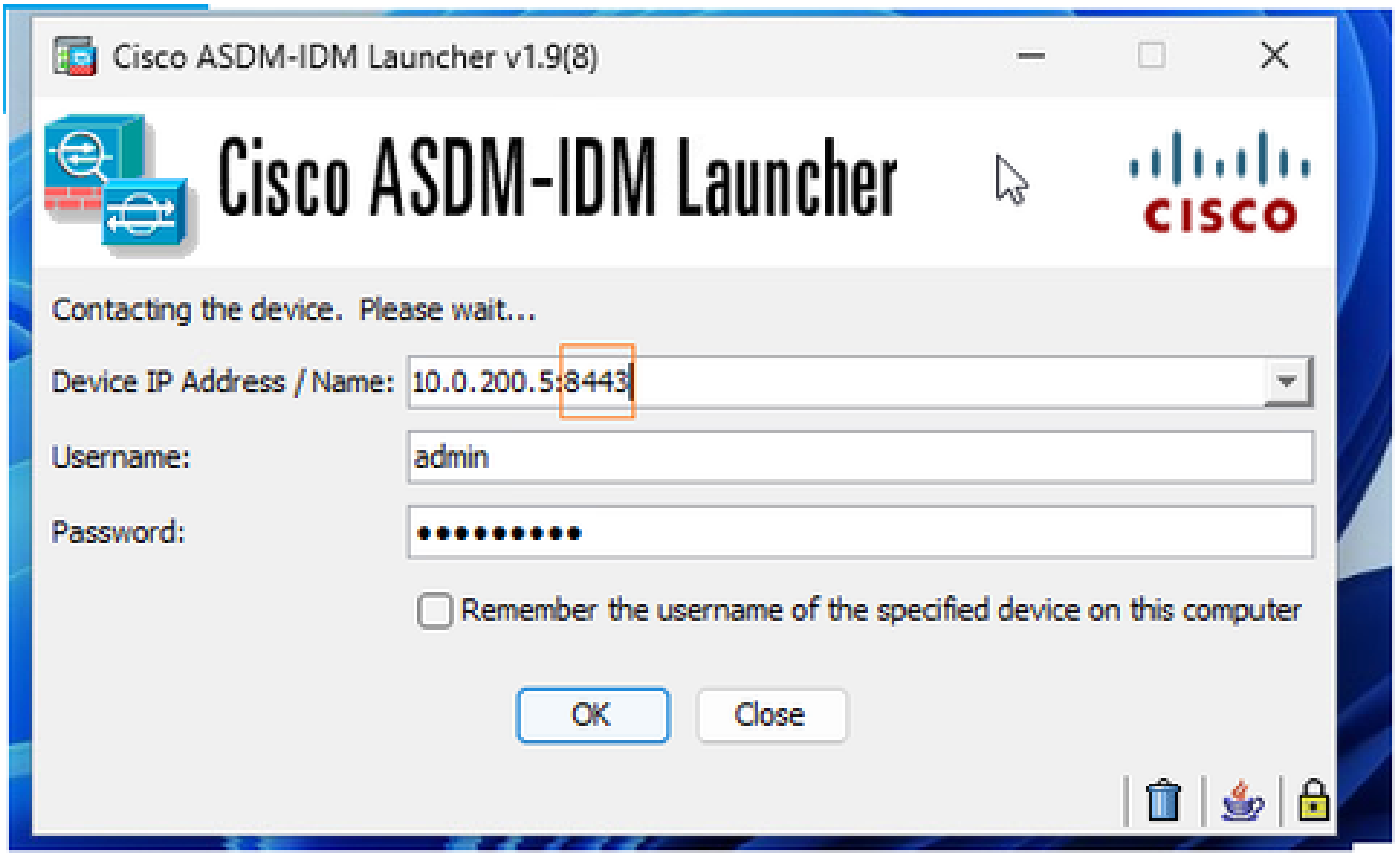
```
<#root>
asa#
show logging

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
```

解决方法

解决方法1

更改ASA HTTP服务器的TCP端口，例如：

```
<#root>

ciscoasa#

configure terminal

ciscoasa(config)#

http server enable 8443
```



解决方法2

更改AnyConnect/Cisco安全客户端的TCP端口，例如：

```
<#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
```

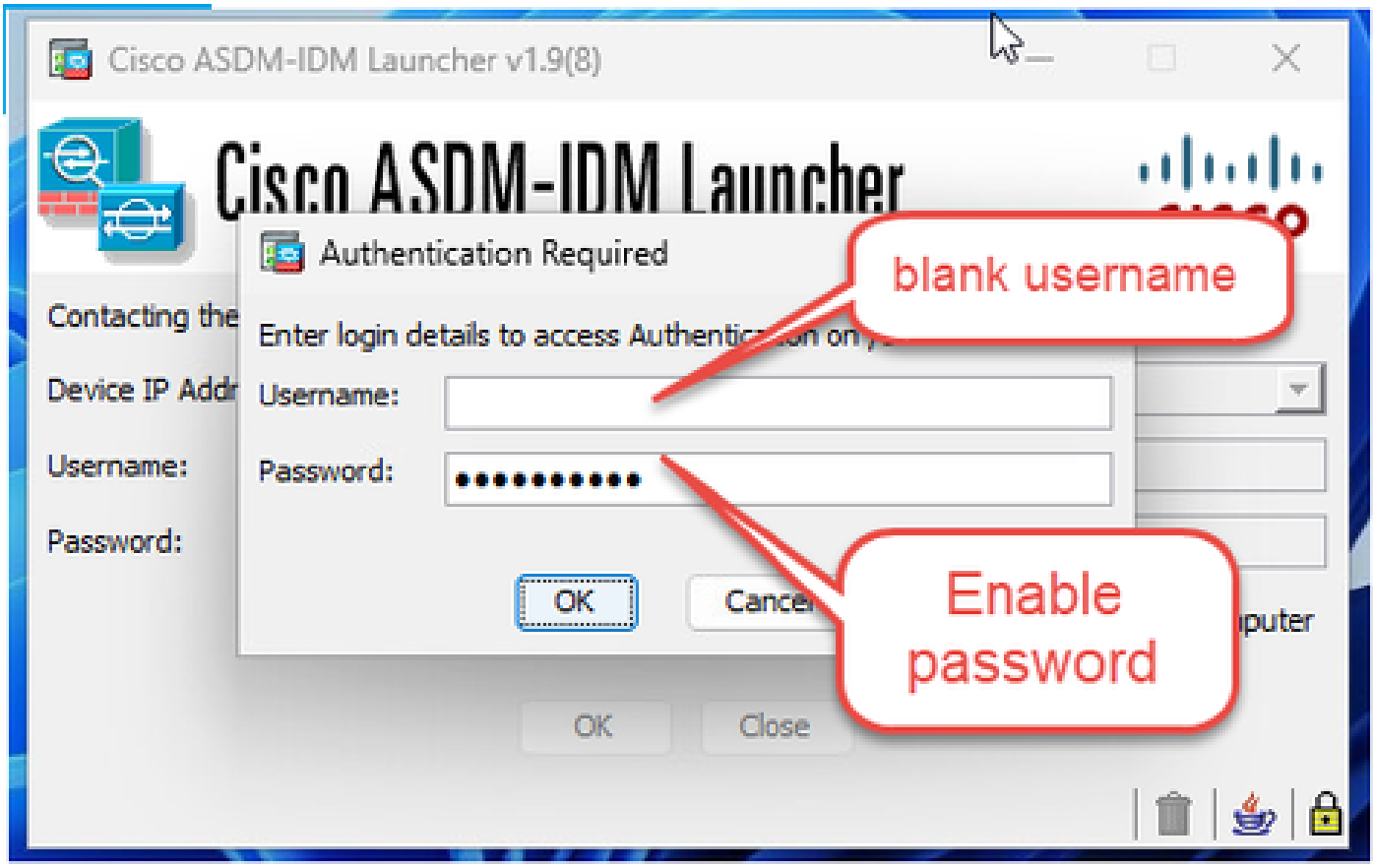
解决方法3

另一种解决方法是删除“aaa authentication http console”配置：

<#root>

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

在这种情况下，您只需使用使能密码即可登录ASDM:



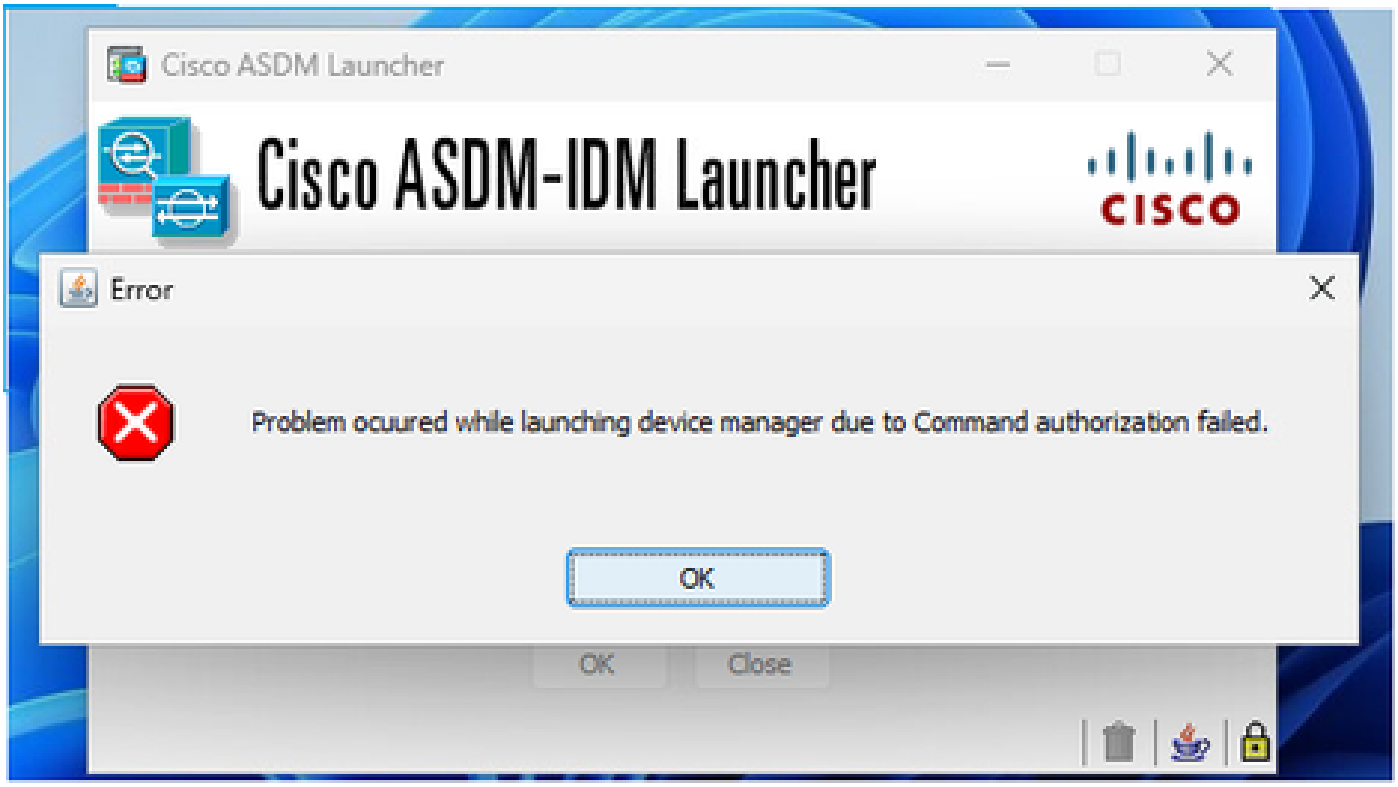
相关缺陷

Cisco Bug ID CSCwb67583

当在同一接口上启用webvpn和ASDM时添加警告

问题2. ASDM命令授权失败

ASDM UI上显示的错误为：



故障排除 — 建议的步骤

检查ASA上的AAA配置并确保：

- 您还配置了aaa身份验证。
- 如果使用远程身份验证服务器，则它可访问并授权命令。

参考

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

问题3.配置ASDM只读访问

有时您想为ASDM用户提供只读访问权限。

故障排除 — 建议的步骤

创建具有自定义权限级别(5)的新用户，例如：

<#root>

asa(config)#

username [username] password [password] privilege 5

此命令创建权限级别为5的用户，即“仅监控”级别。用所需的用户名和密码替换“[username]”和“[password]”。

详细信息

本地命令授权允许您将命令分配到16个权限级别（0到15）之一。 默认情况下，每个命令都分配到权限级别0或15。您可以将每个用户定义为处于特定权限级别，每个用户都可以在分配的权限级别或更低级别输入任何命令。ASA支持本地数据库、RADIUS服务器或LDAP服务器中定义的用户权限级别（如果将LDAP属性映射到RADIUS属性）。

步骤

第 1 步	选择Configuration > Device Management > Users/AAA > AAA Access > Authorization。
步骤 2	选中Enable authorization for ASA command access > Enable复选框。
步骤 3	从Server Group下拉列表中选择LOCAL。
步骤 4	启用本地命令授权时，您可以选择手动为单个命令或命令组分配权限级别，或启用预定义的用户帐户权限。 ·单击Set ASDM Defined User Roles以使用预定义的用户帐户权限。 系统将显示ASDM Defined User Roles Setup对话框。单击Yes使用预定义的用户帐户权限：Admin(权限级别15，对所有CLI命令具有完全访问权限；只读(权限级别5，具有只读访问权限);和Monitor Only(权限级别3，仅具有对Monitoring部分的访问权限)。 ·单击Configure Command Privileges手动配置命令级别。 系统将显示Command Privileges Setup对话框。您可以通过从命令模式下拉列表中选择所有模式来查看所有命令，也可以选择配置模式以查看该模式下可用的命令。例如，如果选择情景，则可以查看情景配置模式下可用的所有命令。如果在用户EXEC模式或特权EXEC模式以及配置模式下可以输入命令，并且该命令在每个模式下执行不同的操作，则可以分别设置这些模式的权限级别。

	Variant列显示show、clear或cmd。您只能为命令的show、clear或configure形式设置权限。命令的configure形式通常是导致配置更改的形式，无论是未修改的命令（不带show或clear前缀）还是不修改形式。 要更改命令级别，请双击该命令或单击编辑。您可以设置介于0和15之间的级别。您只能配置main命令的权限级别。例如，您可以分别配置所有aaa命令的级别，但无法配置aaa authentication命令和aaa authorization命令的级别。 要更改显示的所有命令的级别，请单击Select All，然后单击Edit。 单击OK接受更改。
步骤 5	单击 Apply。 系统会分配授权设置，并将更改保存到运行配置中。

参考

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

问题4. ASDM多重身份验证(MFA)

故障排除 — 建议的步骤

在撰写本文时，ASDM不支持MFA（或2FA）。 此限制包括MFA和PingID等解决方案。

参考

Cisco Bug id CSCvs85995

增强版：使用双因素身份验证或MFA的ASDM访问

问题5. ASDM外部身份验证配置

故障排除 — 建议的步骤

您可以使用LDAP、RADIUS、RSA SecurID或TACACS+在ASDM上配置外部身份验证。

参考

- 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

问题6. ASDM本地身份验证失败

故障排除 — 建议的步骤

如果使用外部身份验证和LOCAL身份验证作为回退，则仅当外部服务器关闭或不运行时，本地身份验证才起作用。只有在这种情况下，LOCAL身份验证才会接管，并且您可以与LOCAL用户连接。

这是因为外部身份验证优先于本地身份验证。

示例：

<#root>

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

参考

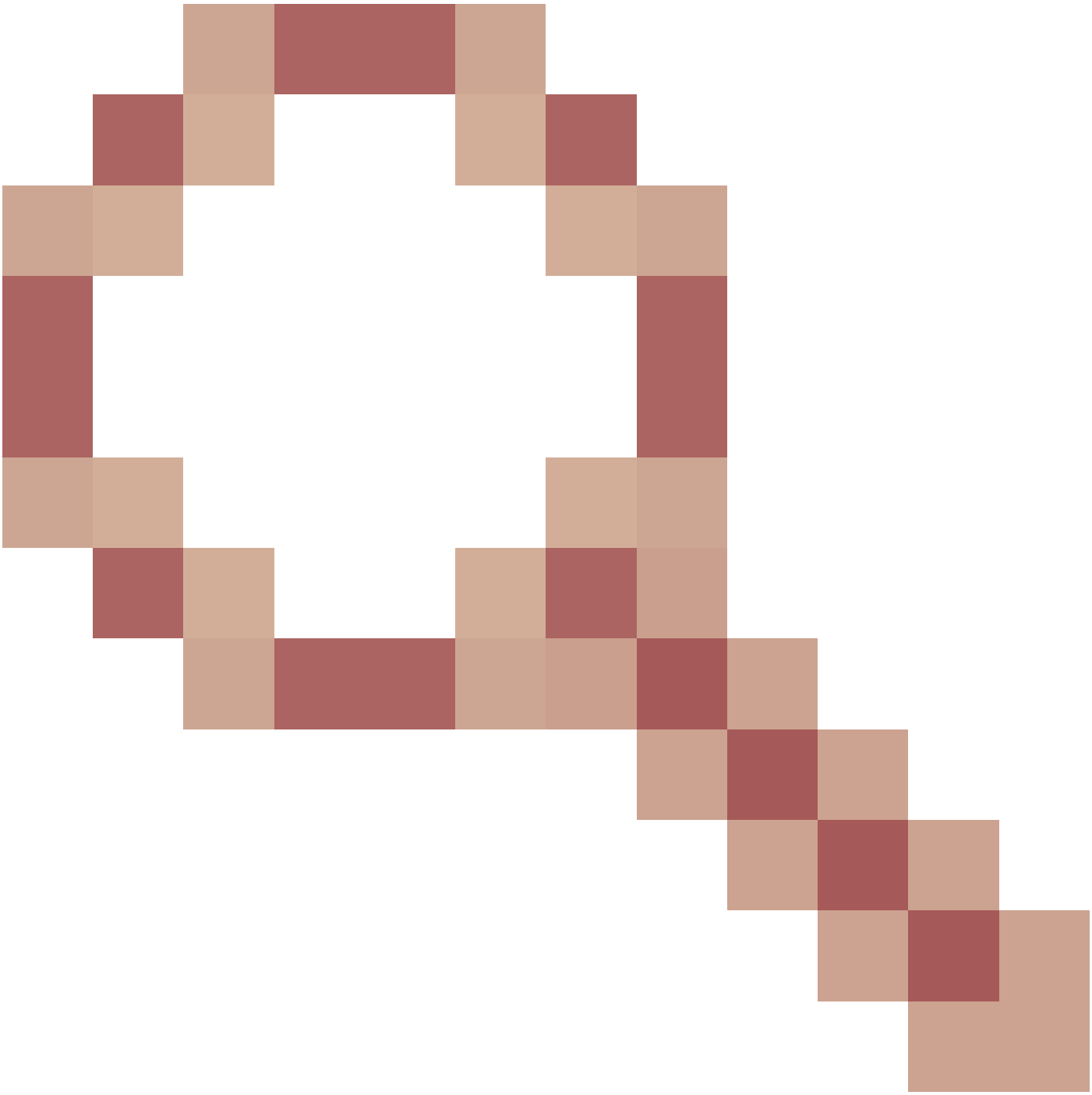
- https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/A-H/asa-command-ref-A-H/aa-ac-commands.html#wp6184732320

问题7. ASDM一次性密码

故障排除 — 建议的步骤

- ASDM OTP（一次性密码）身份验证支持在ASA版本8.x - 9.x和单路由模式下添加。
- 用于ASA防火墙透明模式和/或多情景模式的ASDM OTP身份验证不进入此类别。

请参阅Cisco Bug id CSCtf23419



增强版：多情景和透明模式中的ASDM OTP身份验证支持

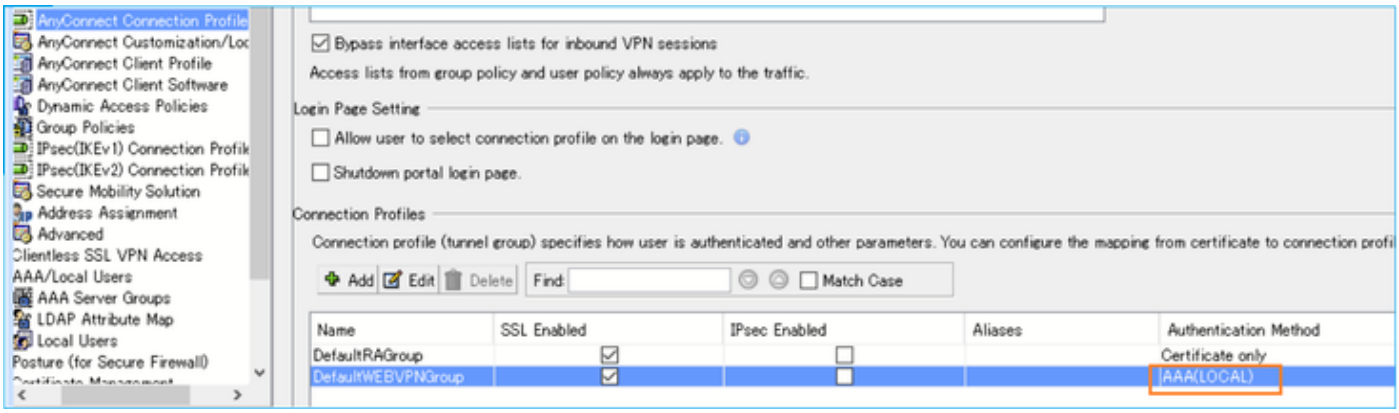
问题8.连接配置文件未显示所有方法

在这种情况下，问题在于ASA CLI配置与ASDM UI不匹配。

具体而言，CLI具有以下功能：

```
<#root>

tunnel-group DefaultWEBVPNGroup webvpn-attributes

 authentication aaa certificate
```

虽然ASDM UI未提及证书方法：



故障排除 — 建议的步骤

这是一个表面问题。ASDM中不显示方法，但使用证书身份验证。

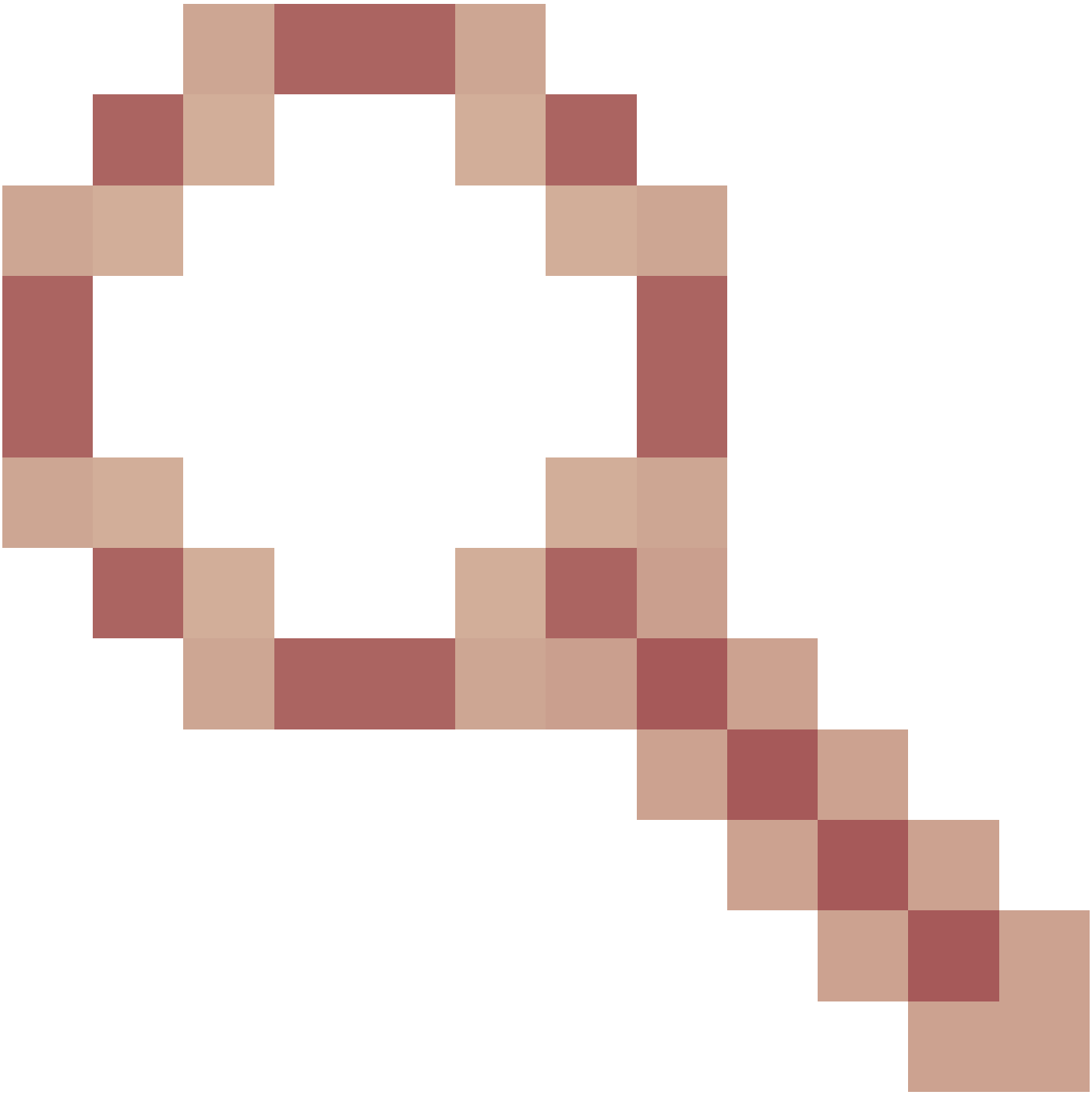
问题9. ASDM会话不超时

症状是不考虑ASDM GUI会话超时。

故障排除 — 建议的步骤

当托管ASA上未设置aaa authentication http console LOCAL命令时，会发生这种情况。

请参阅Cisco Bug id CSCwj70826



增强版：添加警告：设置会话超时，需要“aaa authentication http console LOCAL”

解决方法

在托管ASA上配置命令“aaa authentication http console LOCAL”。

问题10. ASDM LDAP身份验证失败

故障排除 — 建议的步骤

第 1 步

确保配置到位，例如：

<#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

第 2 步

检查LDAP服务器状态：

<#root>

asa#

show aaa-server

好的场景：

<#root>

Server status:

ACTIVE

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

坏情形：

<#root>

Server status:

FAILED

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

第 3 步

通过暂时禁用LDAP身份验证，检查LOCAL身份验证正常工作。

第 4 步

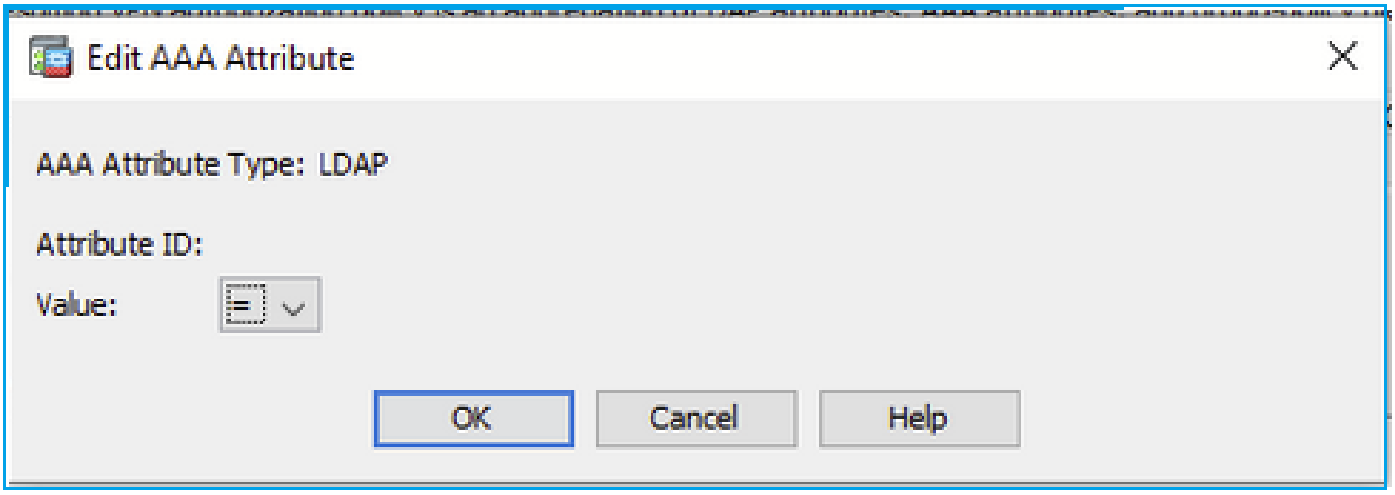
在ASA上运行LDAP调试并尝试验证用户：

```
<#root>

#

debug ldap 255
```

在调试中查找包含“失败”等提示的行。

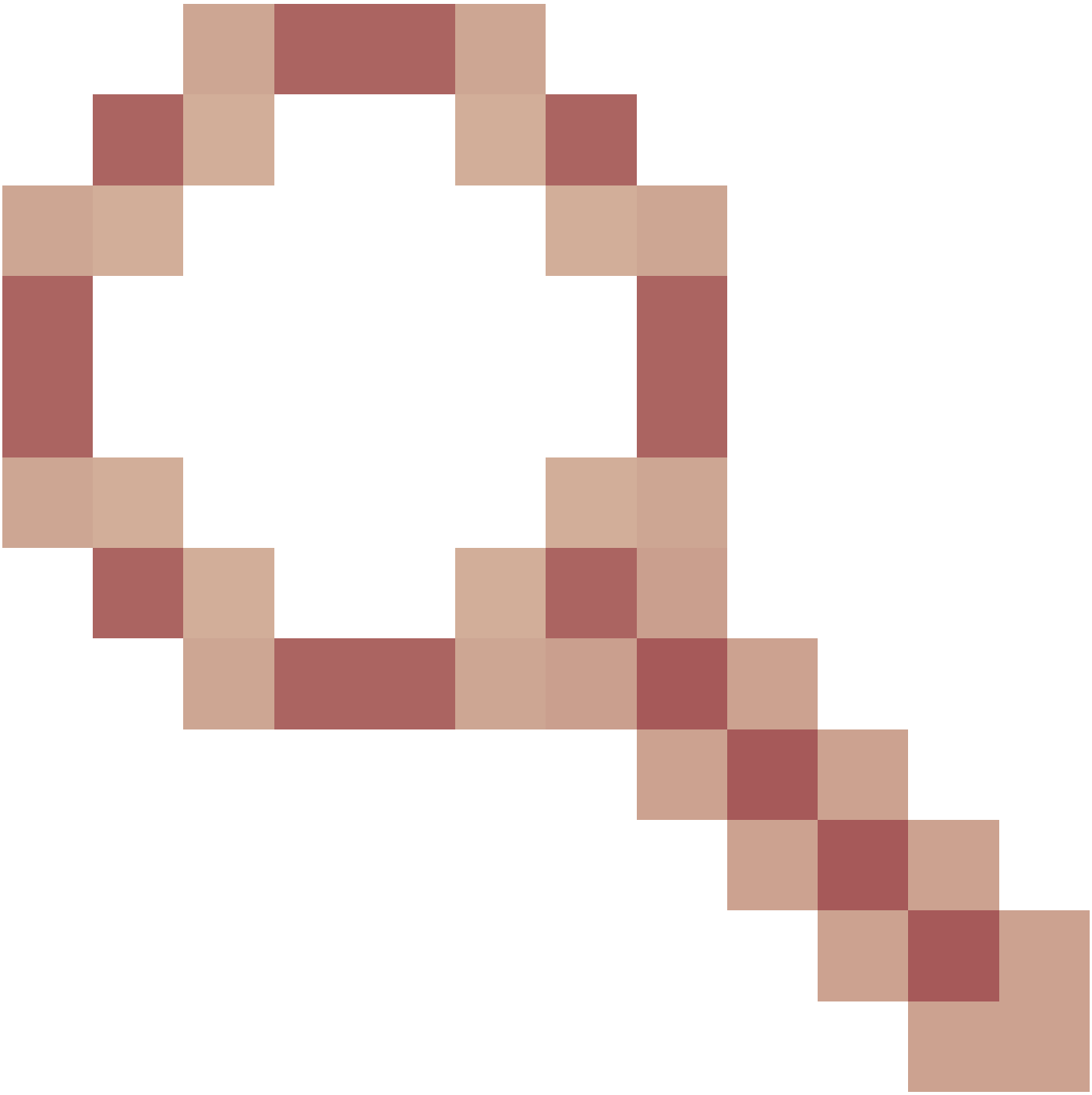
问题11.缺少ASDM Webvpn DAP配置

在ASDM AAA Attributes上的DAP配置下，类型(Radius/LDAP)不可见，仅查看=和!= on下拉列表：

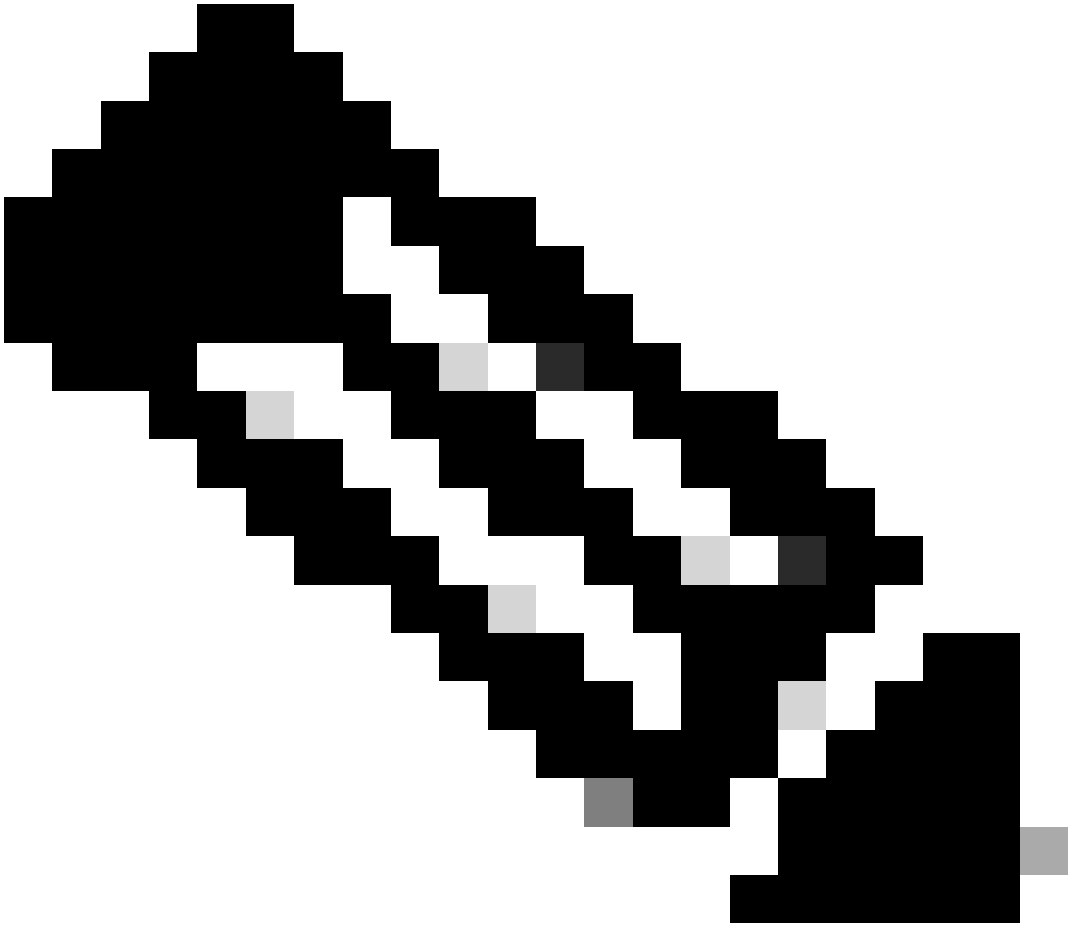


故障排除 — 建议的步骤

这是Cisco Bug id CSCwa跟踪的软件缺陷99370



ASDM:DAP配置缺少AAA属性类型(Radius/LDAP)

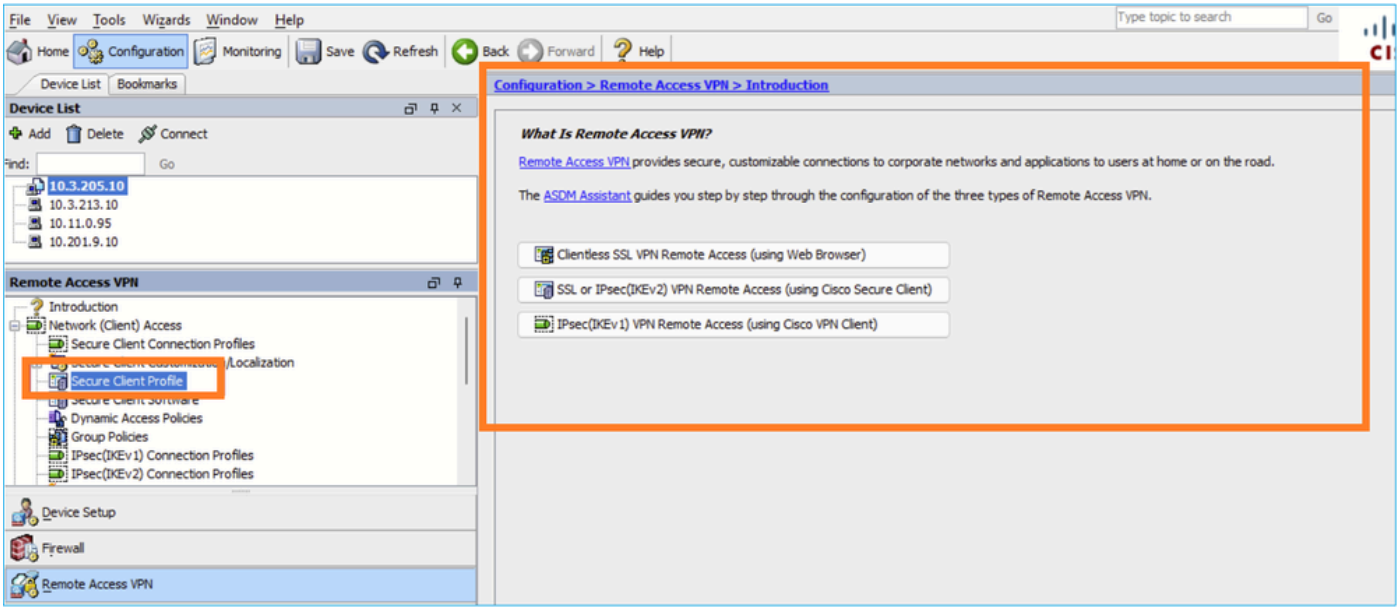


注意：此缺陷在最新的ASDM软件版本中已修复。有关详细信息，请查看缺陷详细信息。

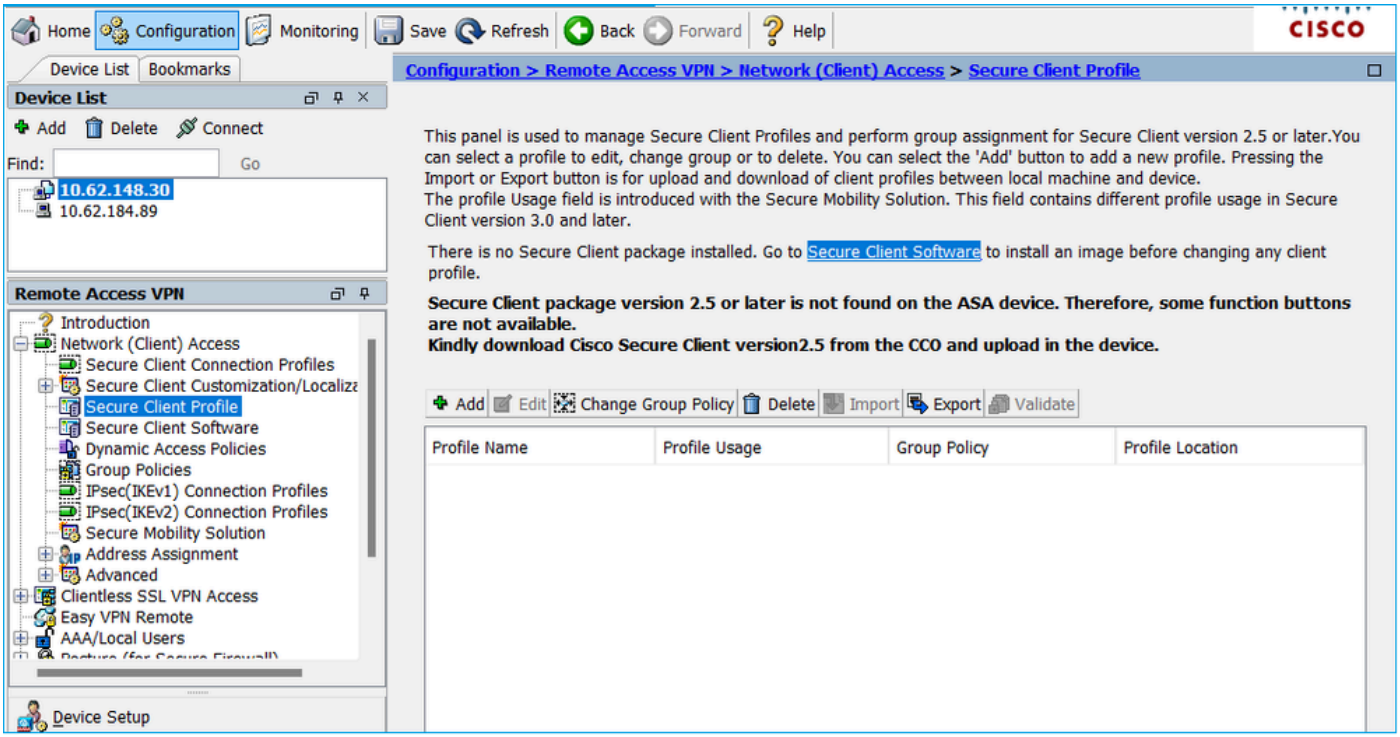
排除ASDM其他问题

问题1.无法访问ASDM上的安全客户端配置文件

ASDM UI显示以下内容：



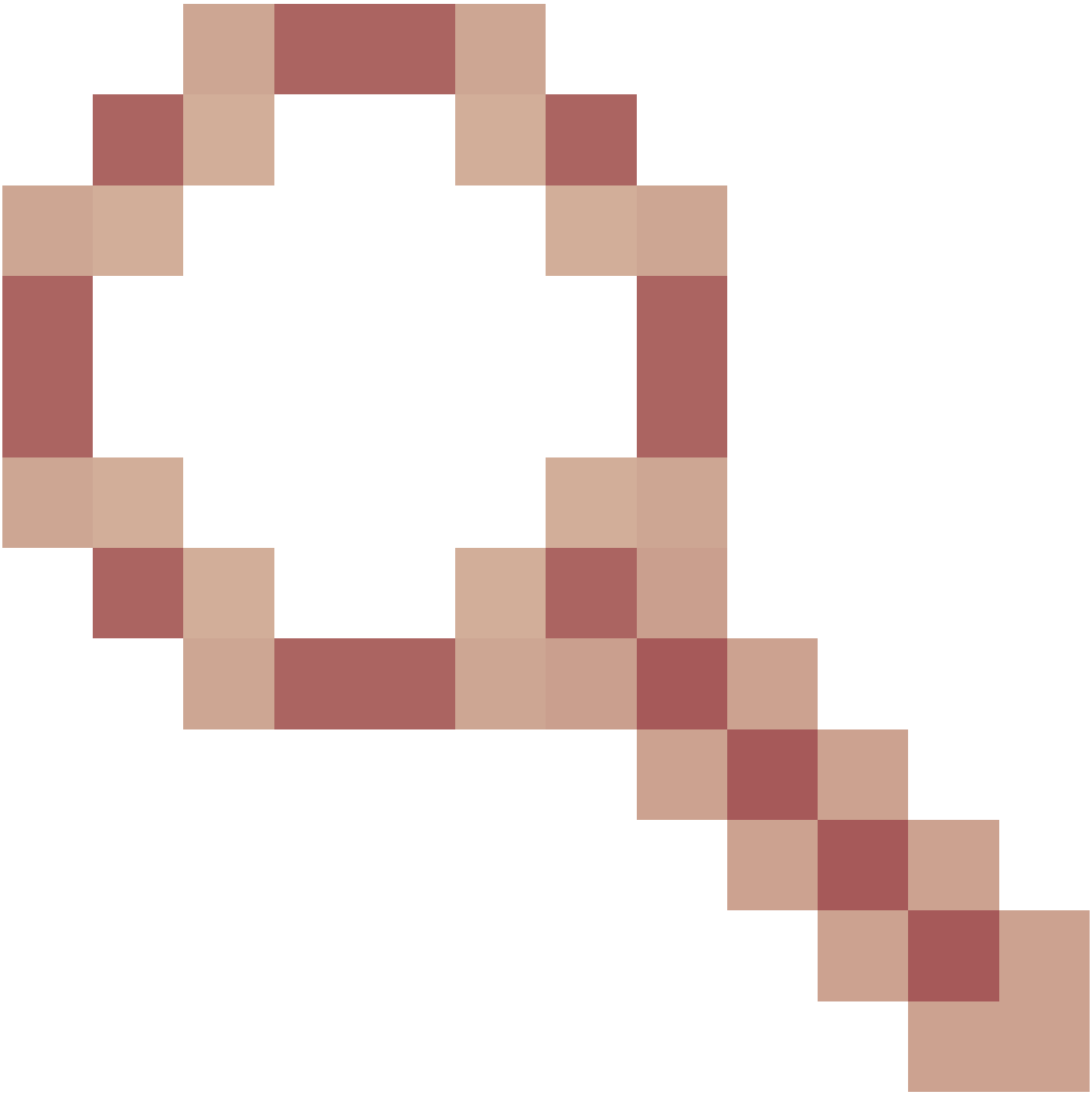
预期的UI输出为：



故障排除 — 建议的步骤

这是一个已知的缺陷：

Cisco Bug id CSCwi56155



无法访问ASDM上的安全客户端配置文件

解决方法:

降级AnyConnect

或

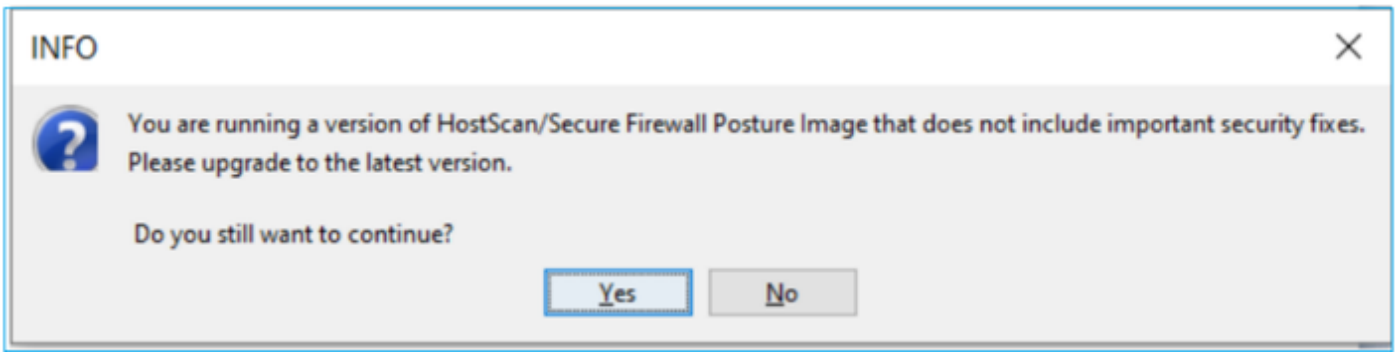
将ASDM升级到版本7.20.2

有关详细信息，请查看缺陷说明。此外，您可以订用缺陷，因此您将收到有关缺陷更新的通知。

问题2. ASDM显示hostscan的弹出窗口 — 映像不包括重要的安全修复

ASDM UI显示：

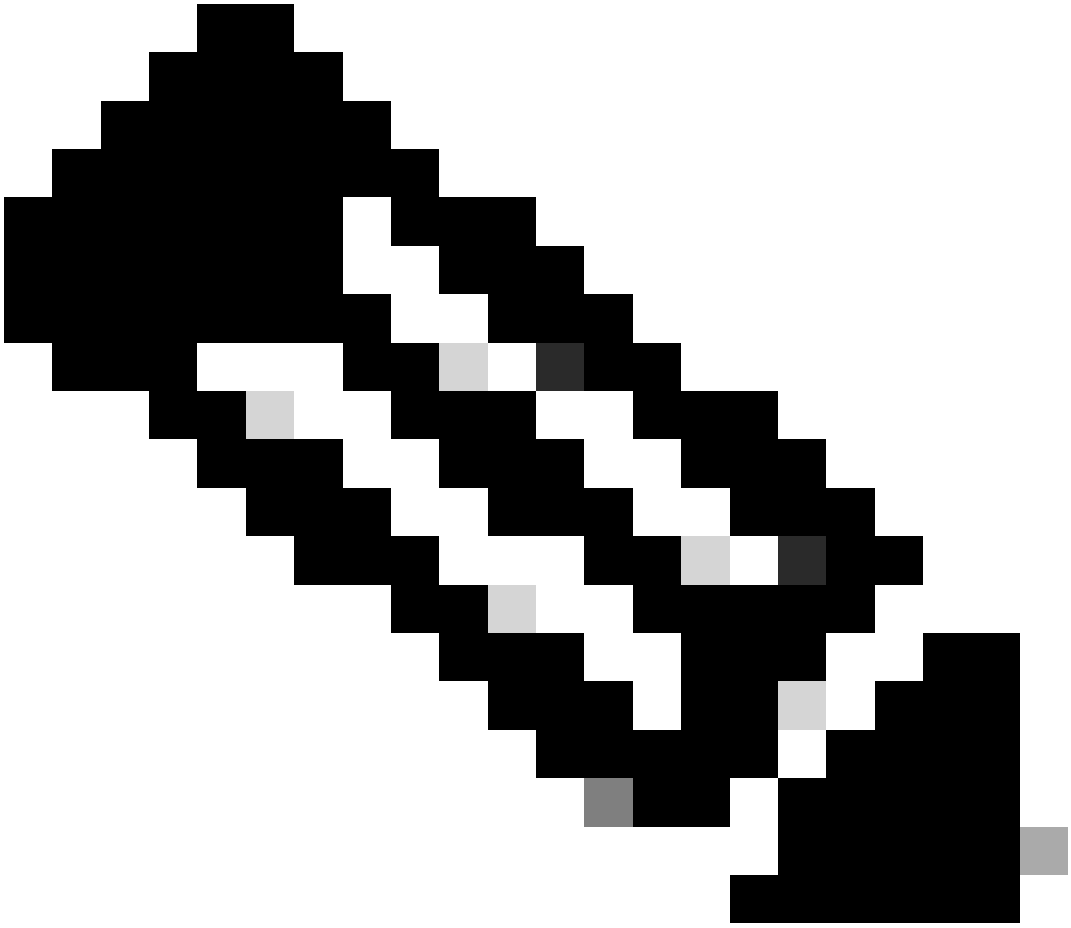
“您运行的HostScan/SecureFirewall安全状态映像版本不包含重要的安全修复程序。请升级到最新版本。是否仍要继续？”



故障排除 — 建议的步骤

这是一个已知的缺陷：

Cisco Bug id CSCwc62461
当登录ASDM弹出以进行hostscan时 — 映像不包含重要的安全修复



注意：此缺陷在最新的ASDM软件版本中已修复。有关详细信息，请查看缺陷详细信息。

解决方法：

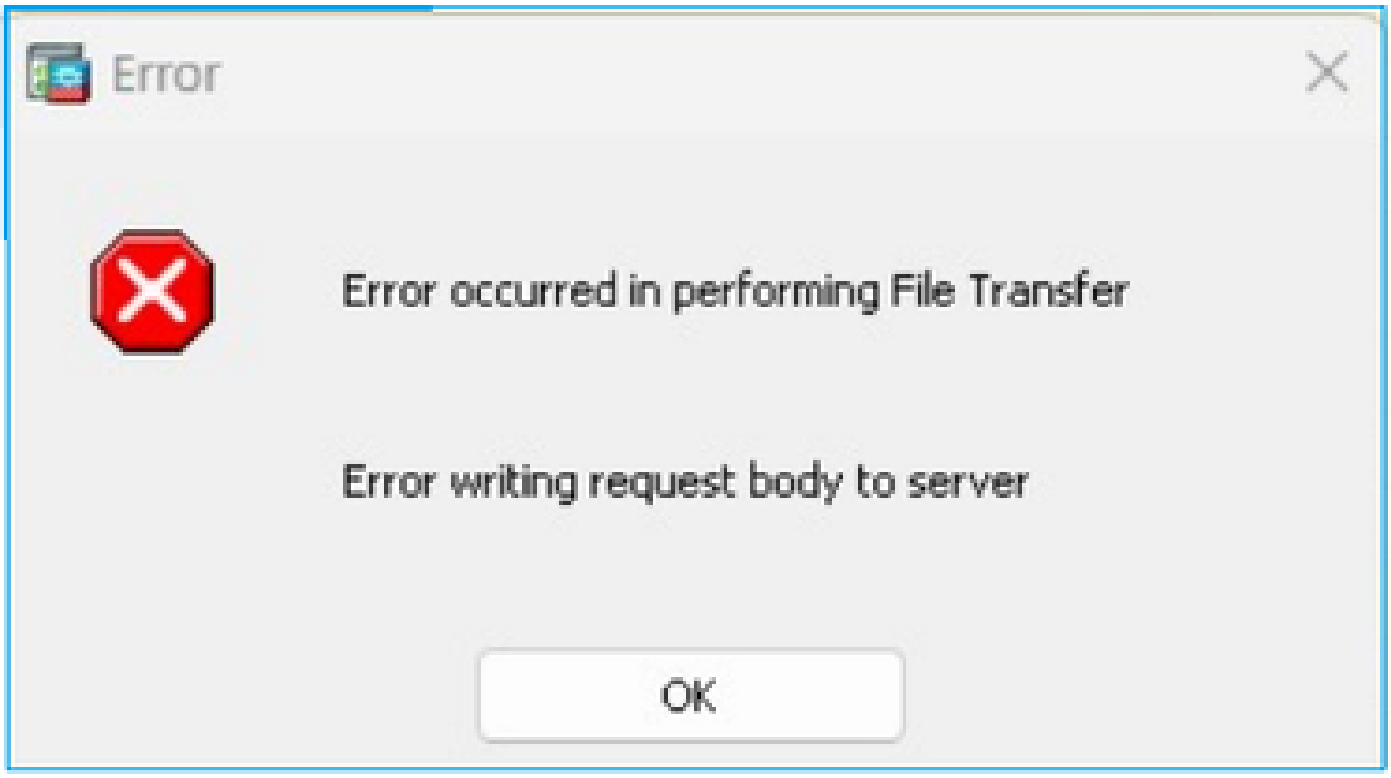
点击弹出消息框上的“是”继续。

问题3.通过ASDM复制映像时，ASDM“将请求正文写入服务器时出错”

ASDM UI显示：

执行文件传输时出错

将请求正文写入服务器时出错



故障排除 — 建议的操作

以下是跟踪的已知缺陷：

Cisco Bug id CSCtf74236

复制映像时ASDM“向服务器写入请求正文时出错”

解决方法

使用SCP/TFTP传输文件。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。