排除ASDM配置、身份驗證和其他問題

目錄

簡介

本文檔介紹自適應安全裝置裝置管理器(ASDM)配置、身份驗證和其他問題的故障排除過程。

背景

本檔案是ASDM疑難排解系列的一部分，並附隨以下檔案：

Link1<>

Link2<>

連結3<>

排除ASDM配置問題

問題1. ASDM不顯示應用於介面的任何訪問控制清單(ACL)

ASDM不顯示應用於介面的任何訪問控制清單(ACL)，即使有應用於相關介面的有效訪問組也是如此。消息改為顯示「0個傳入規則」。 觀察到在介面的訪問組配置中配置的L3和L2 ACL具有以下症狀：

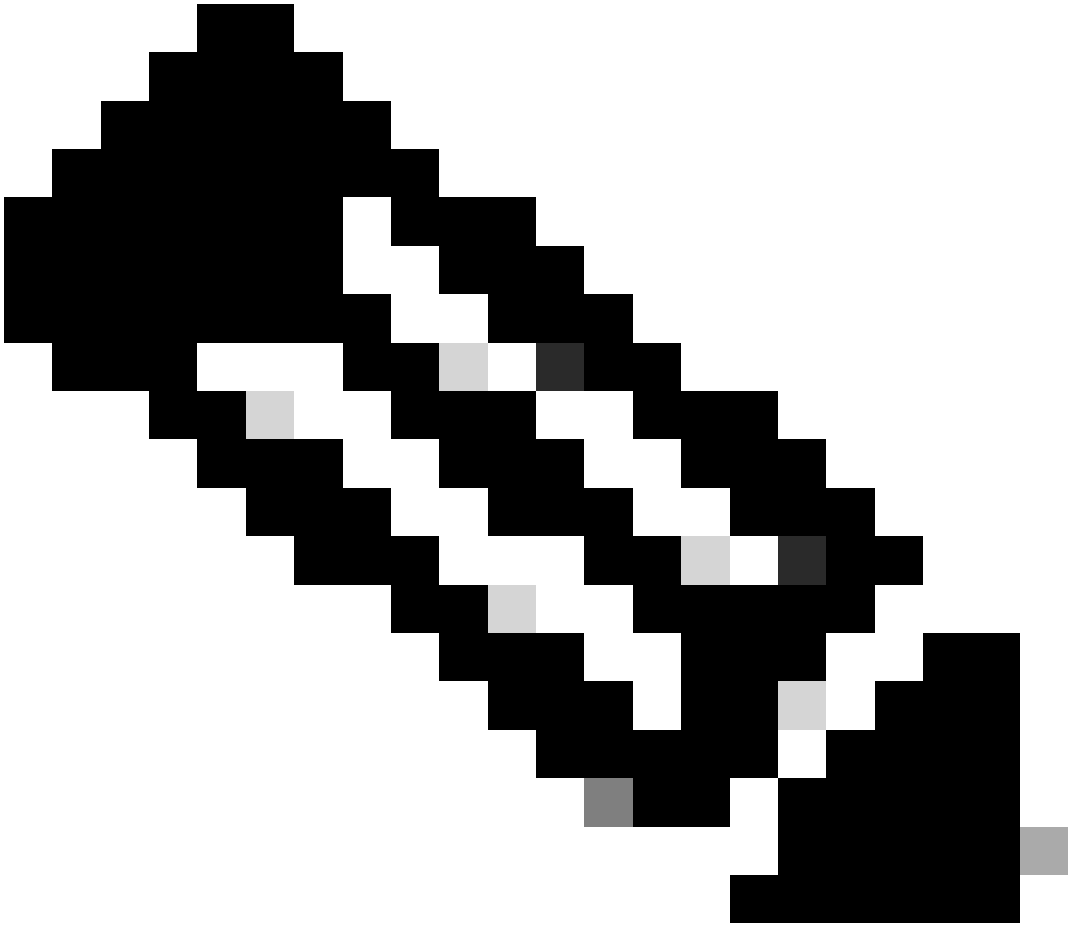
<#root>

```
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
```

疑難排解 — 建議動作

請參閱軟體思科錯誤ID CSCwj14147 「如果L2和L3 acl混合，ASDM無法載入存取群組組組組態。」



附註：此缺陷已在最近的ASDM軟體版本中修復。有關詳細資訊，請檢視缺陷詳細資訊。

問題2. ASA CLI和ASDM UI之間的命中計數不一致

ASDM中的命中計數項與防火牆輸出上的show access-list命令所報告的訪問清單命中計數不一致。

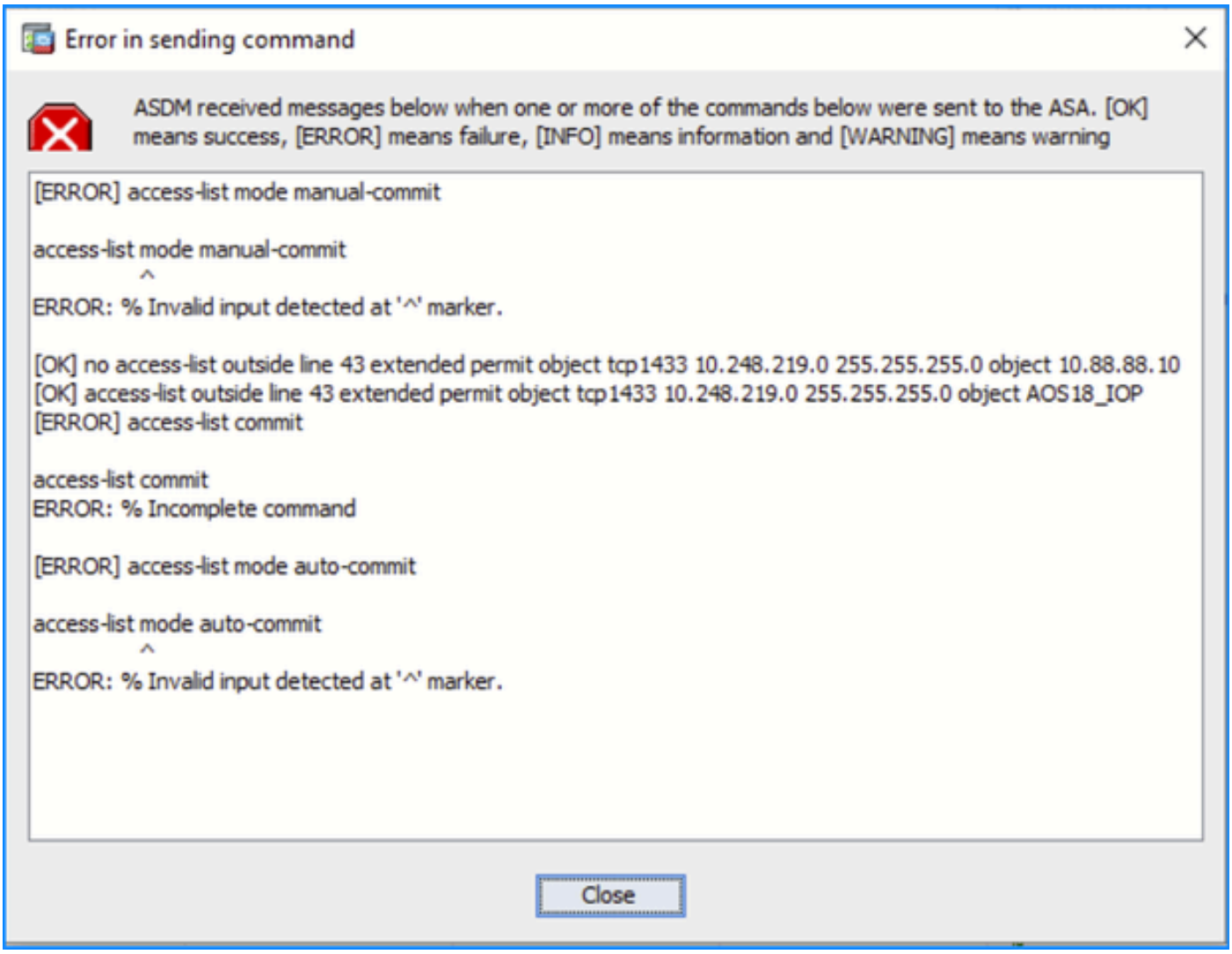
疑難排解 — 建議動作

請參閱軟體思科錯誤ID CSCtq38377「ENH:ASDM應在ASA上使用ACL雜湊計算，而不是本地計算」和思科錯誤ID CSCtq38405「ENH:ASA需要向ASD提供ACL雜湊資訊的機制」

問題3.「錯誤：%在「^」標籤處檢測到無效輸入。 在ASDM中編輯ACL時的錯誤消息

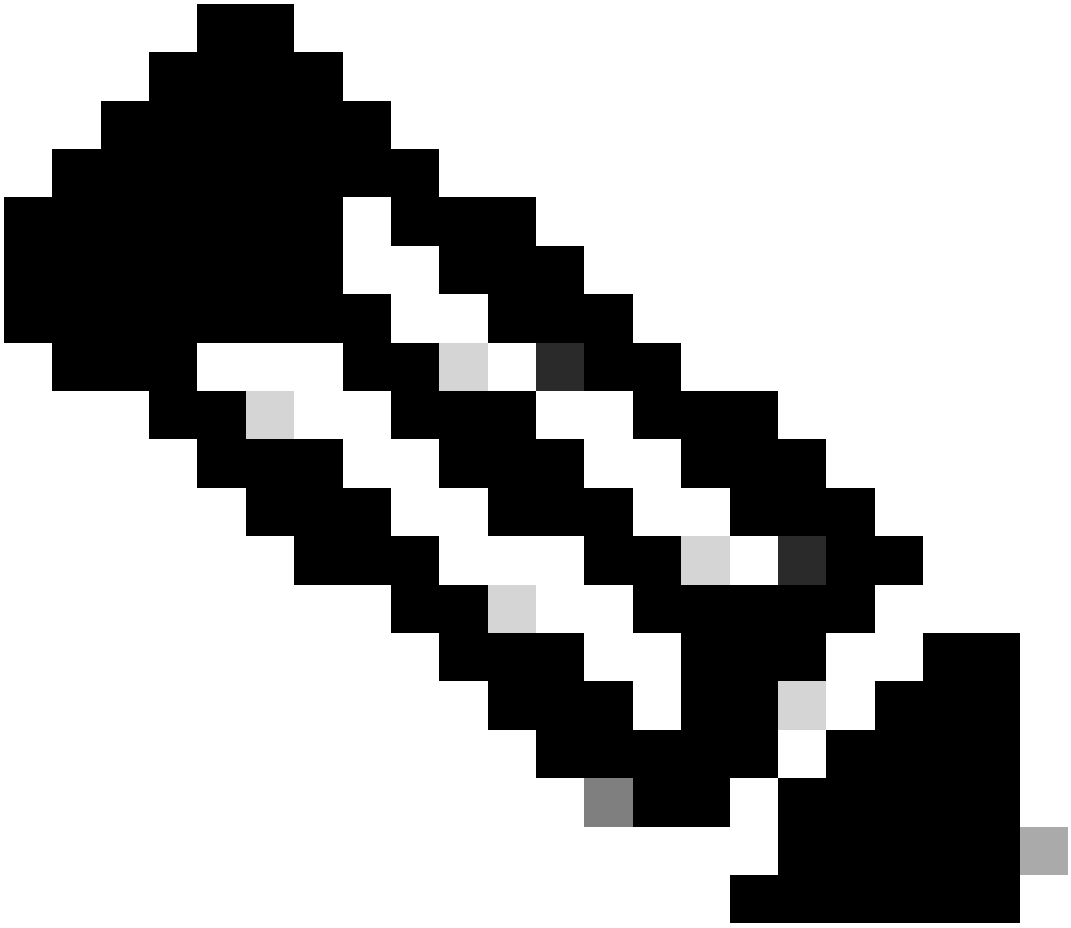
「錯誤：%在「^」標籤處檢測到無效輸入。 在ASDM中編輯ACL時會顯示錯誤消息：

```
[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.
```



疑難排解 — 建議動作

請參閱軟體思科錯誤ID CSCvq05064「Edit an entry(ACL)from ASDM gives an error(編輯來自ASDM的條目(ACL)出現錯誤)」。將ASDM與OpenJRE/Oracle - 7.12.2版和Cisco錯誤ID CSCvp88926 「Sending additional commands while deleting access-list」一起使用時。



附註：這些缺陷已在最近的ASDM軟體版本中得到修復。有關詳細資訊，請檢視缺陷詳細資訊。

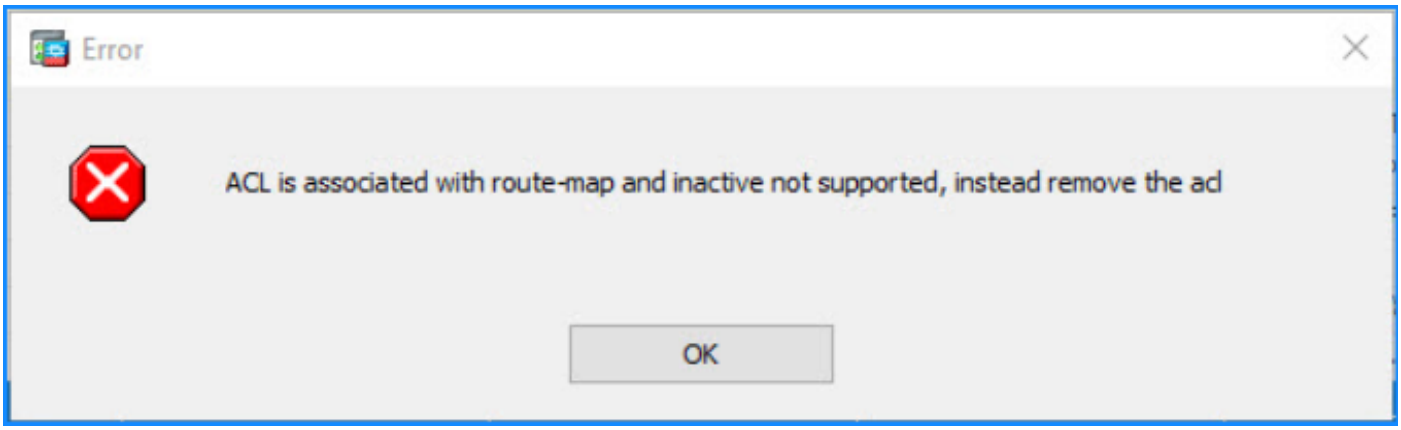
問題4. 「錯誤：ACL與路由對映和不支援的非活動狀態相關聯，在特定情況下應刪除acl錯誤消息

「錯誤：ACL與路由對映關聯，但不支援非活動，請改為移除acl在以下情況之一中顯示的錯誤消息：

1. 在基於策略的路由配置中使用的ASDM中編輯ACL:

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

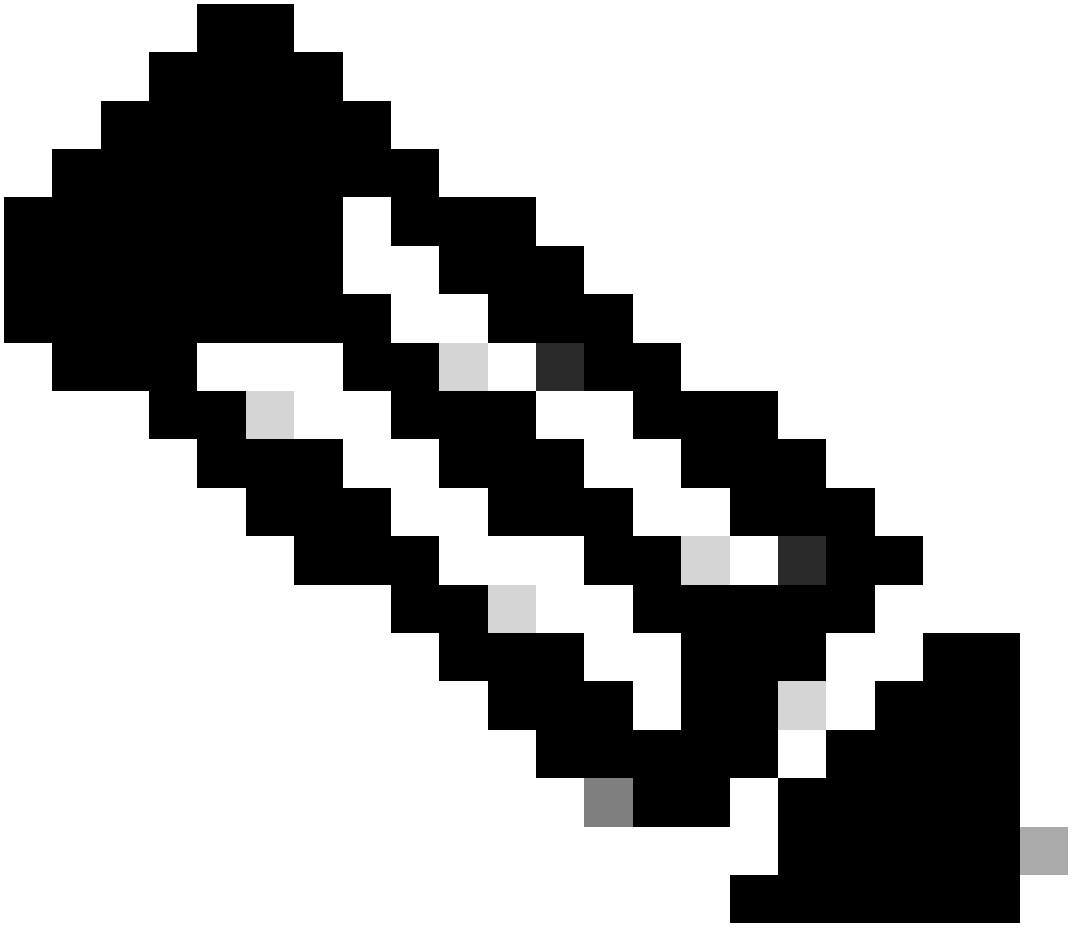
錯誤：ACL與路由對映關聯，但不支援非活動，請刪除acl



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

疑難排解 — 建議動作

1. 請參閱軟體思科錯誤ID CSCwb57615「Configuring pbr access-list with line number failed.」。 因應措施是從配置中排除「line」引數。
2. 請參閱軟體思科錯誤ID CSCwe3465「Unable to Edit the ACL objects if it is already in use，get the exception」。



附註：這些缺陷已在最近的ASA軟體版本中得到修復。有關詳細資訊，請檢視缺陷詳細資訊。

問題5. ASDM即時日誌檢視器中沒有隱式拒絕連線的日誌

ASDM Real-Time Log Viewer不顯示隱式拒絕連線的日誌。

疑難排解 — 建議動作

訪問清單末尾的隱式deny不會生成系統日誌。如果希望所有遭到拒絕的流量都生成系統日誌，請在ACL末尾新增帶有log關鍵字的規則。

問題6. ASDM在嘗試修改任何網路對象或對象組時凍結

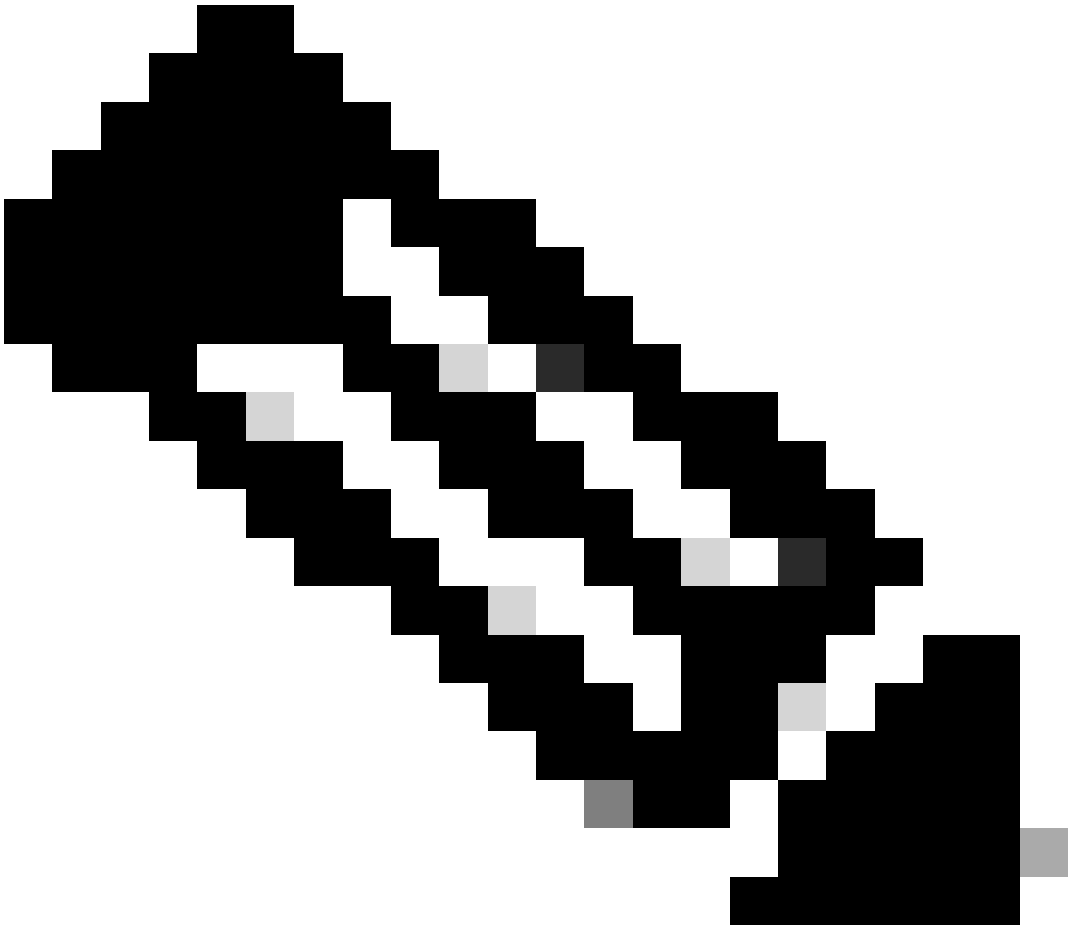
嘗試從Addresses頁籤下的Configuration > Firewall > Access Rules頁面修改任何網路對象或對象組時，ASDM將凍結。遇到此問題時，使用者無法編輯網路對象視窗中的任何引數。

疑難排解 — 建議動作

請參閱軟體思科錯誤ID CSCwj1250「ASDM在編輯網路物件或網路物件組時凍結」。 解決方法是禁用topN主機統計資訊收集：

<#root>

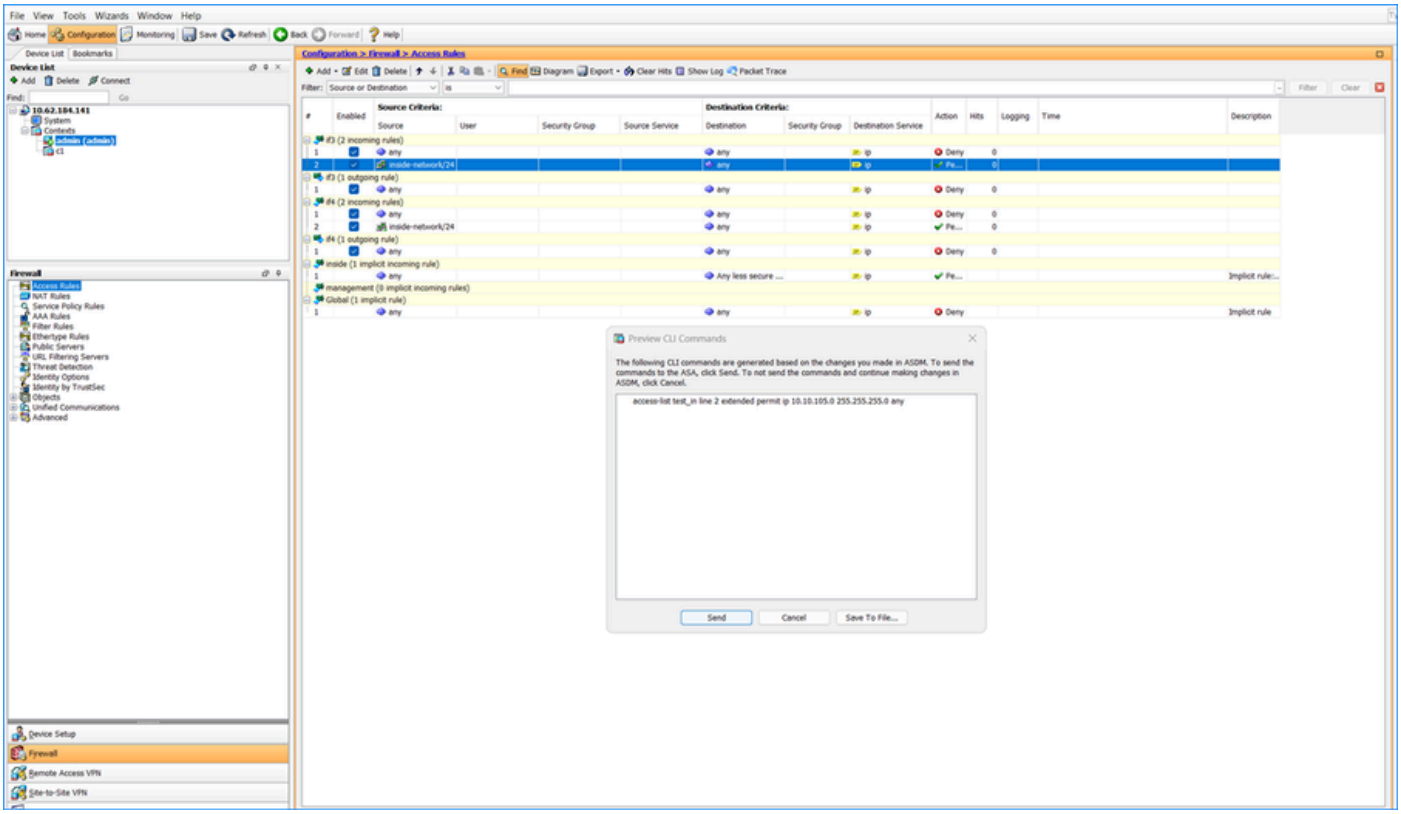
```
ASA(config)#
no hpm topN enable
```



附註：此缺陷已在最近的ASDM軟體版本中修復。有關詳細資訊，請檢視缺陷詳細資訊。

問題7. ASDM可以為不同的介面顯示額外的訪問控制清單規則

如果修改了介面級訪問控制清單，ASDM可以顯示不同介面的其他訪問控制清單規則。在本例中，傳入規則#2被新增到介面if3 ACL。ASDM還會顯#2介面if4的錯誤，但使用者未配置此規則。命令預覽正確顯示了一個掛起的更改。這是使用者介面顯示問題。



疑難排解 — 建議動作

請參閱軟體思科錯誤ID CSCwm71434 「ASDM可能顯示重複的介面存取清單專案」。

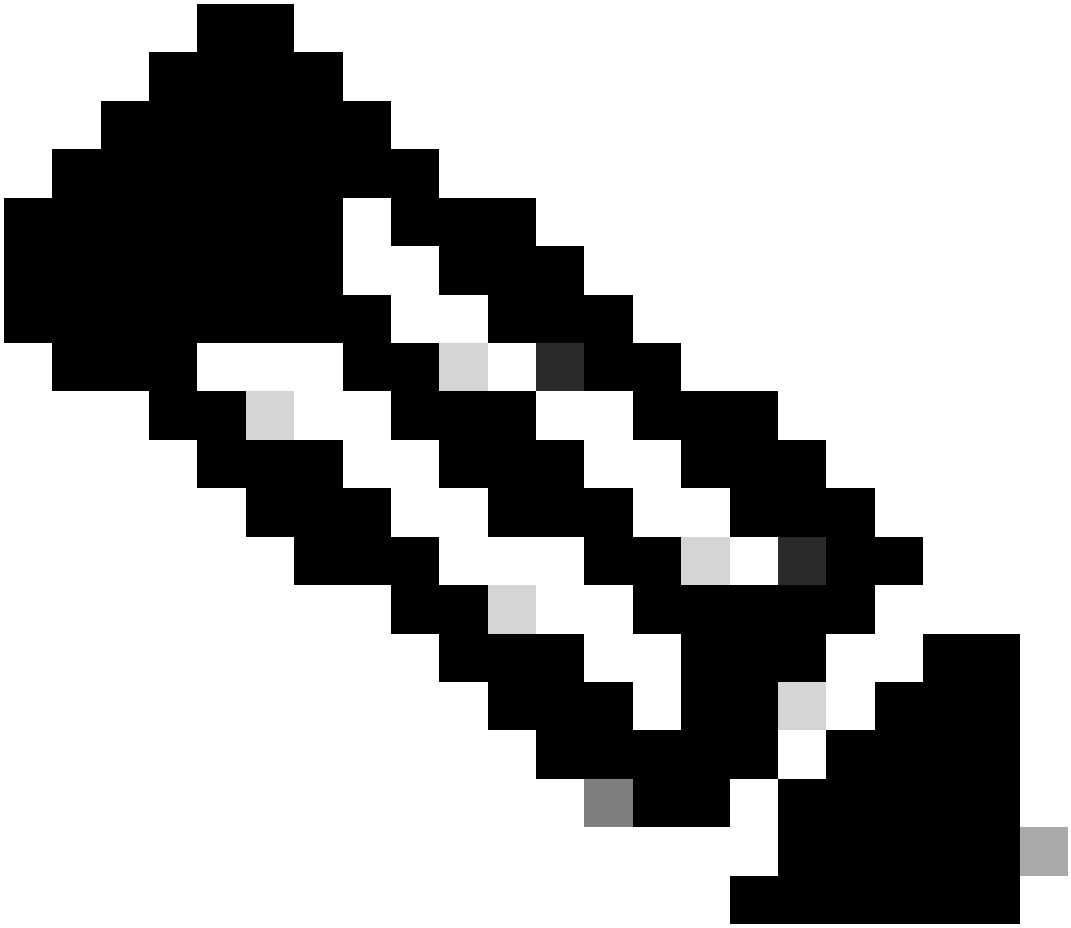
問題8.即時日誌檢視器中沒有即時日誌

即時日誌檢視器中未顯示任何日誌

疑難排解 — 建議動作

1. 確保日誌記錄已配置。請參閱ASDM手冊1:Cisco ASA系列常規操作ASDM配置指南，7.22，章節：記錄。

2. 請參閱軟體思科錯誤ID CSCvf82966 "ASDM — 記錄：無法檢視即時日誌」。

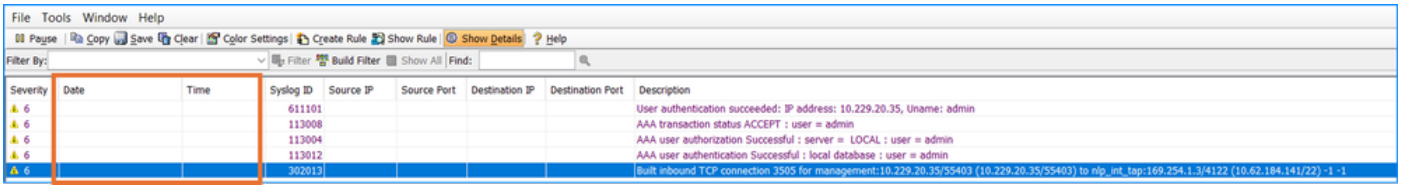


附註：此缺陷已在最近的ASDM軟體版本中修復。有關詳細資訊，請檢視缺陷詳細資訊。

參考資料

- ASDM第1冊：Cisco ASA系列常規操作ASDM配置指南，7.22，章節：記錄。

問題9.即時日誌檢視器中的「日期」和「時間」列為空



疑難排解 — 建議動作

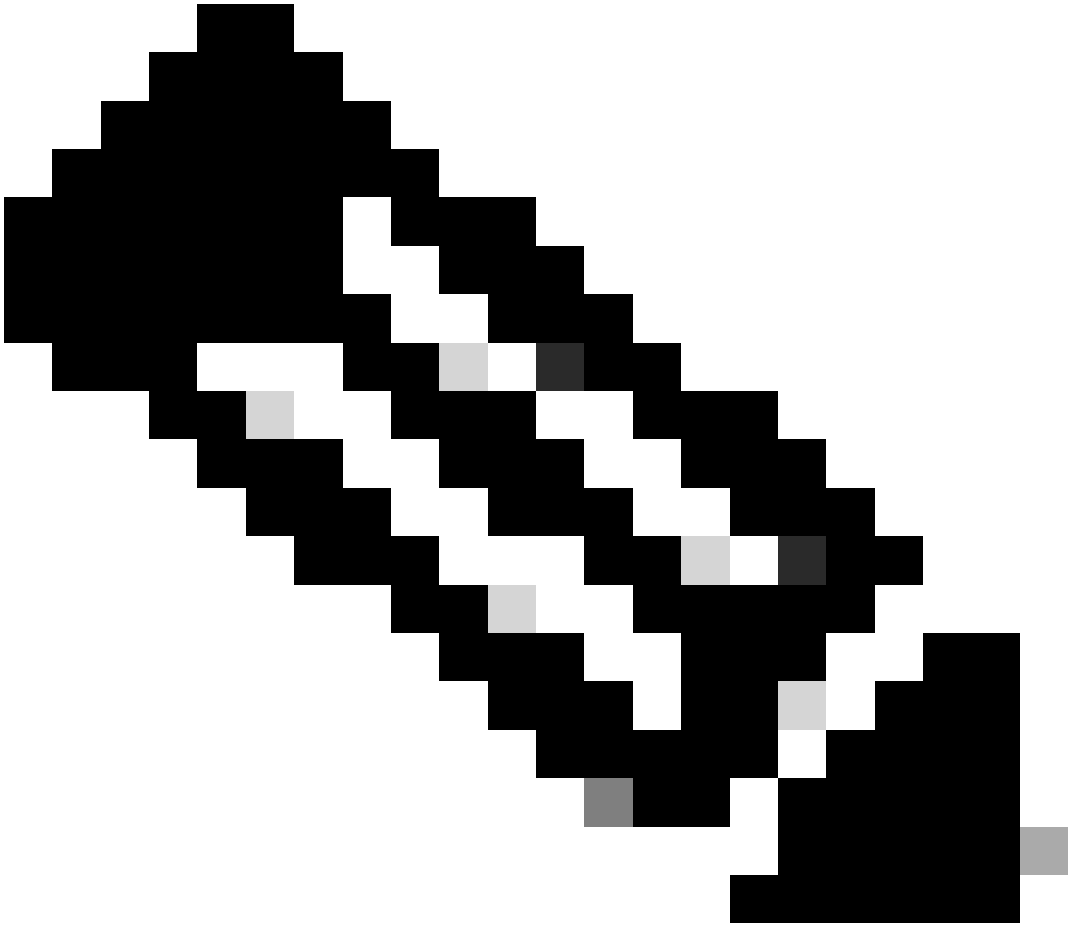
1. 檢查是否使用RFC5424日誌記錄時間戳格式：

```
<#root>

#

show run logging


logging enable

logging timestamp rfc5424
```

2. 如果使用RFC5424記錄時間戳格式，請參閱軟體思科錯誤ID CSCvs5212 "ASDM ENH:事件日誌檢視器能夠使用rfc5424時間戳格式顯示ASA系統日誌」。因應措施是避免使用RFC5424格式：

```
<#root>

firewall(config)#

no logging timestamp rfc5424


firewall(config)#

logging timestamp
```

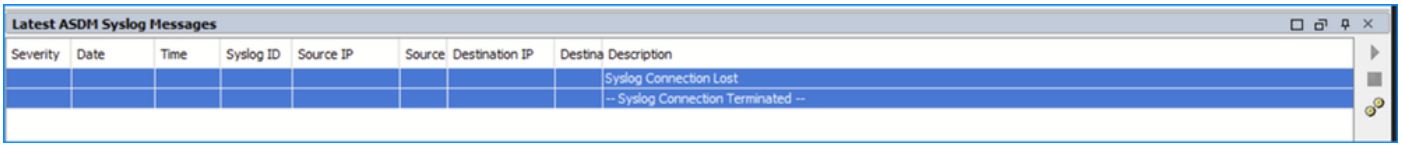
3. 此外，請參閱軟體缺陷Cisco錯誤ID CSCwh70323 「Timestamp entry missing for some syslog messages sent to syslog server」。



附註：此缺陷已在最近的ASDM軟體版本中修復。有關詳細資訊，請檢視缺陷詳細資訊。

問題十。 在多情景ASA中切換到其他情景後，登入到ASDM可能會失敗

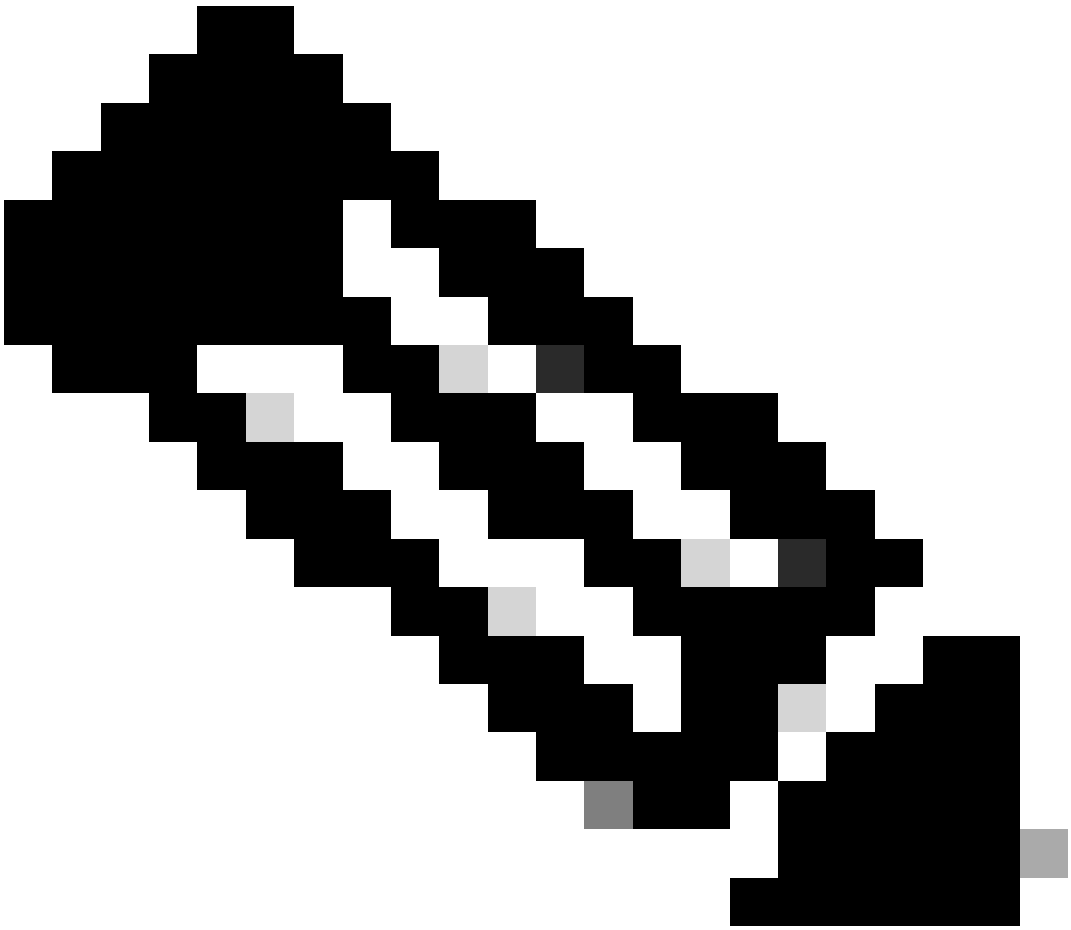
Home頁中的Latest ASDM Syslog Messages頁籤顯示「Syslog Connection Lost」和「Syslog Connection Terminated」消息：



疑難排解 — 建議動作

確保日誌記錄已配置。請參閱軟體思科錯誤ID CSCvz15404 "ASA:多情景模式：ASDM日誌記錄將

在切換到其他情景時停止。」



附註：此缺陷已在最近的ASDM軟體版本中修復。有關詳細資訊，請檢視缺陷詳細資訊。

問題十一 在不同情景之間切換時，ASDM會話突然終止

在不同情景之間切換時，ASDM會話突然終止，並出現錯誤消息「The maximum number of management sessions for protocol http or user exists exists（協定http或使用者的最大管理會話數已存在）」。請稍後再試」。這些日誌顯示在系統日誌消息中：

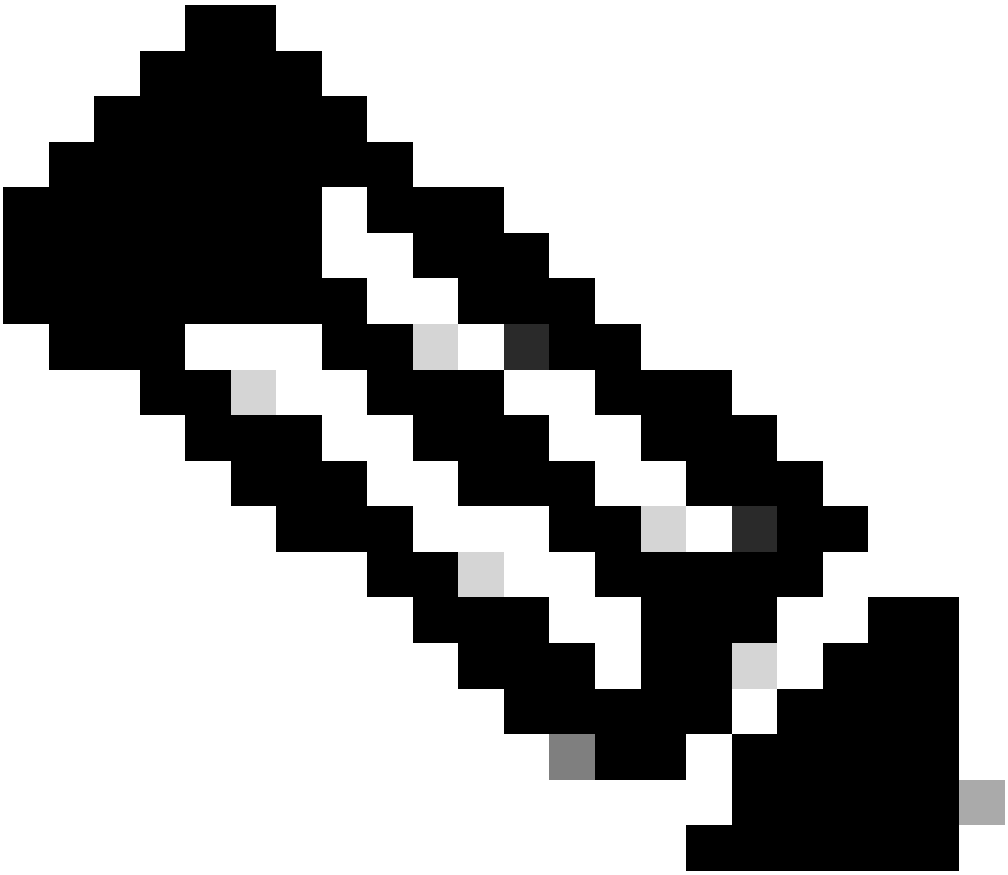
```
%ASA-3-768004: QUOTA: management session quota exceeded for http protocol: current 5, protocol limit 5

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

疑難排解 — 建議動作

1. 檢查當前ASDM資源使用率是否已達到Limit。在這種情況下，Denied計數器增加：

```
<#root>

firewall #

show resource usage resource ASDM


Resource                Current         Peak       Limit        Denied Context
ASDM

5

            5

5



10

 admin
```

2. 請參閱軟體思科錯誤ID CSCvs72378 「ASDM作業階段在不同環境之間交換時突然終止」。



附註：此缺陷已在最近的ASA軟體版本中得到修復。有關詳細資訊，請檢視缺陷詳細資訊。

3. 如果軟體版本具有思科錯誤ID CSCvs72378的修正程式，且目前的資源達到上限，請斷開部分現有ASDM作業階段。您可以關閉ASDM，或者清除運行ASDM的主機IP地址的HTTPS連線。在本示例中，假設ASDM上的HTTP伺服器在預設HTTPS埠443上運行：

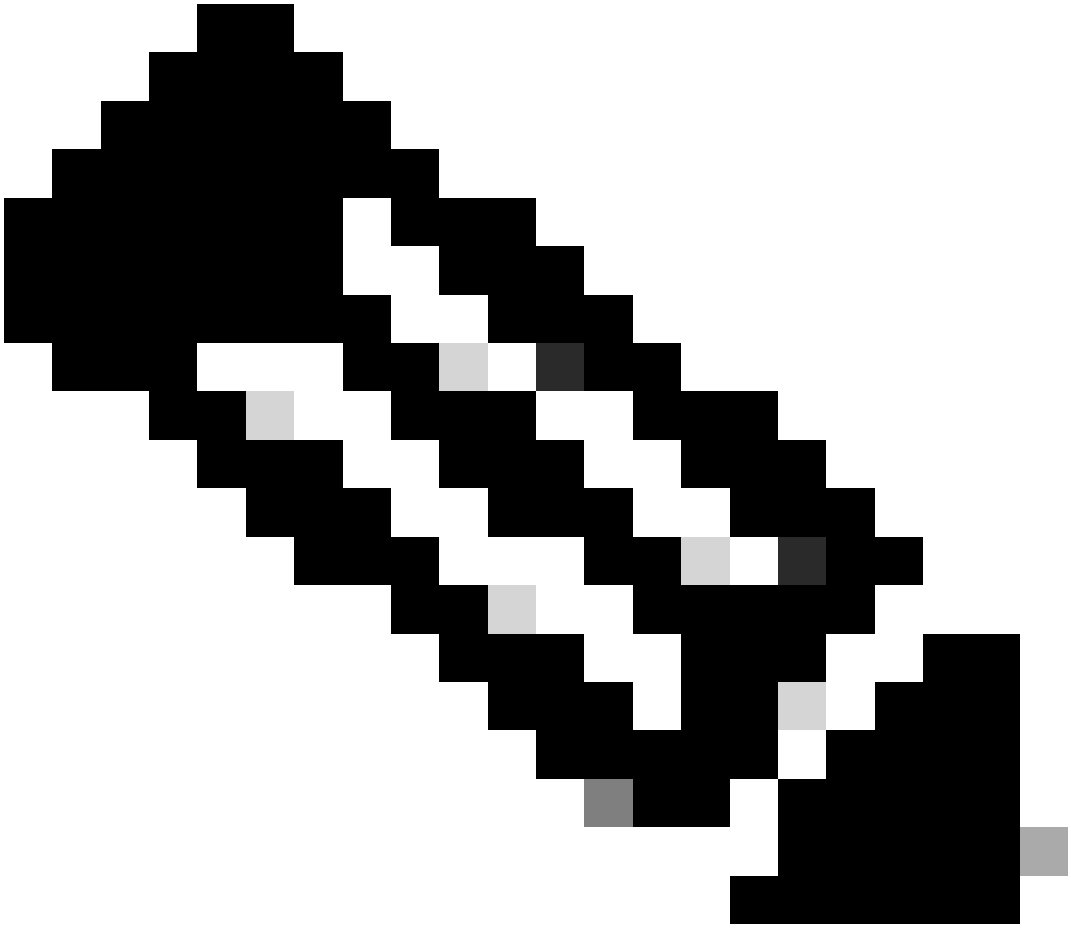
```
<#root>

#

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
```

問題12. ASDM隨機退出/終止，並顯示消息「ASDM從ASA裝置收到要斷開的消息。ASDM現在將退出。」

在多情景ASA上，ASDM隨機退出/終止，並顯示消息「ASDM從ASA裝置收到要斷開的消息」。ASDM現在將退出。」

疑難排解 — 建議動作

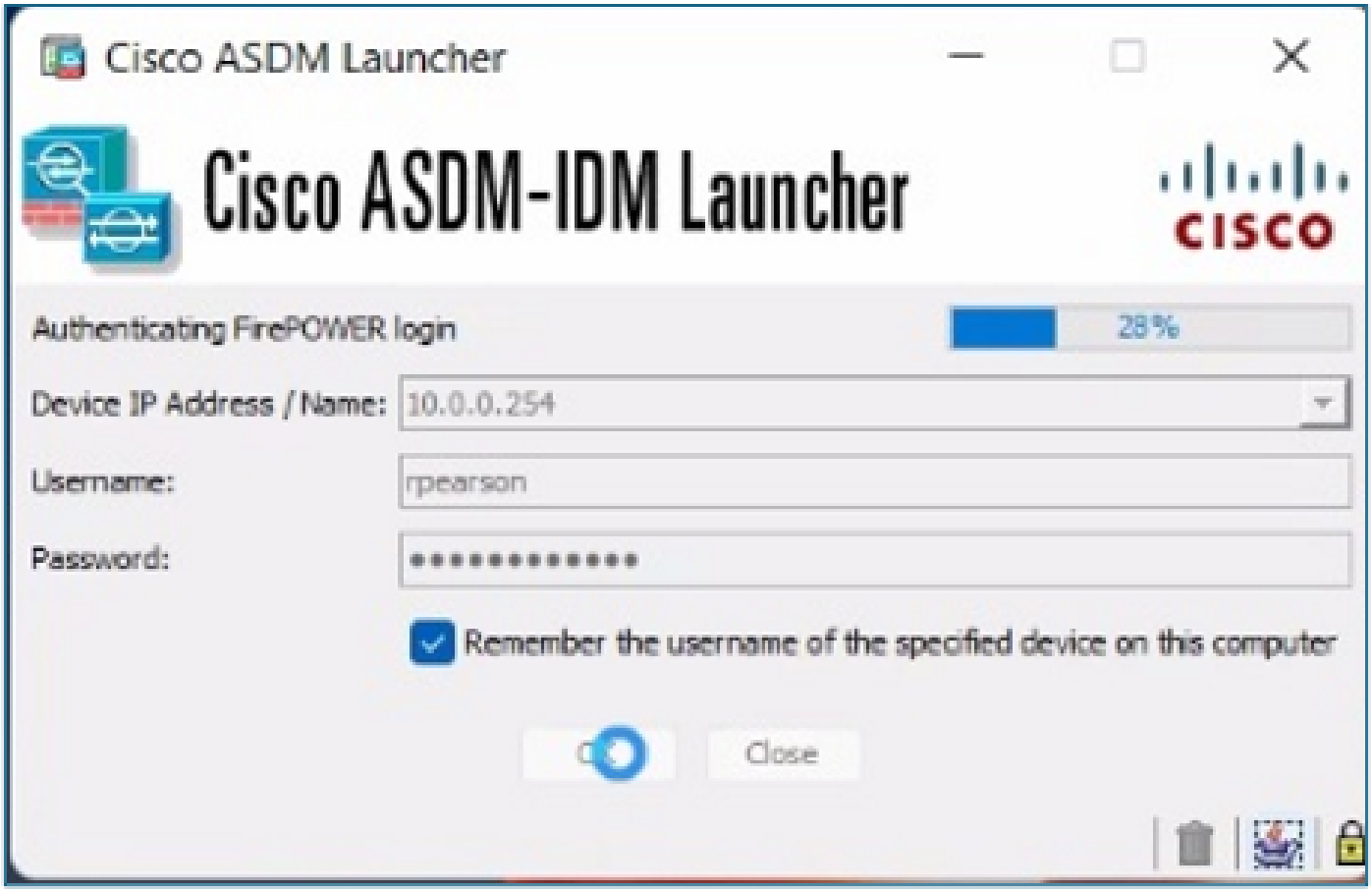
請參閱軟體缺陷Cisco錯誤ID CSCwh04395 「ASDM應用程式隨機退出/終止，並顯示多內容設定上的警示訊息」。



附註：此缺陷已在最近的ASA軟體版本中得到修復。有關詳細資訊，請檢視缺陷詳細資訊。

問題13. ASDM負載掛起，並顯示消息「Authentication FirePOWER login」

ASDM負載掛起，並顯示消息「Authentication FirePOWER login」：

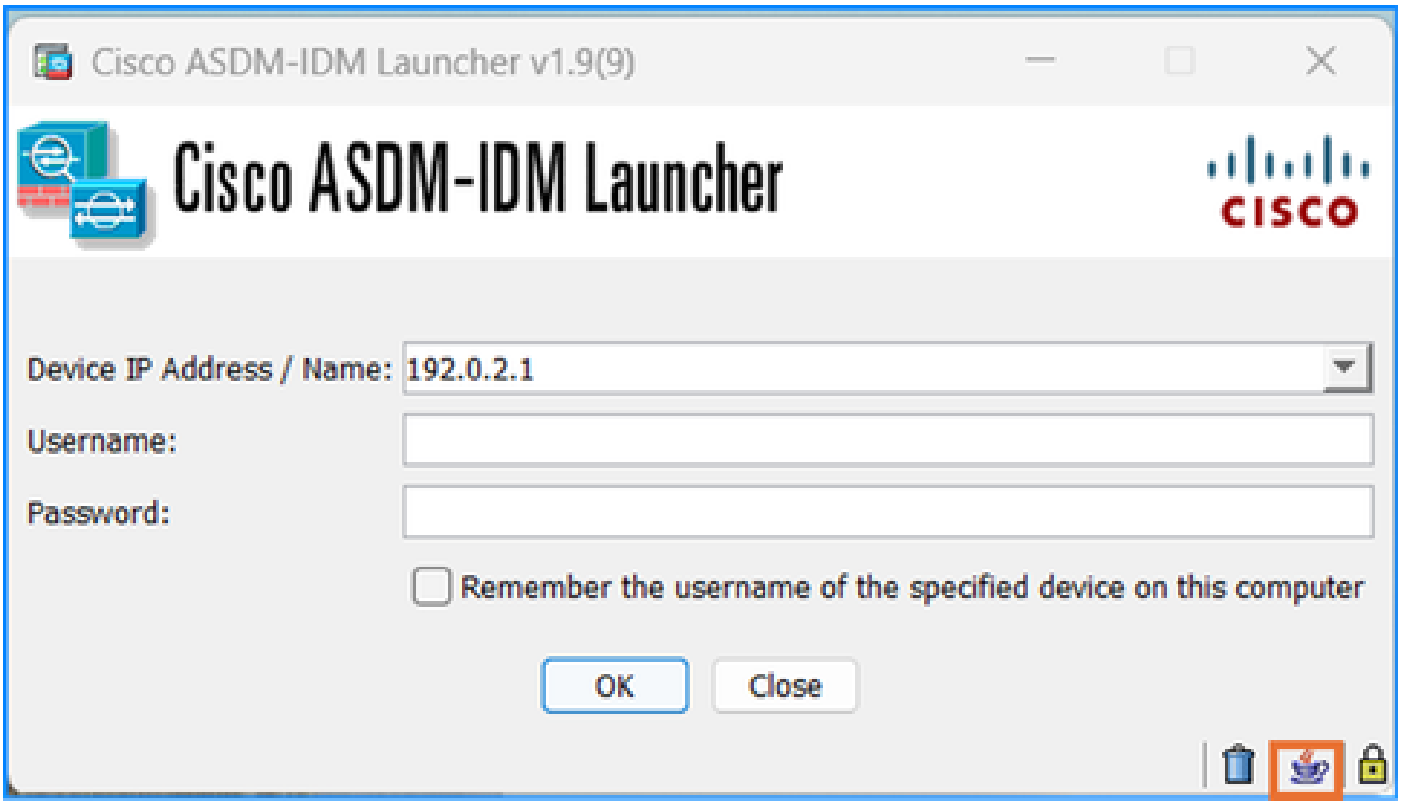


Java控制檯日誌顯示「Failed to connect to FirePower， continuing without it」（無法連線到FirePower，繼續而不連線）消息：

<#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)
```

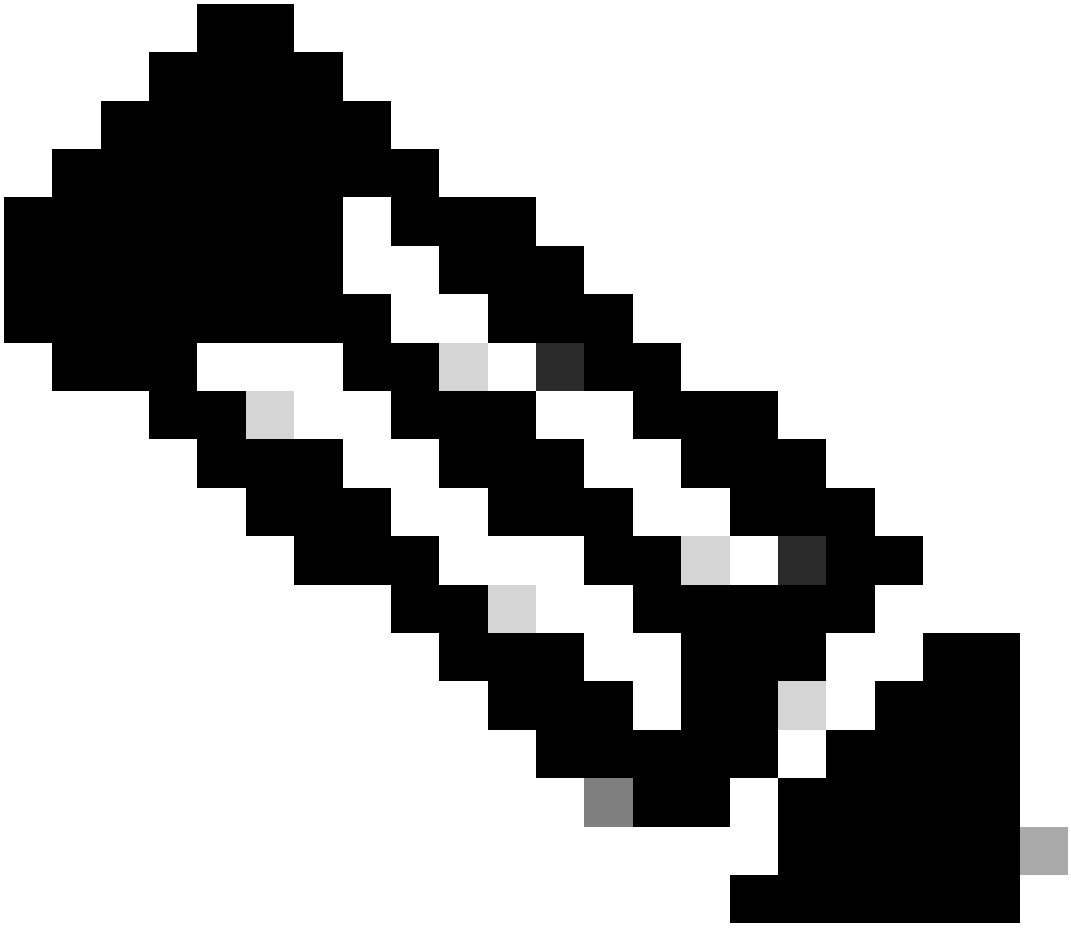
要驗證此症狀，請啟用Java控制檯日誌：



疑難排解 — 建議動作

請參閱軟體思科錯誤ID CSCwe15164 "ASA:ASDM無法顯示SFR頁籤，直到通過CLI「喚醒」。因應措施：

1. 關閉ASDM管理器。
2. 獲取對SFR的SSH訪問，並將使用者切換到root(sudo su)。
3. 執行完上述步驟後，再次重新啟動ASDM，它能夠載入Firepower(SFR)頁籤。



附註：此缺陷已在最近的Firepower軟體版本中得到修復。有關詳細資訊，請檢視缺陷詳細資訊。

問題14:ASDM不顯示Firepower模組管理/配置

Firepower模組配置在ASDM上不可用。

疑難排解 — 建議動作

1. 確保ASA、ASDM、Firepower模組和作業系統版本相容。 請參閱思科安全防火牆ASA版本說明、思科安全防火牆ASDM版本說明、思科安全防火牆ASA相容性:

- ASA 9.14/ASDM 7.14/Firepower 6.6是ASA 5525-X、5545-X和5555-X上ASA FirePOWER模組的最終版本。
- ASA 9.12/ASDM 7.12/Firepower 6.4.0是ASA 5515-X和5585-X上ASA FirePOWER模組的最

終版本。

- ASA 9.9/ASDM 7.9(2)/Firepower 6.2.3是ASA 5506-X系列和5512-X上ASA FirePOWER模組的最終版本。
- 除非另有說明，否則ASDM版本與所有以前的ASA版本向後相容。例如，ASDM 7.13(1)可以管理ASA 9.10(1)上的ASA 5516-X。
- ASA 9.8(4.45)+、9.12(4.50)+、9.14(4.14)+和9.16(3.19)+不支援ASDM進行FirePOWER模組管理；您必須使用FMC來管理這些版本的模組。這些ASA版本需要ASDM 7.18(1.152)或更高版本，但對ASA FirePOWER模組的ASDM支援在7.16後終止。
- ASDM 7.13(1)和ASDM 7.14(1)不支援ASA 5512-X、5515-X、5585-X和ASASM;必須升級到ASDM 7.13(1.101)或7.14(1.48)才能恢復ASDM支援。

2. 如果版本相容，請檢查模組是否已啟動並正在運行：

<#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
```

如果模組關閉，可以使用sw-module module reset命令重置模組，然後重新載入模組軟體。

參考資料

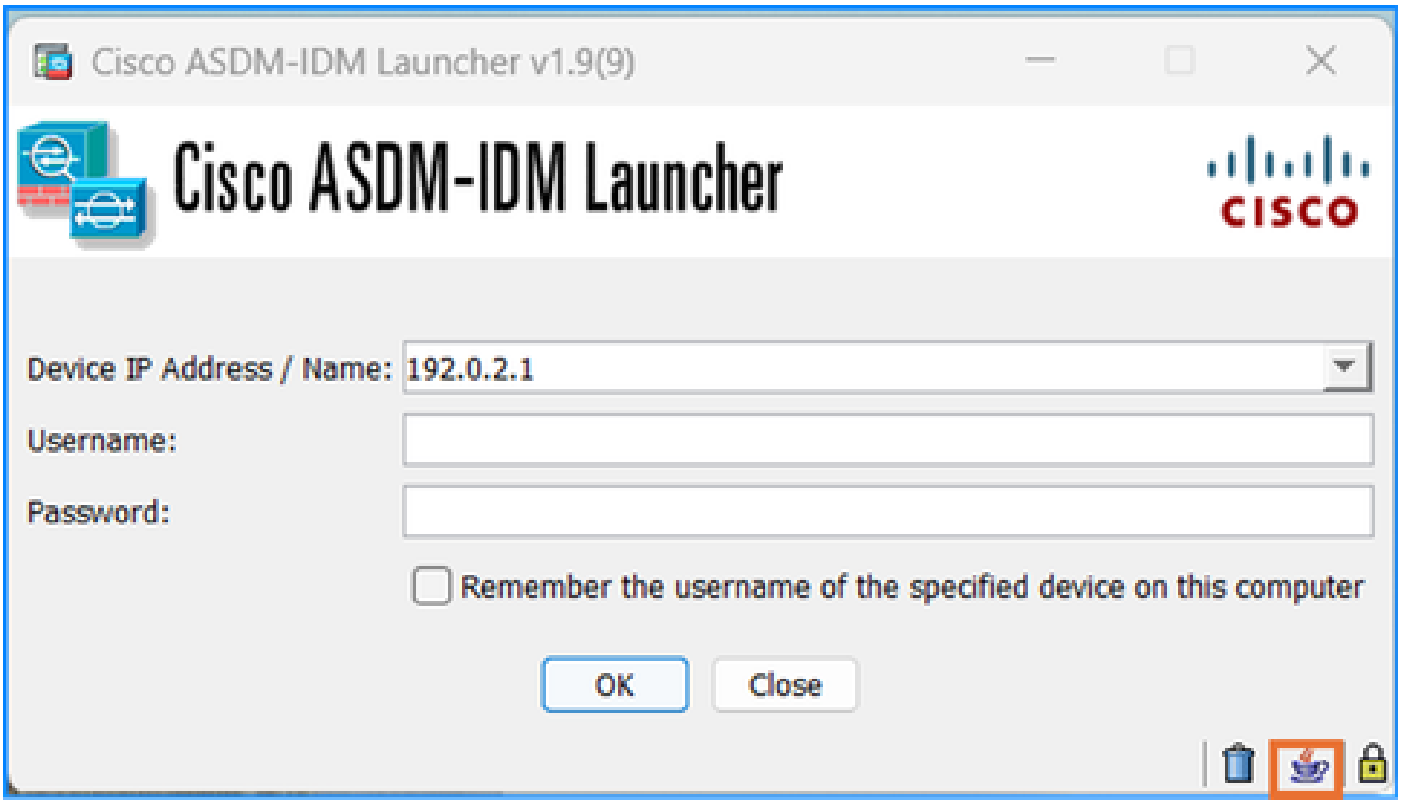
- 《 Cisco Secure Firewall ASA發佈說明》
- Cisco Secure Firewall ASDM發行說明
- Cisco安全防火牆ASA相容性

問題15.在ASDM上無法訪問安全客戶端配置檔案

Java控制檯日誌顯示"java.lang.ArrayIndexOutOfBoundsException:3」錯誤消息：

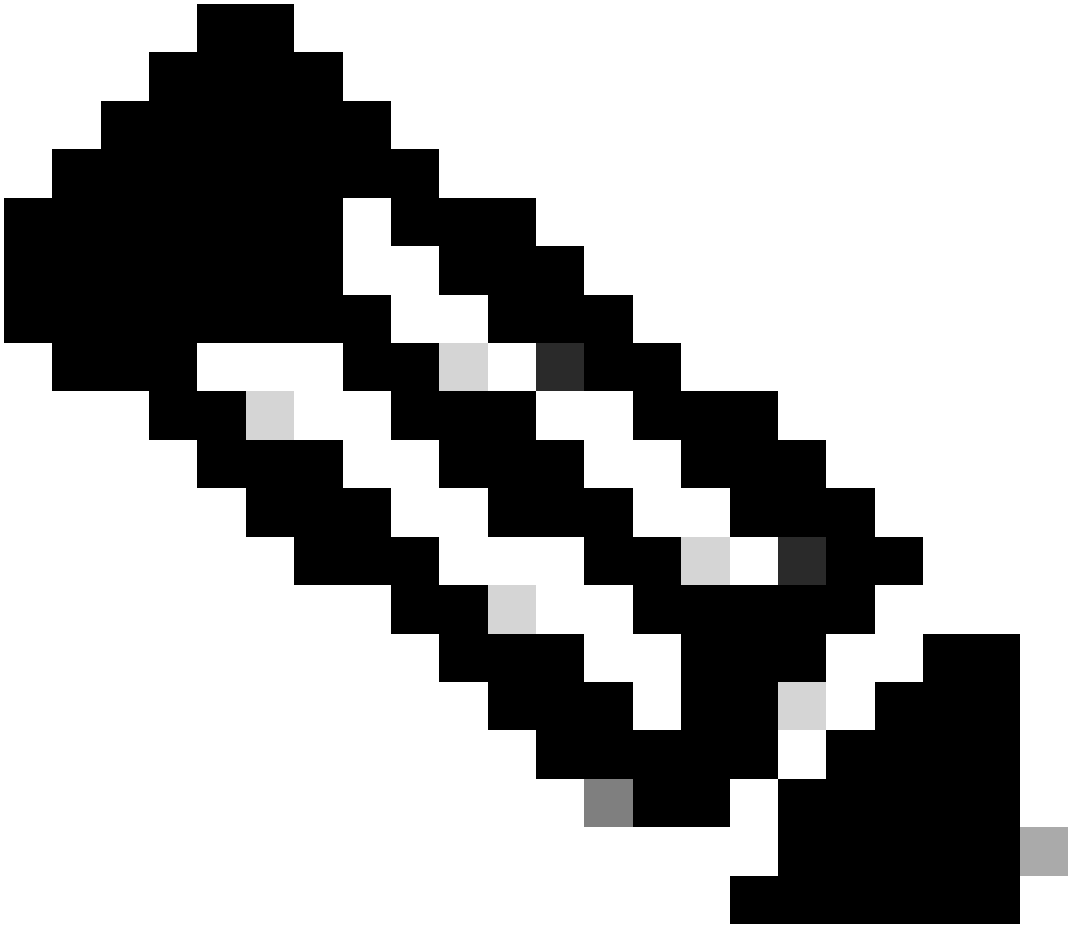
```
<#root>

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)
```

要驗證此症狀，請啟用Java控制檯日誌：



疑難排解 — 建議動作

請參閱軟體思科錯誤ID CSCwi56155 「Unable to access Secure Client Profile on ASDM（無法存取ASDM上的安全使用者端設定檔）」。



附註：此缺陷已在最近的ASDM軟體版本中修復。有關詳細資訊，請檢視缺陷詳細資訊。

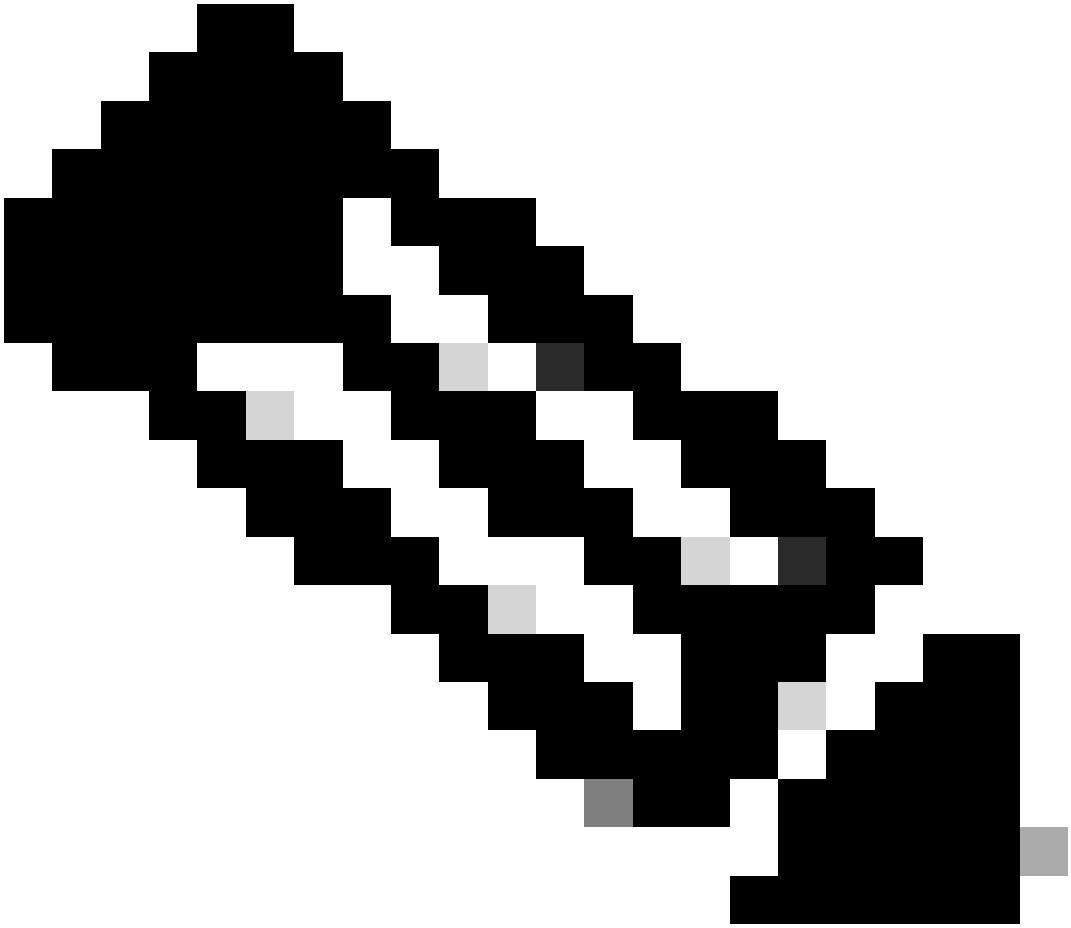
問題16.無法編輯ASDM上的安全客戶端配置檔案XML配置檔案

如果ASA裝置上存在低於版本4.8的AnyConnect映像，則無法在ASA裝置上編輯ASDM Configuration > Remote Access VPN > Network(Client)Access中的安全客戶端配置檔案XML配置檔案。

錯誤消息「裝置上的安全客戶端映像中沒有配置檔案編輯器外掛」。請轉到「網路（客戶端）訪問」>「安全客戶端軟體」並安裝Secure Client Image 2.5版或更高版本，然後重試」如圖所示。

疑難排解 — 建議動作

請參閱軟體思科錯誤ID CSCwk64399 「ASDM — 無法編輯安全使用者端設定檔」。解決方法是設定另一個優先順序較低的AnyConnect映像。



附註：此缺陷已在最近的ASDM軟體版本中修復。有關詳細資訊，請檢視缺陷詳細資訊。

問題17.配置更改後安全客戶端映像丟失

在ASDM Configuration > Network(Client)Access > Secure Client Profile中進行更改後，缺少Configuration > Network(Client)Access > Secure Client Software中的映像。

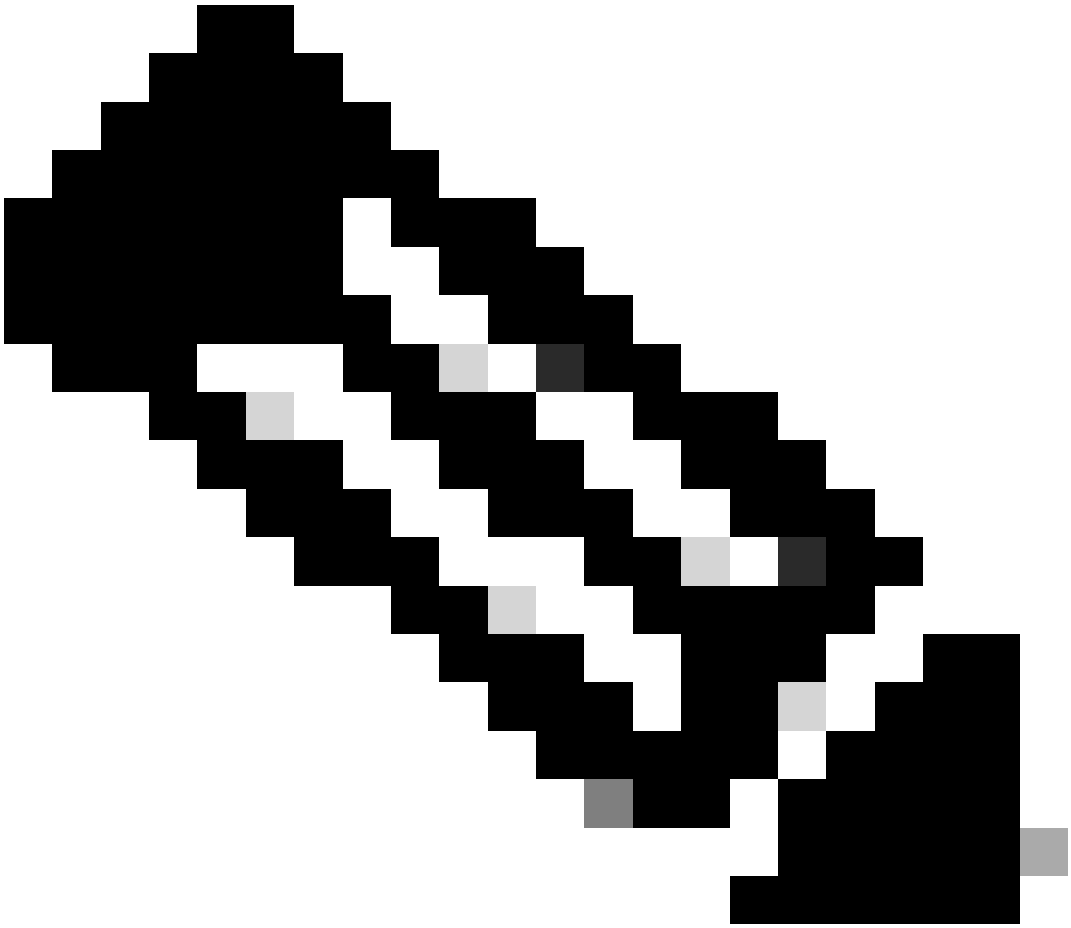
疑難排解 — 建議動作

請參閱軟體思科錯誤ID CSCwf23826 「Secure Client Software is not displayed after modifying the Secure Client Profile Editor in ASDM（修改ASDM中的安全使用者端設定檔編輯器後未顯示安全使用者端軟體）」。解決方法選項：

- 按一下ASDM中的「刷新」圖示

或

- 關閉並重新開啟ASDM



附註：此缺陷已在最近的ASDM軟體版本中修復。有關詳細資訊，請檢視缺陷詳細資訊。

問題十八 http server session-timeout和http server idle-timeout命令無效

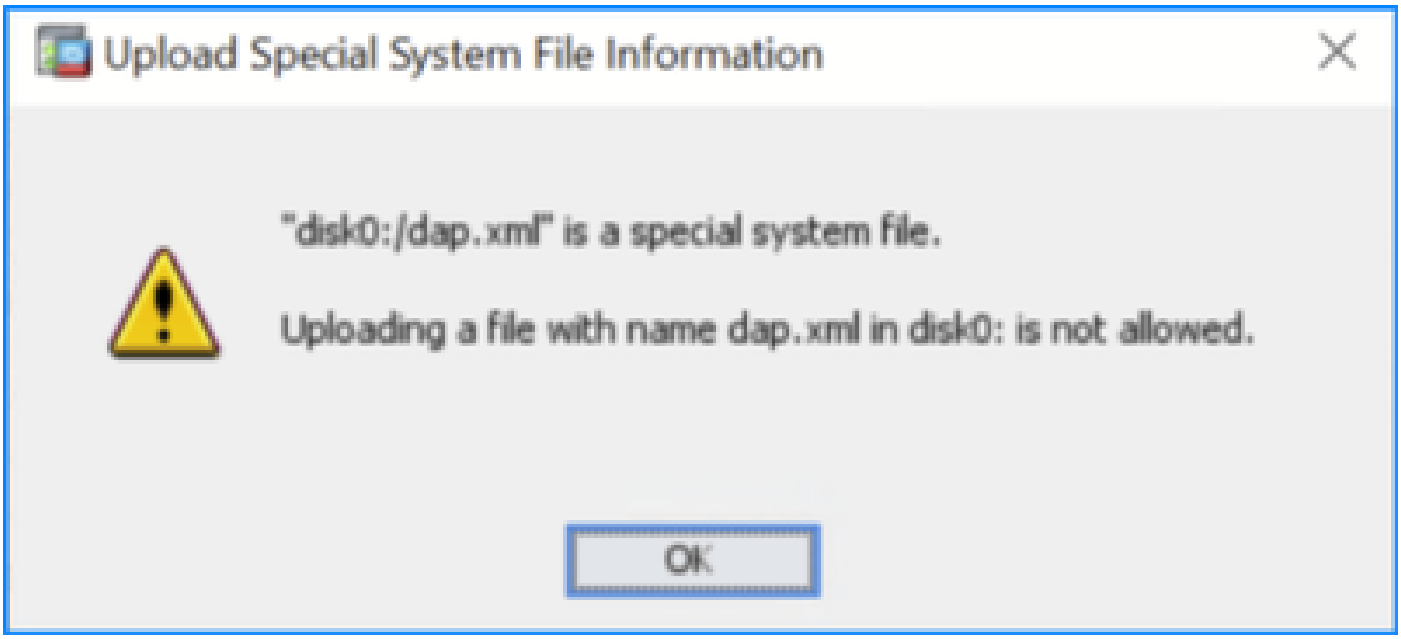
http server session-timeout和http server idle-timeout命令在多情景模式ASA中不起作用。

疑難排解 — 建議動作

請參閱軟體思科錯誤ID CSCtx41707 「Support for http server timeout command in multi-context mode」。這些命令是可配置的，但值不起作用。

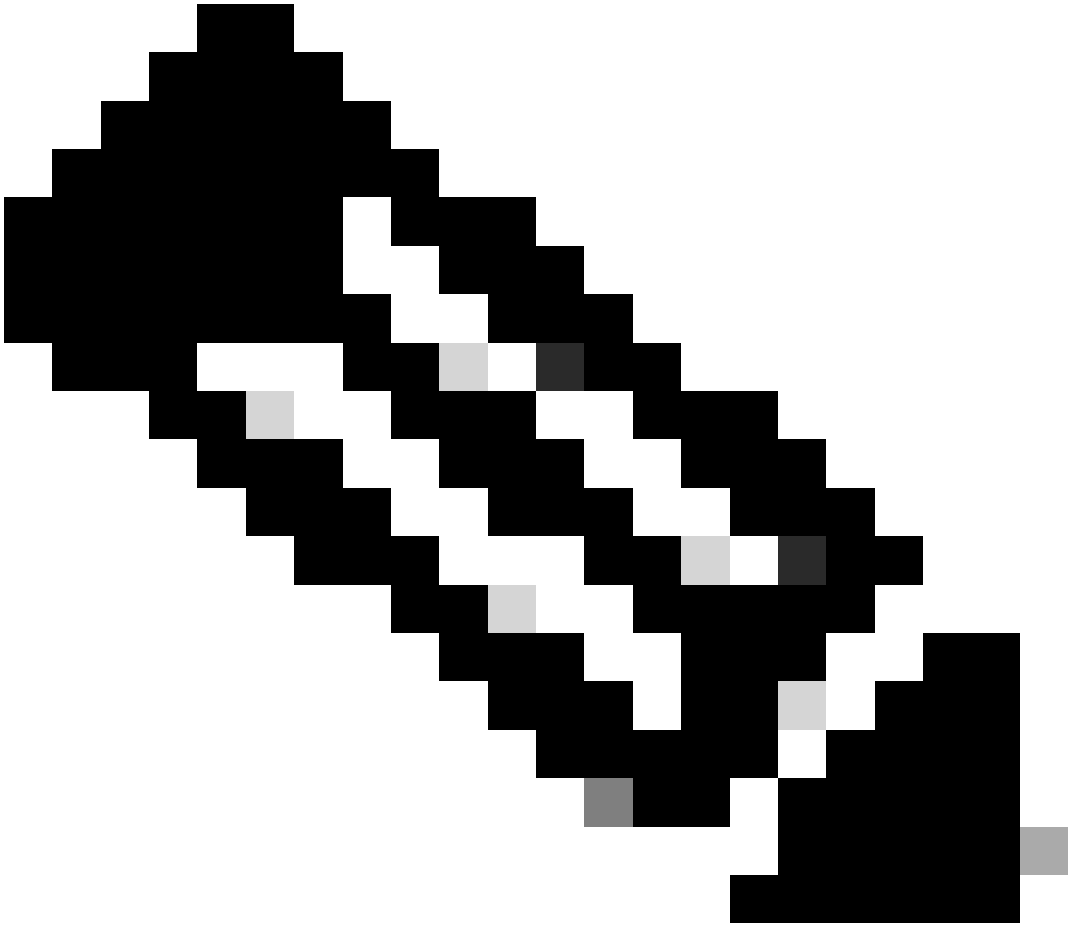
問題十九。 ASDM上的Dap.xml複製失敗

通過ASDM中的「檔案管理」視窗將dap.xml複製到ASA失敗，並出現錯誤「disk0:/dap.xml is a special system file」。將名為dap.xml的檔案上傳到disk0:不允許":



疑難排解 — 建議動作

請參閱軟體思科錯誤ID CSCvt62162 "Cannot copy dap.xml using File Management in ASDM 7.13.1"。解決方法是使用FTP或TFTP等協定將檔案直接複製到ASA。



附註：此缺陷已在最近的ASDM軟體版本中修復。有關詳細資訊，請檢視缺陷詳細資訊。

問題20.在ASDM上看不到IKE策略和IPSEC建議

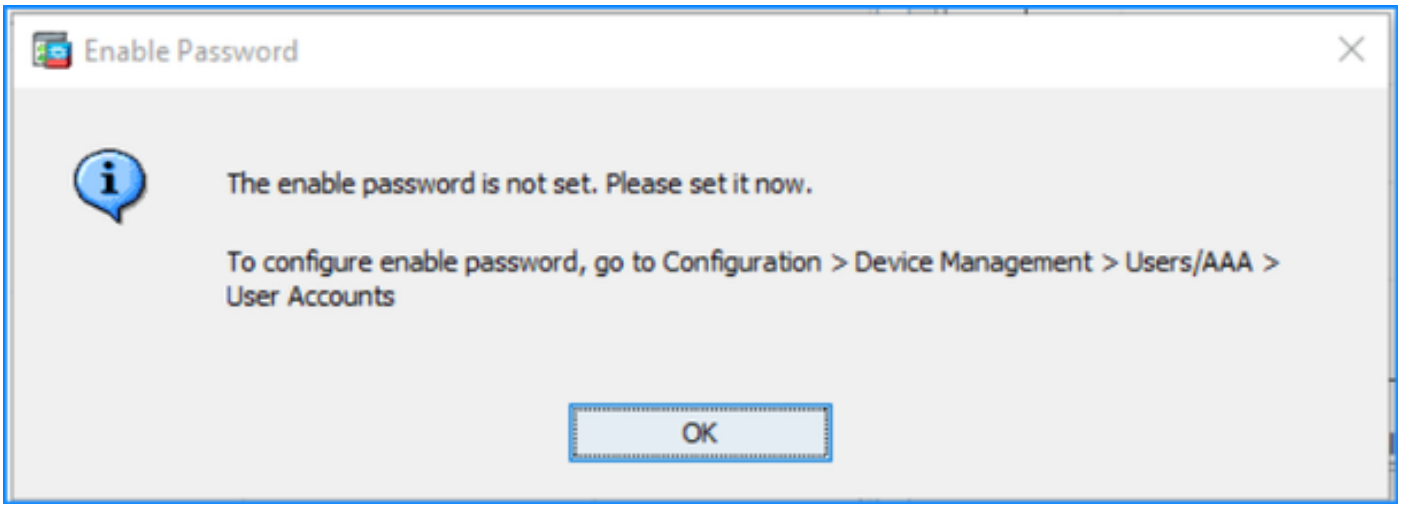
ASDM在Configurations > Site-to-Site VPN 視窗中不顯示IKE策略和IPSEC提議。

疑難排解 — 建議動作

請參閱軟體Cisco錯誤ID CSCwm42701 「ASDM在IKE原則和IPSEC提案標籤中顯示為空白」。

問題21. ASDM顯示消息「The enable password is not set.請立即設定。」

ASDM顯示消息「The enable password is not set.請立即設定。」 在命令列中更改啟用密碼後：



疑難排解 — 建議動作

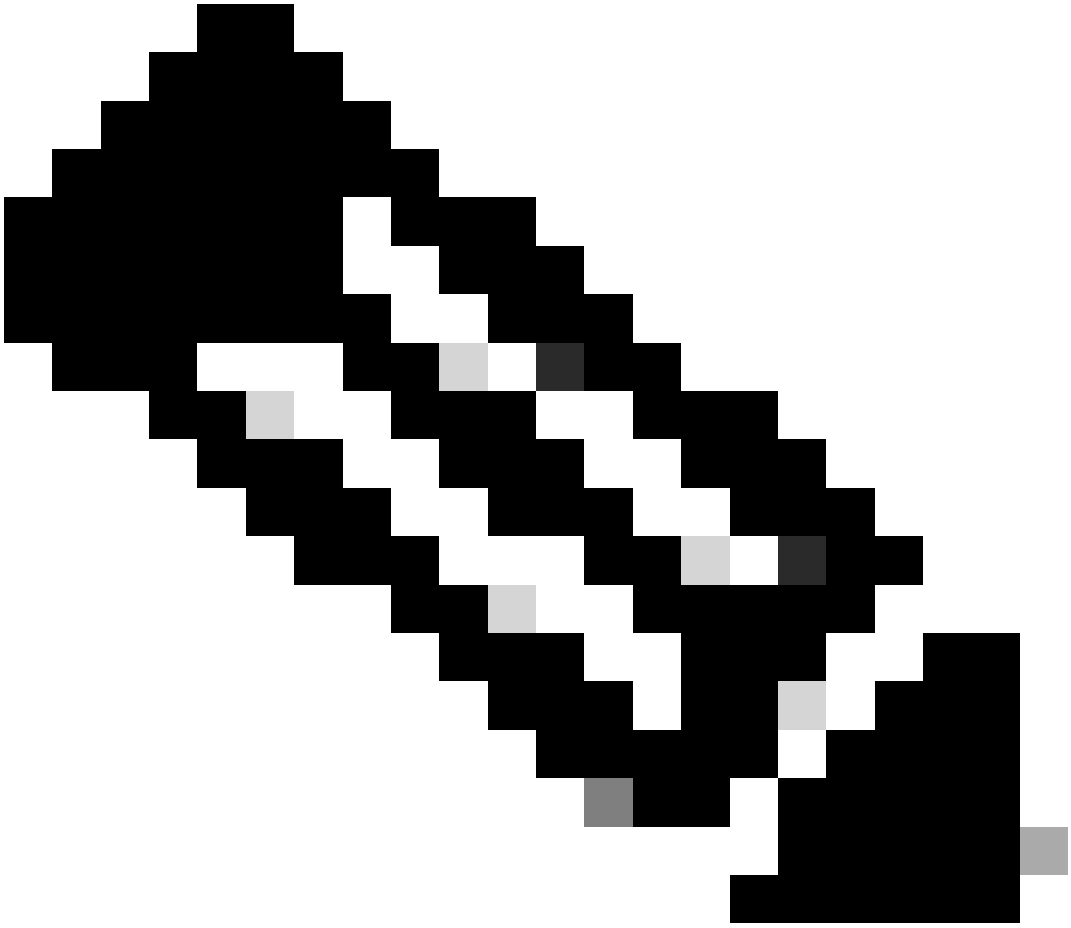
請參閱軟體思科錯誤ID CSCvq42317 「ASDM提示在CLI上設定啟用密碼後變更啟用密碼」。

問題二十二 刷新ASDM UI後，ASDN對象消失

將對象組和對象主機新增到現有對象組時，刷新ASDM後，對象組從ASDM清單中消失。要匹配此缺陷，對象名稱必須以數字開頭。

疑難排解 — 建議動作

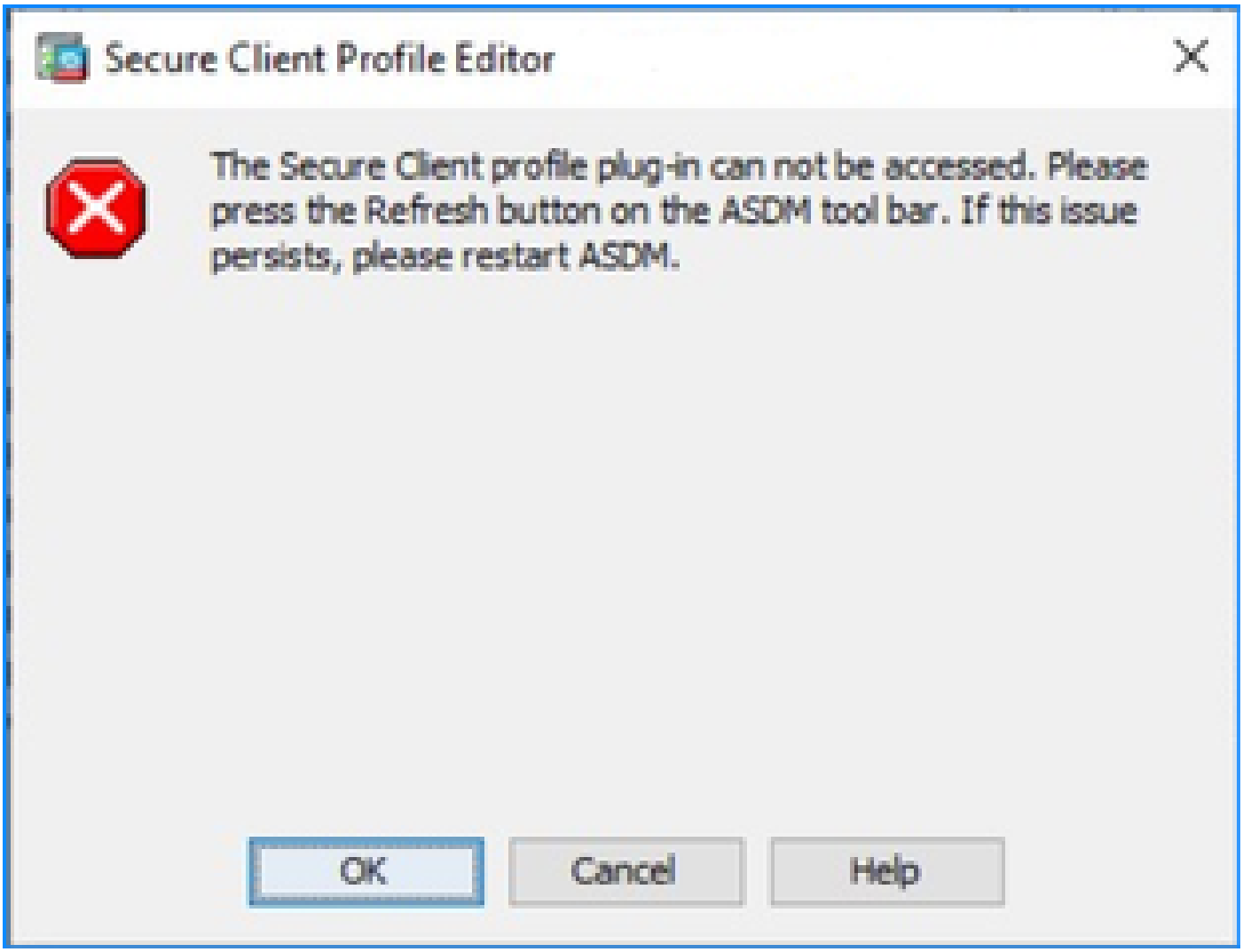
請參閱軟體思科錯誤ID CSCwf71723「ASDM正在失去已設定的物件/物件群組」。



附註：此缺陷已在最近的ASDM軟體版本中修復。有關詳細資訊，請檢視缺陷詳細資訊。

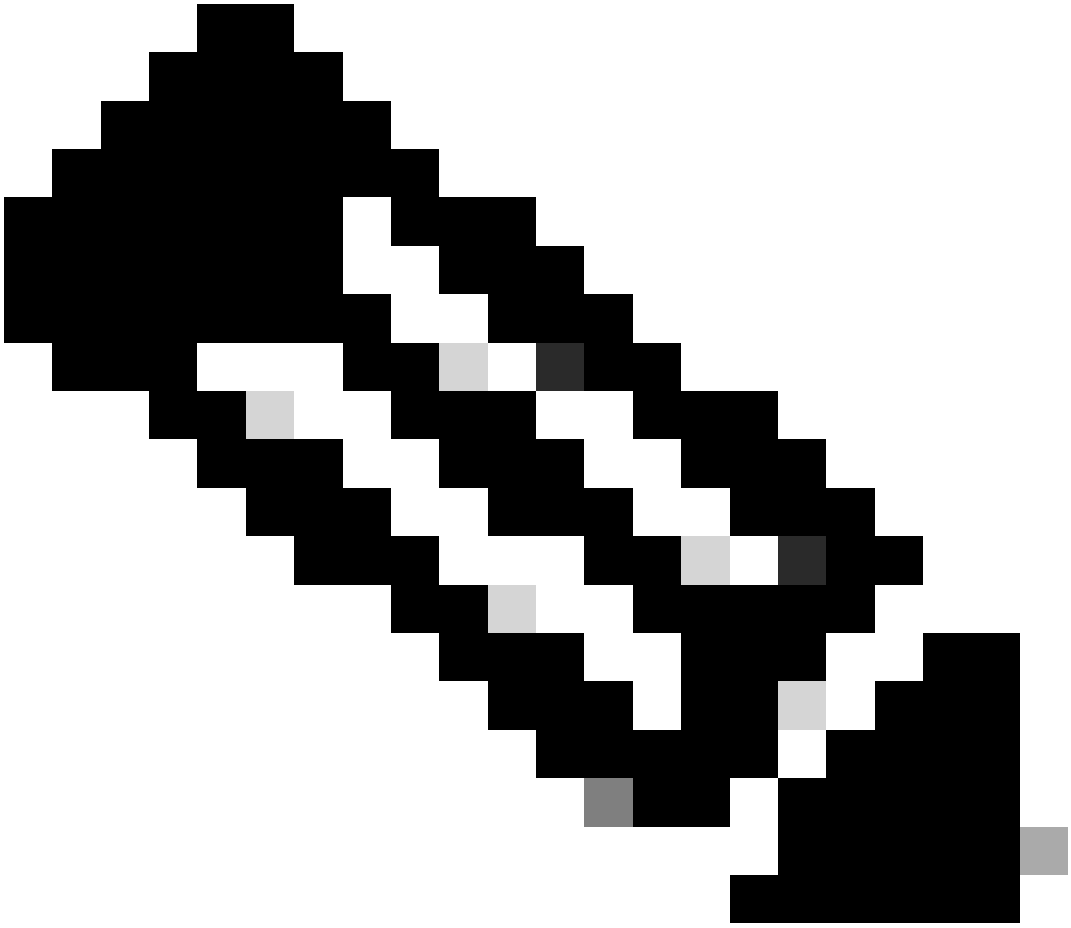
問題23.無法為低於4.5的版本編輯AnyConnect客戶端配置檔案

無法為4.5版之前的AnyConnect配置檔案編輯AnyConnect客戶端配置檔案。錯誤消息為「The Secure Client profile plug-in cannot be access（無法訪問安全客戶端配置檔案外掛）」。請按ASDM工具欄上的「刷新」按鈕。如果此問題仍然存在，請重新啟動ASDM。」：



疑難排解 — 建議動作

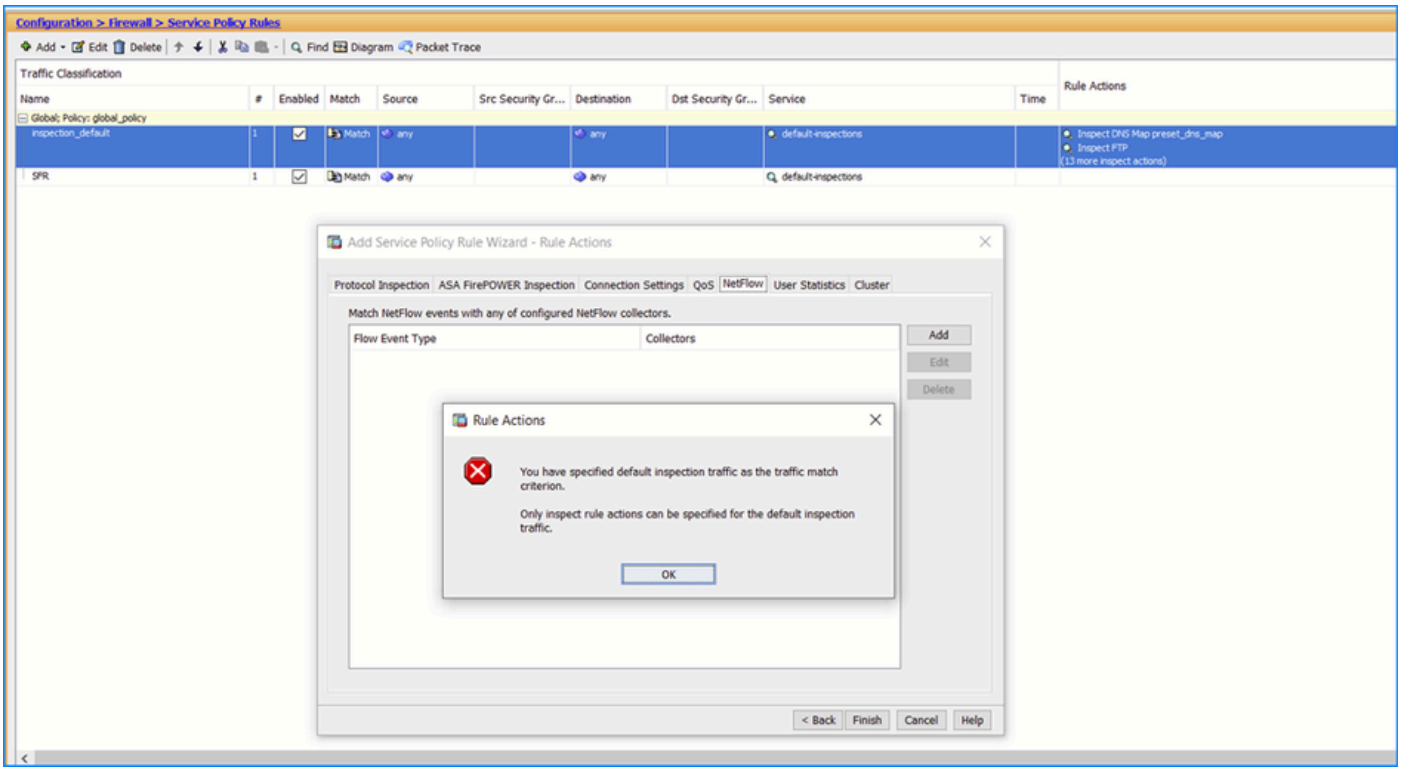
請參閱軟體思科錯誤ID CSCwf16947 "ASDM — 無法載入Anyconnect設定檔編輯器"。



附註：此缺陷已在最近的ASDM軟體版本中修復。有關詳細資訊，請檢視缺陷詳細資訊。

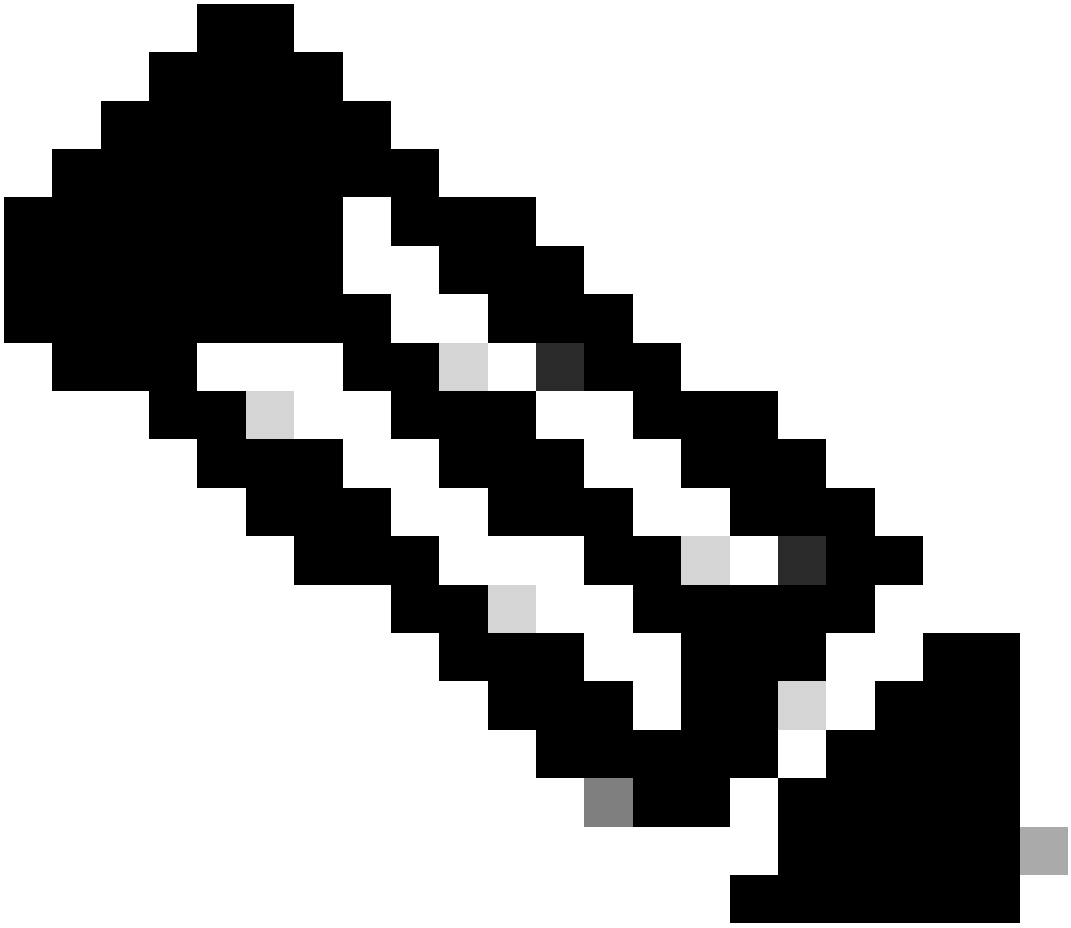
問題24.無法導航到編輯服務策略>規則操作> ASA FirePOWER檢查頁籤

在ASDM 7.8.2版中，使用者無法導航到Edit Service Policy > Rule Actions > ASA FirePOWER Inspection頁籤，並顯示錯誤：「您已指定預設檢測流量作為流量匹配條件。只能為預設檢測流量指定檢查規則操作。" 即使已選擇ACL進行重新導向，也會發生以下情況：



疑難排解 — 建議動作

請參閱軟體思科錯誤ID CSCvg15782 「ASDM — 升級至版本7.8(2)後無法檢視修改SFR流量重新導向」。解決方法是使用CLI編輯策略對映配置。



附註：此缺陷已在最近的ASDM軟體版本中修復。有關詳細資訊，請檢視缺陷詳細資訊。

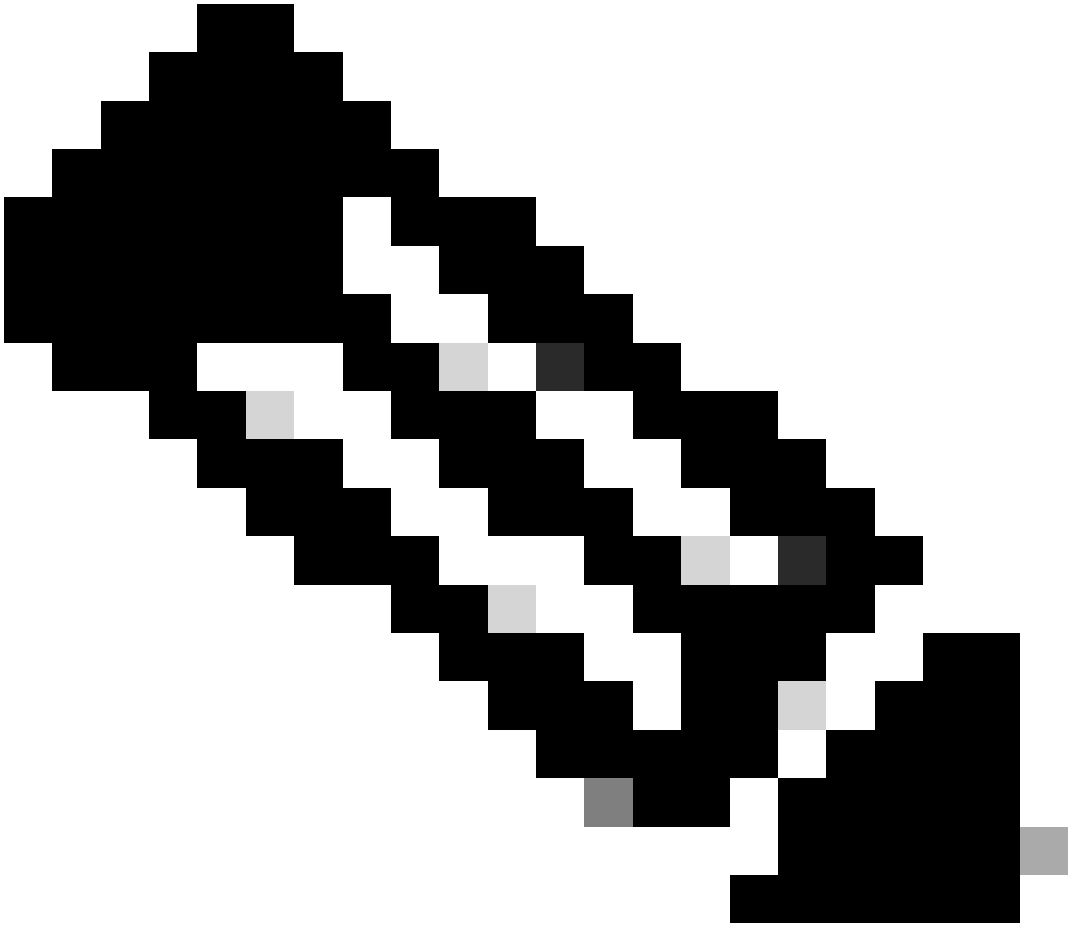
問題25. ASDM上的AnyConnect映像5.1版和AnyConnect配置檔案編輯器

在Secure Client軟體5.1版中觀察到以下症狀：

1. 載入Win/Mac/Linux包時未列出組策略模組名稱
2. ASDM無法開啟AnyConnect配置檔案編輯器。

疑難排解 — 建議動作

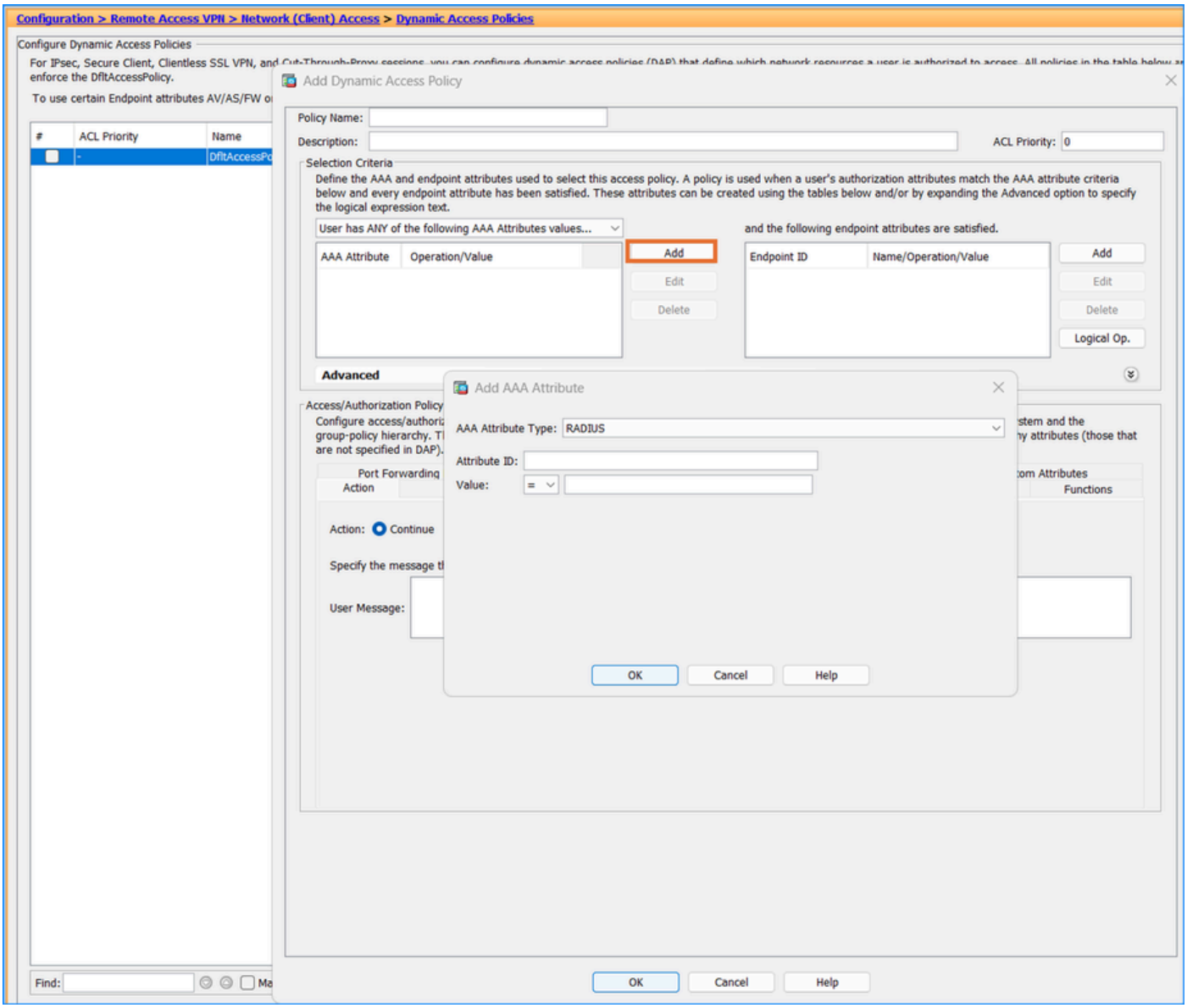
請參閱軟體思科錯誤ID CSCwh7417 "ASDM:使用CSC映像5.1時，無法載入AnyConnect配置檔案編輯器和組策略。解決方法是使用較低版本的Secure Client。



附註：此缺陷已在最近的ASDM軟體版本中修復。有關詳細資訊，請檢視缺陷詳細資訊。

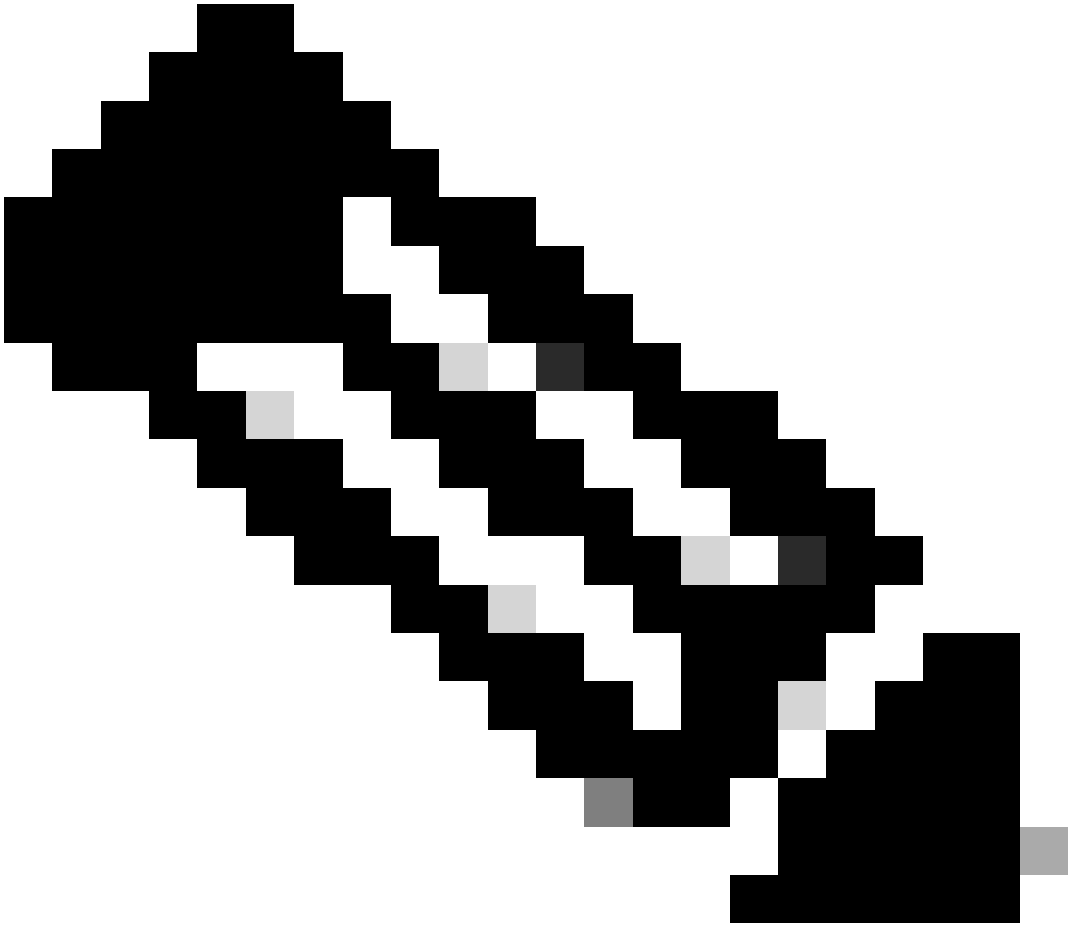
問題二十六 AAA屬性型別(Radius/LDAP)在ASDM中不可見

AAA屬性型別(Radius/LDAP)在ASDM > Configuration > Remote Access VPN > Network(Client)Access > Dynamic Access Policies>Add > On AAA attribute field > Add > Select Radius or LDAP中不可見：



疑難排解 — 建議動作

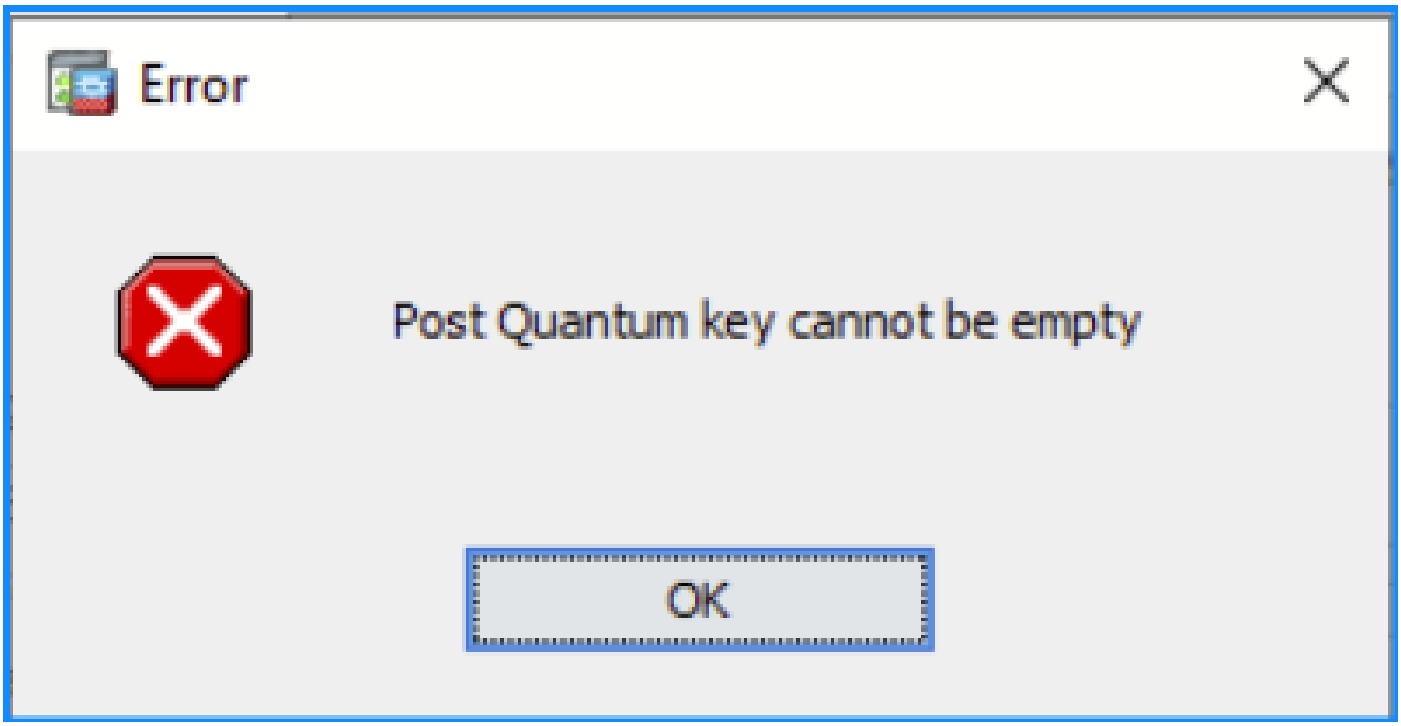
請參閱軟體思科錯誤ID CSCwa99370 "ASDM:ASDM:DAP config missing AAA Attributes type(Radius/LDAP)"和Cisco bug ID CSCwd16386 "ASDM:DAP config missing AAA Attributes type(Radius/LDAP)"。



附註：這些缺陷已在最近的ASDM軟體版本中得到修復。有關詳細資訊，請檢視缺陷詳細資訊。

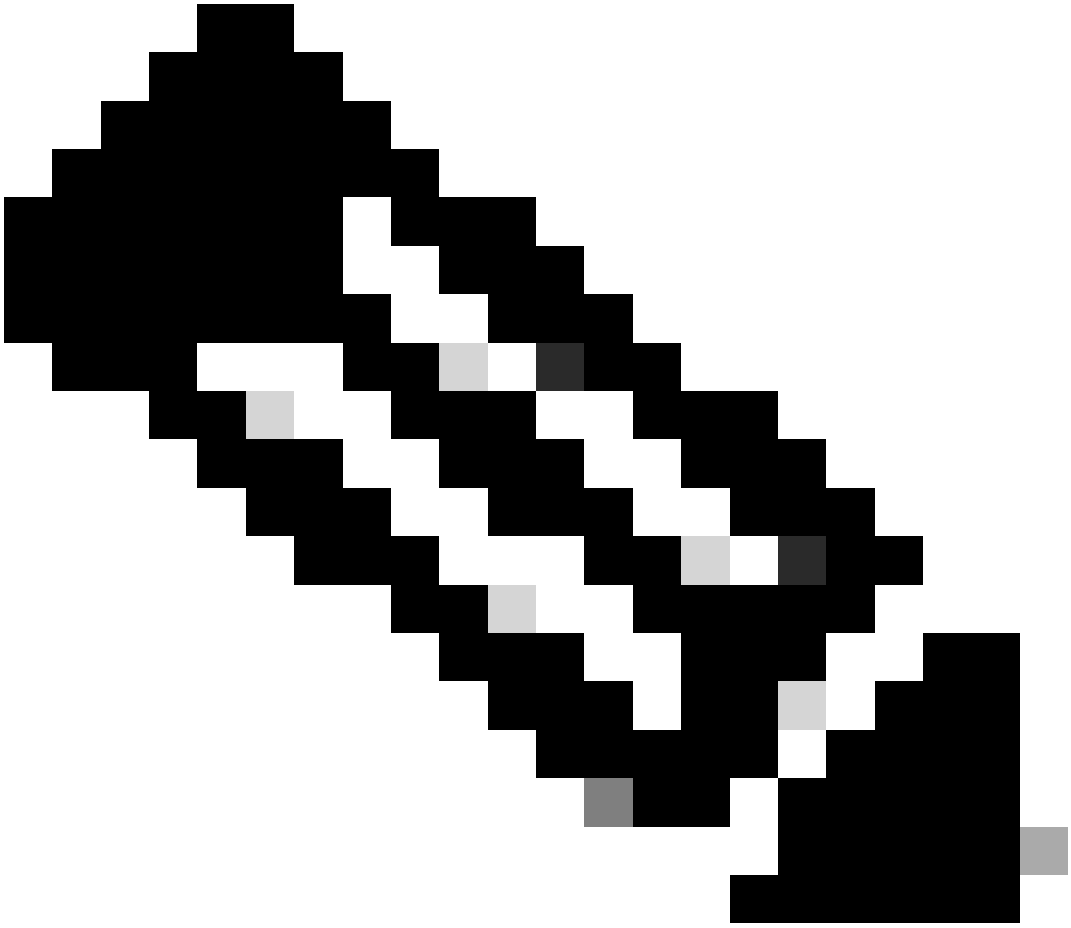
問題二十七 ASDM上顯示「Post Quantum key cannot be empty」錯誤

編輯ASDM > Configuration > Remote Access VPN > Network(Client)Access>IPsec(IKEv2)Connection Profiles中的Advanced部分時，會顯示錯誤「Post Quantum key cannot be empty」：



疑難排解 — 建議動作

請參閱軟體思科錯誤ID CSCwe58266 「ASDM IKev2組態 — 量子金鑰後不能為空錯誤訊息」。



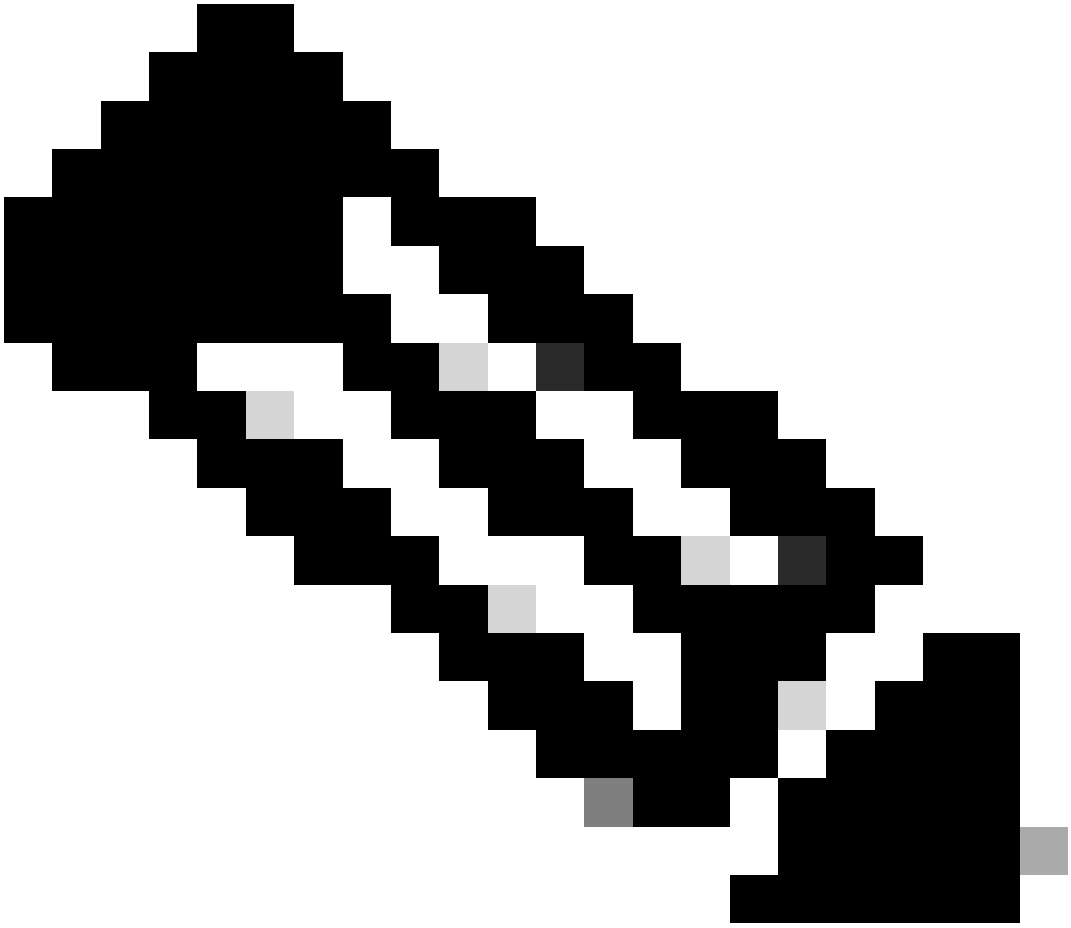
附註：此缺陷已在最近的ASDM軟體版本中修復。有關詳細資訊，請檢視缺陷詳細資訊。

問題二十八 ASDM在使用選項「使用位置」時不會顯示任何結果

當使用「使用位置」選項時，ASDM不會顯示任何結果，該選項是通過導航到Configuration > Firewall > Objects > Network Objects/Groups並按一下右鍵Object找到的。

疑難排解 — 建議動作

請參閱軟體思科錯誤ID CSCwd98702 「Where used」選項（在ASDM中無法使用）。



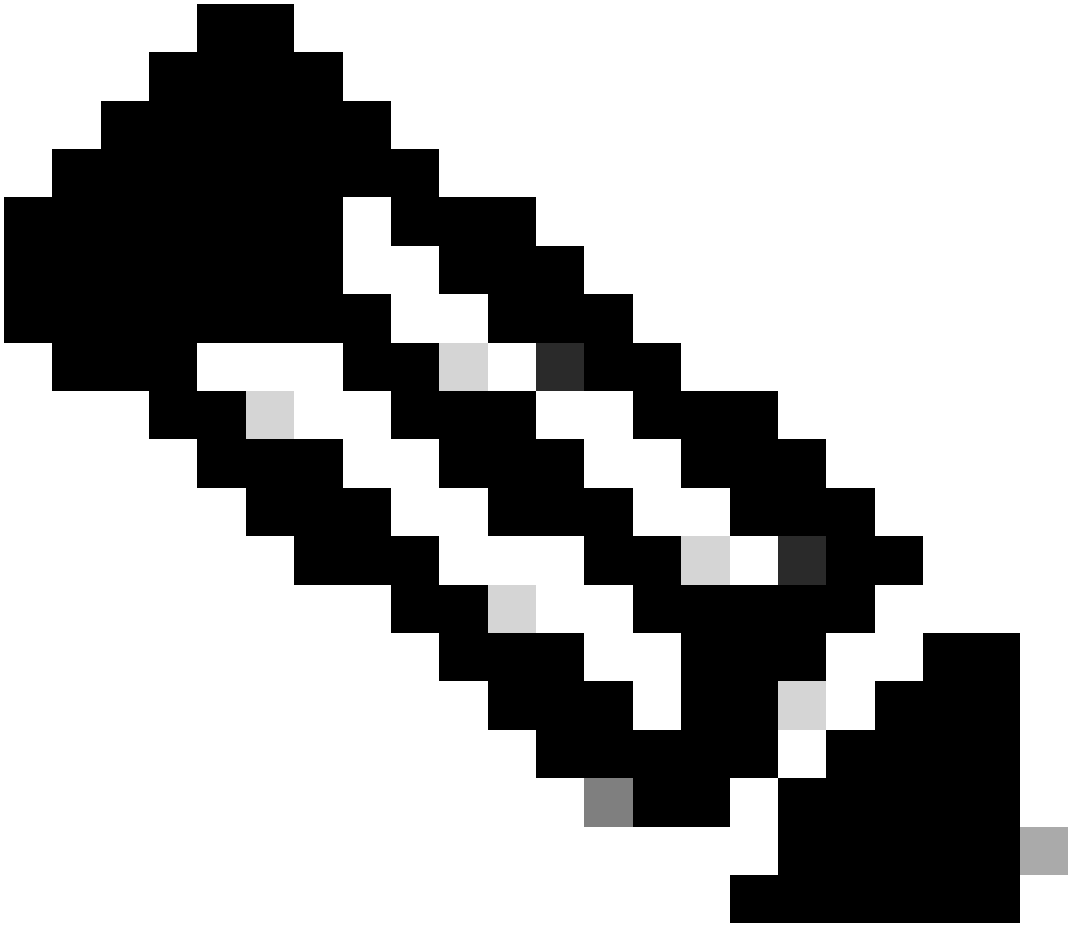
附註：此缺陷已在最近的ASDM軟體版本中修復。有關詳細資訊，請檢視缺陷詳細資訊。

問題二十九 刪除網路對象時，無法刪除警告消息「[網路對象]，因為此消息在下面使用」

在Configuration > Firewall > Objects > Network Objects/Groups中刪除網路組中引用的網路對象時，ASDM不會顯示警告消息「[Network Object] cannot be deleted because it in the following」。

疑難排解 — 建議動作

請參閱軟體思科錯誤ID CSCwe67056 "[網路物件]無法刪除，因為它用於以下"警告未顯示"中。



附註：此缺陷已在最近的ASDM軟體版本中修復。有關詳細資訊，請檢視缺陷詳細資訊。

問題三十。 ASDM中「網路對象/組」頁籤的可用性問題

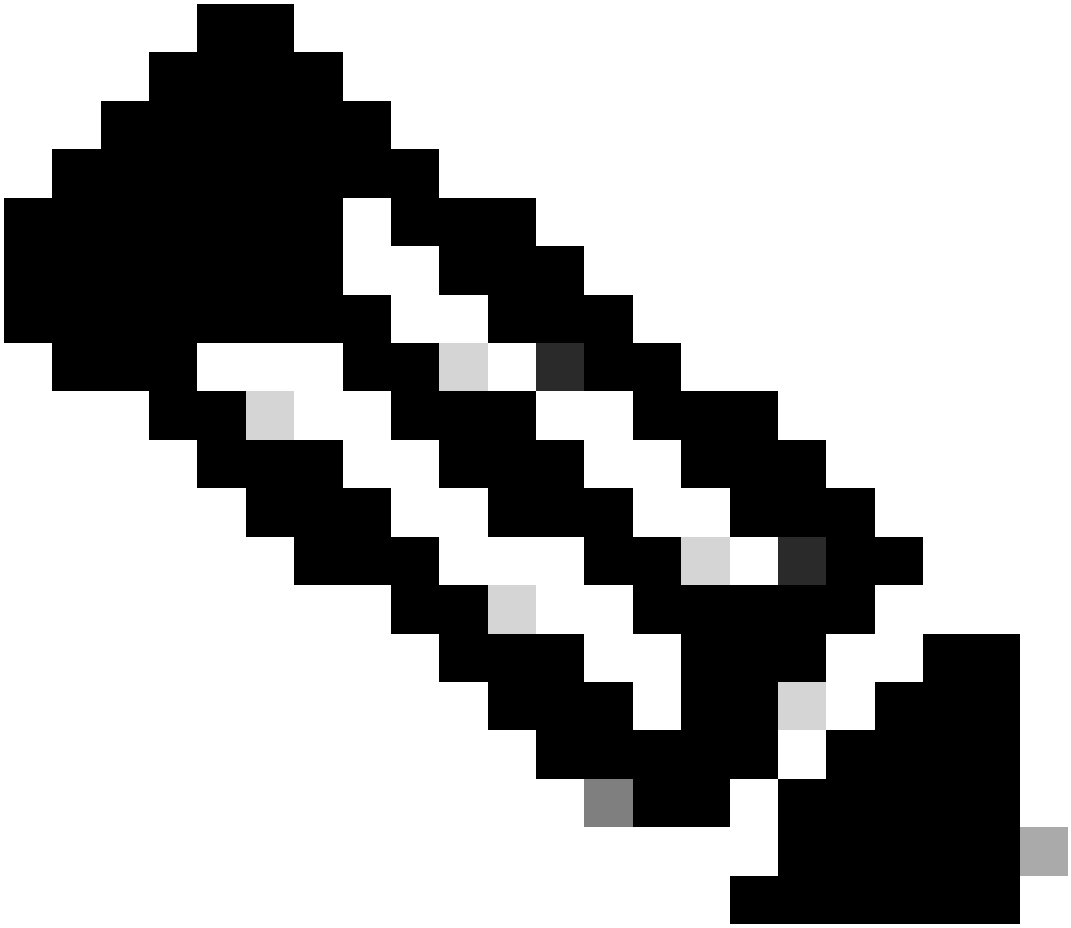
觀察到以下一個或多個症狀：

- 「Add/Edit Object Group Windows」的「Create new Object Member」部分中的「Name」文本輸入標籤為「optional」。 但是，除非輸入名稱，否則用於建立和新增對象的「Add>>」按鈕將被禁用。
- 當使用者按一下「使用位置……」時開啟的「使用例項」頁籤 上下文選單僅列出直接引用該對象的實體（ACL、路由對映、對象組）。它還必須遞迴地列出第二、第三等。順序引用（即使用包含對象的對象組的ACL也必須列為對象的「用法」）。
- 上下文選單中的「刪除」操作也會顯示此行為。它會自動刪除直接引用該對象的任何實體（如果刪除對象時該實體變為空）。 當第二次、第三次等等，它不會這樣操作。由於刪除了對象和第一個訂單引用，訂單引用將變為空。

使用者可以相信ASDM會阻止由於從其餘配置中刪除對象而變為空的實體。然而，情況未必如此。

疑難排解 — 建議動作

請參閱軟體思科錯誤ID CSCwe86257 「ASDM中網路物件/群組標籤的可用性」。

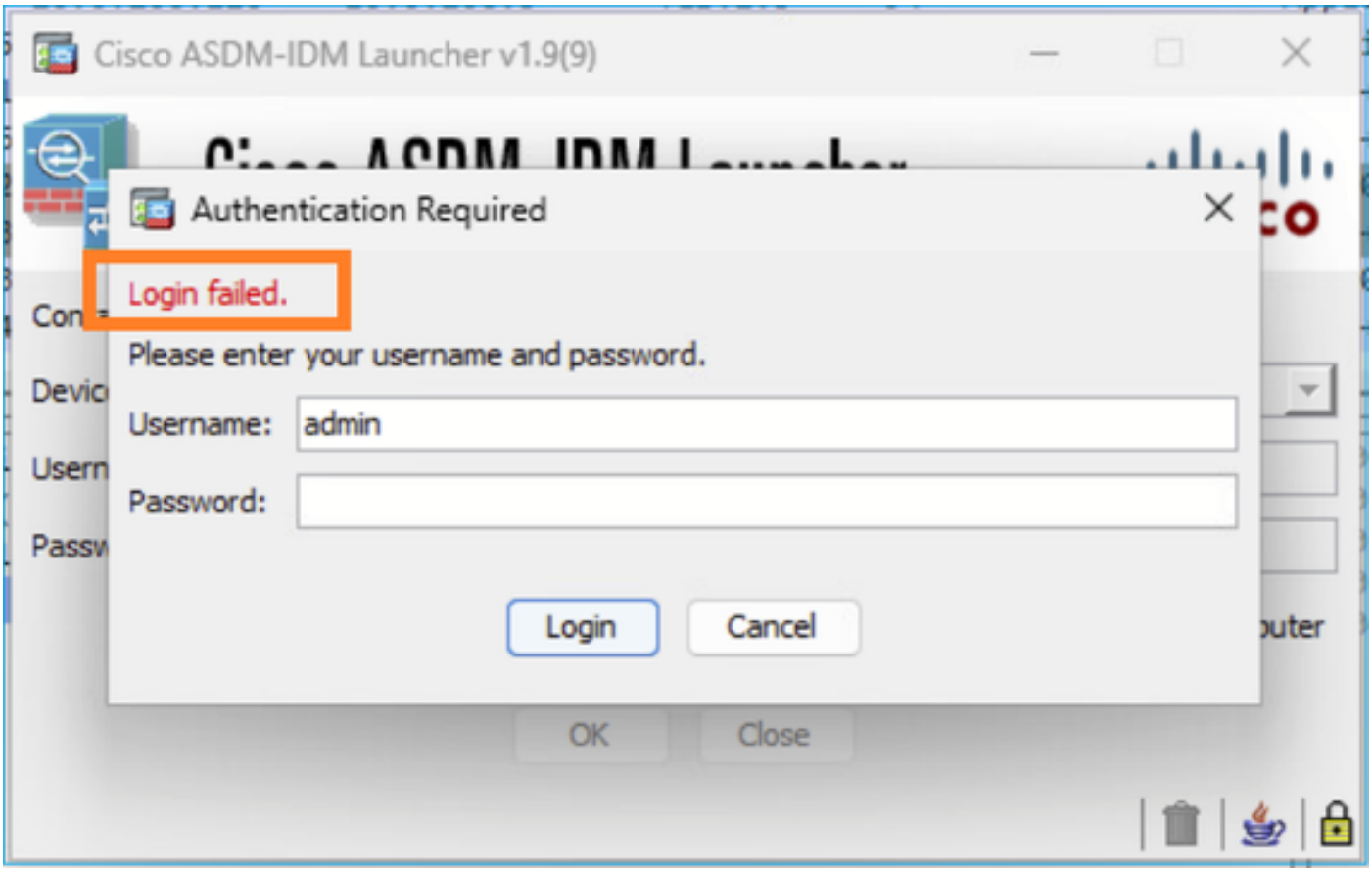


附註：此缺陷已在最近的ASDM軟體版本中修復。有關詳細資訊，請檢視缺陷詳細資訊。

排除ASDM身份驗證問題

問題1. ASDM登入失敗

ASDM UI上顯示的錯誤為：



疑難排解 — 建議動作

當在同一介面上同時啟用HTTP和Webvpn Cisco Secure Client(AnyConnect)時，可以看到此錯誤。因此，必須滿足以下所有條件：

1. AnyConnect/Cisco Secure Client在介面上啟用
2. HTTP伺服器在與AnyConnect/Cisco安全客戶端相同的介面和埠上啟用

範例：

```
<#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：啟用「debug http 255」，您可以看到ASDM和Webvpn之間的衝突：

```
<#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
```

另外請注意，儘管登入失敗，但ASA系統日誌顯示身份驗證成功：

```
<#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
```

因應措施

解決方法1

更改ASA HTTP伺服器的TCP埠，例如：

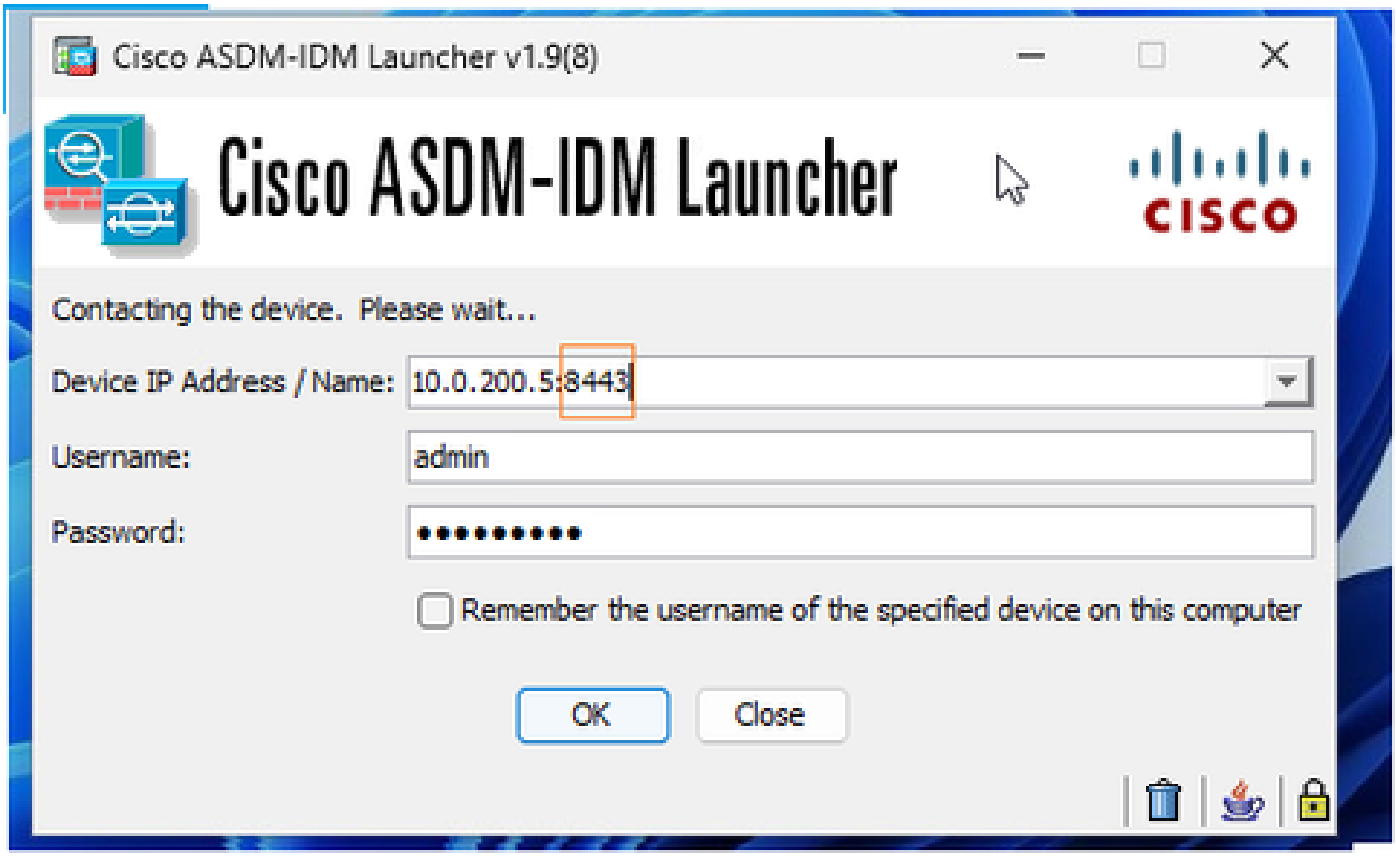
<#root>

ciscoasa#

configure terminal

ciscoasa(config)#

http server enable 8443



解決方法2

更改AnyConnect/Cisco安全客戶端的TCP埠，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
```

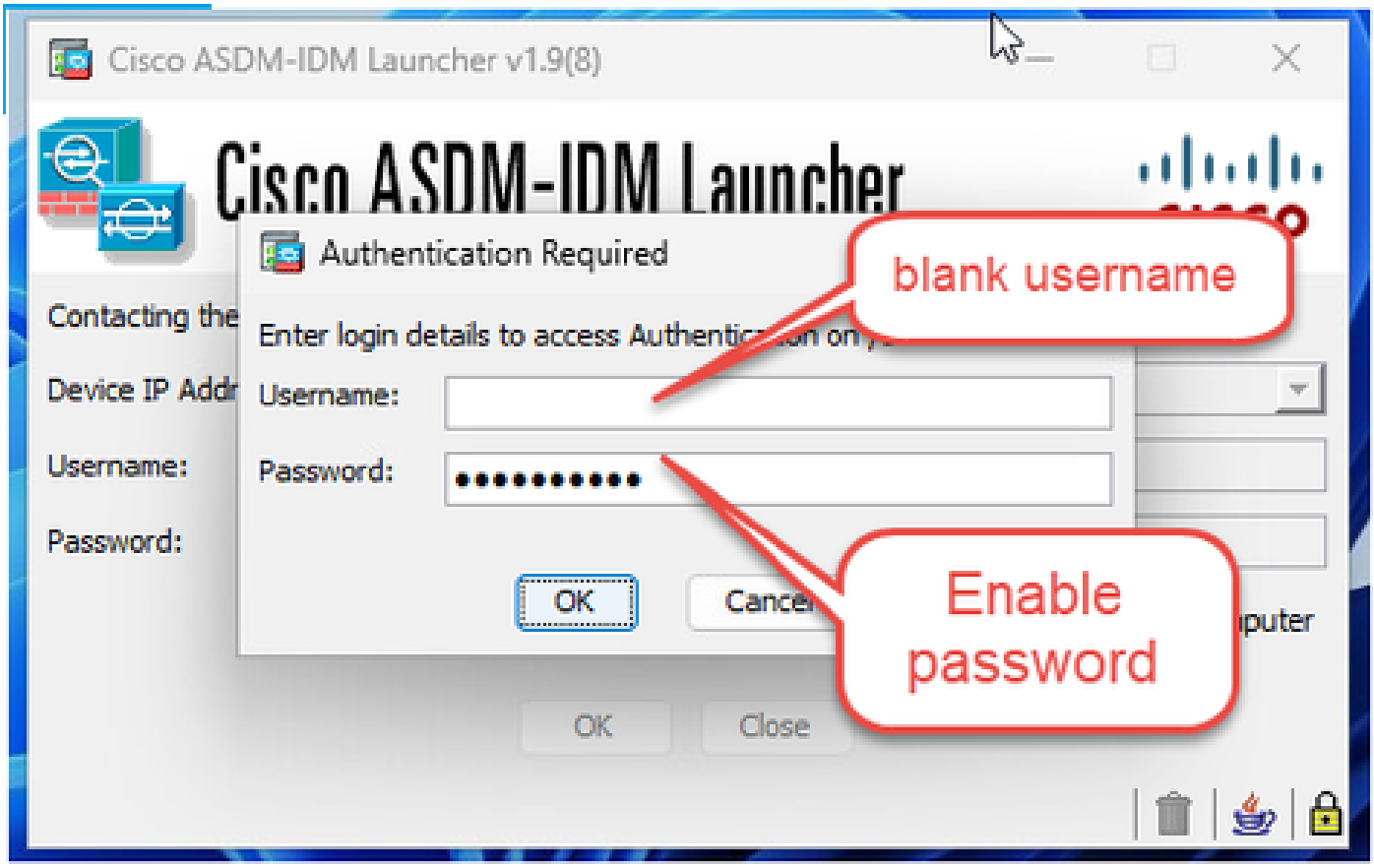
解決方法3

另一種解決方法是刪除「aaa authentication http console」配置：

<#root>

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

在這種情況下，您只需使用啟用密碼即可登入到ASDM:



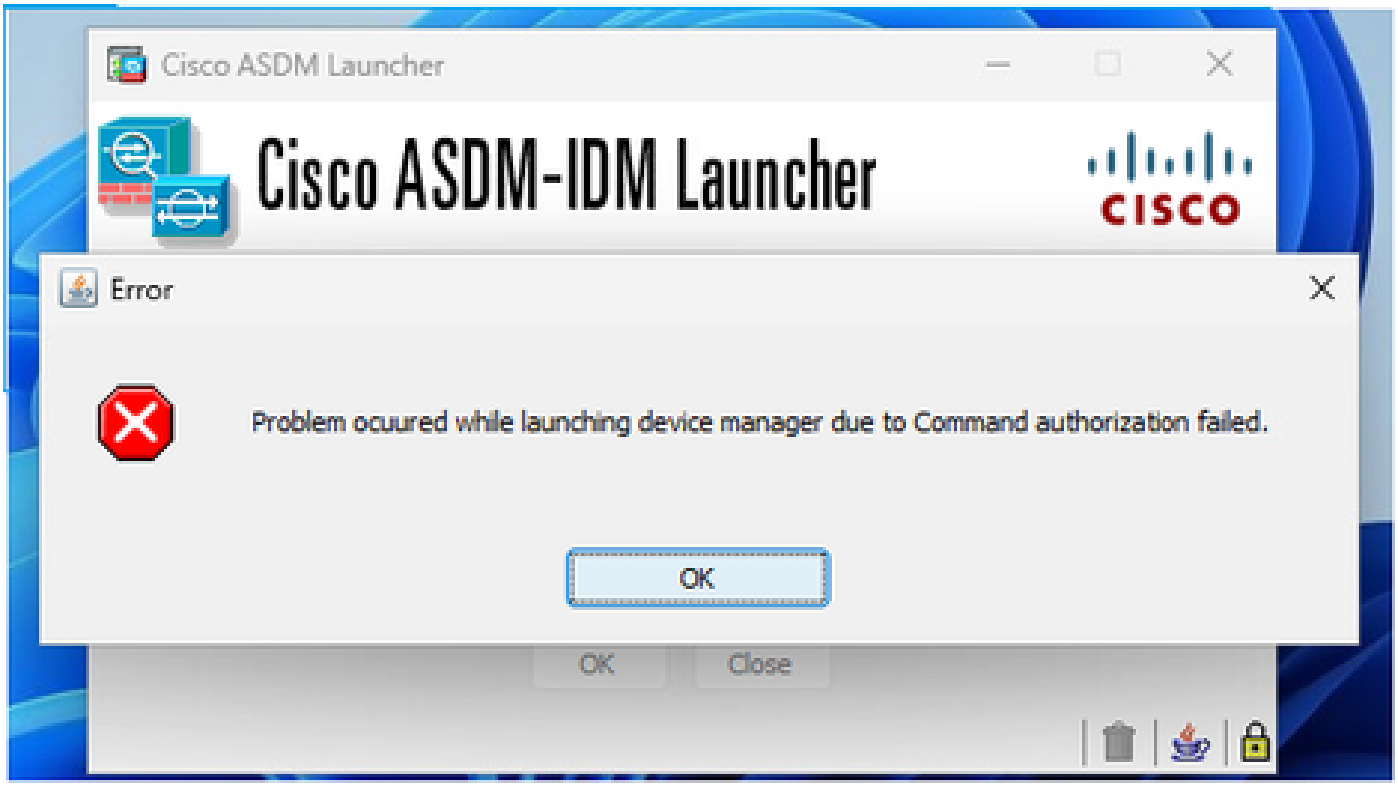
相關缺陷

思科錯誤ID CSCwb67583

當在同一介面上啟用webvpn和ASDM時新增警告

問題2. ASDM命令授權失敗

ASDM UI上顯示的錯誤為：



疑難排解 — 建議步驟

檢查ASA上的AAA配置並確保：

- 您還配置了aaa身份驗證。
- 如果使用遠端身份驗證伺服器，則它可訪問並授權命令。

參考

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

問題3.配置ASDM只讀訪問

有時您想為ASDM使用者提供只讀訪問許可權。

疑難排解 — 建議步驟

建立具有自定義許可權級別(5)的新使用者，例如：

<#root>

asa(config)#

username [username] password [password] privilege 5

此命令建立許可權級別為5的使用者，即「僅監控」級別。將「[username]」和「[password]」替換為所需的使用者名稱和密碼。

詳細資料

本地命令授權允許您將命令分配到16個許可權級別（0到15）之一。 預設情況下，將每個命令分配給許可權級別0或15。您可以將每個使用者定義為處於特定許可權級別，並且每個使用者都可以在分配的許可權級別或更低級別輸入任何命令。ASA支援在本地資料庫、RADIUS伺服器或LDAP伺服器中定義的使用者許可權級別（如果將LDAP屬性對映到RADIUS屬性）。

程式

步驟 1	選擇Configuration > Device Management > Users/AAA > AAA Access > Authorization。
步驟 2	選中Enable authorization for ASA command access > Enable覈取方塊。
步驟 3	從Server Group下拉選單中選擇LOCAL。
步驟 4	啟用本地命令授權時，您可以選擇手動將許可權級別分配給單個命令或命令組，或者啟用預定義的使用者帳戶許可權。 ·按一下Set ASDM Defined User Roles以使用預定義的使用者帳戶許可權。 出現「ASDM Defined User Roles Setup」對話方塊。按一下Yes使用預定義的使用者帳戶許可權：Admin(許可權級別15，擁有對所有CLI命令的完全訪問許可權；唯讀（許可權級別5，具有只讀訪問許可權）；和Monitor Only(許可權級別3，僅有權訪問Monitoring部分)。 ·按一下Configure Command Privileges以手動配置命令級別。 出現Command Privileges Setup對話方塊。您可以從Command Mode下拉選單中選擇All Modes來檢視所有命令，也可以選擇配置模式來檢視該模式下可用的命令。例如，如果選擇上下文，則可以檢視在上下文配置模式下可用的所有命令。如果可以在使用者EXEC模式或特權EXEC模式以及配置模式下輸入命令，並且該命令在每個模式下執行不同的操作，則可以分別設定這些模式的許可權級別。

	Variant列顯示show、clear或cmd。您只能為命令的show、clear或configure形式設定許可權。命令的configure形式通常是導致配置更改的形式，如unmodified命令（不帶show或clear字首）或no形式。 要更改命令的級別，請按兩下該命令或按一下編輯。您可以將0到15之間的級別設定。您只能配置main命令的許可權級別。例如，您可以分別配置所有aaa命令的級別，但不配置aaa authentication命令和aaa authorization命令的級別。 要更改顯示的所有命令的級別，請按一下Select All，然後按一下Edit。 按一下OK接受更改。
步驟 5	按一下「Apply」。 分配授權設定，並將更改儲存到運行配置。

參考

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

問題4. ASDM多重身份驗證(MFA)

疑難排解 — 建議步驟

在撰寫本文時，ASDM不支援MFA（或2FA）。 此限制包括MFA和PingID等解決方案。

參考

思科錯誤ID CSCvs85995

ENH:使用雙因素身份驗證或MFA的ASDM訪問

問題5. ASDM外部身份驗證配置

疑難排解 — 建議步驟

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

參考資料

- 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

問題6. ASDM本地身份驗證失敗

疑難排解 — 建議步驟

如果您使用外部身份驗證和LOCAL身份驗證作為回退，則只有在外部伺服器關閉或者不工作的情況下，本地身份驗證才起作用。只有在這種情況下，LOCAL身份驗證才會接管並且您可以與LOCAL使用者連線。

這是因為外部身份驗證優先於本地身份驗證。

範例：

<#root>

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

參考

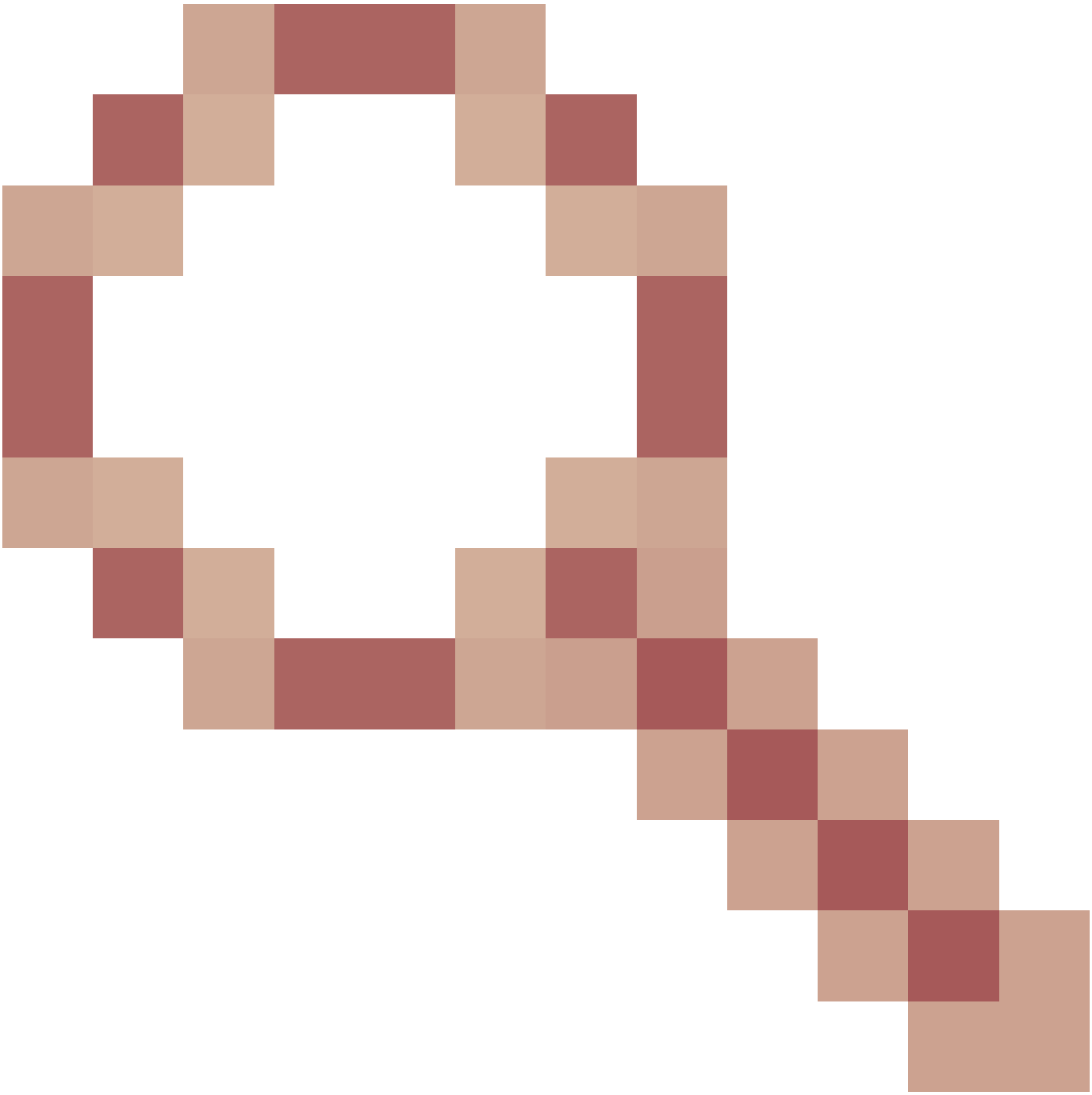
- https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/A-H/asa-command-ref-A-H/aa-ac-commands.html#wp6184732320

問題7. ASDM一次性密碼

疑難排解 — 建議步驟

- 在ASA 8.x - 9.x版本中以及在僅單路由模式下新增了ASDM OTP（一次性密碼）身份驗證支援。
- 用於ASA防火牆透明模式和/或多情景模式的ASDM OTP身份驗證不進入此類別。

請參閱思科錯誤id CSCtf23419



ENH:多情景和透明模式中的ASDM OTP身份驗證支援

問題8.連線配置檔案未顯示所有方法

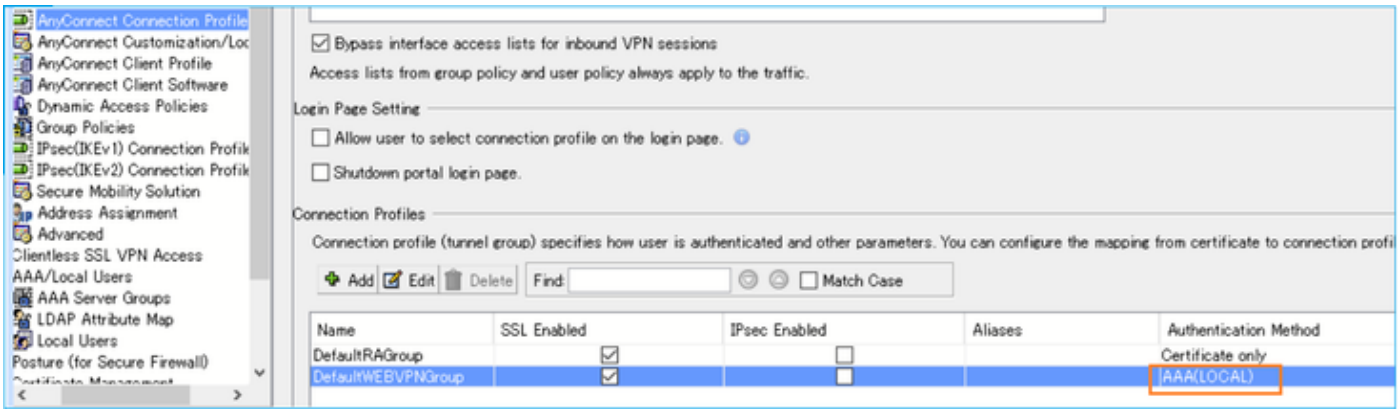
本例中的問題是ASA CLI配置與ASDM UI不匹配。

具體來說，CLI具有以下功能：

<#root>

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

而ASDM UI未提及證書方法：



疑難排解 — 建議步驟

這是一個表面問題。此方法未顯示在ASDM中，但使用證書身份驗證。

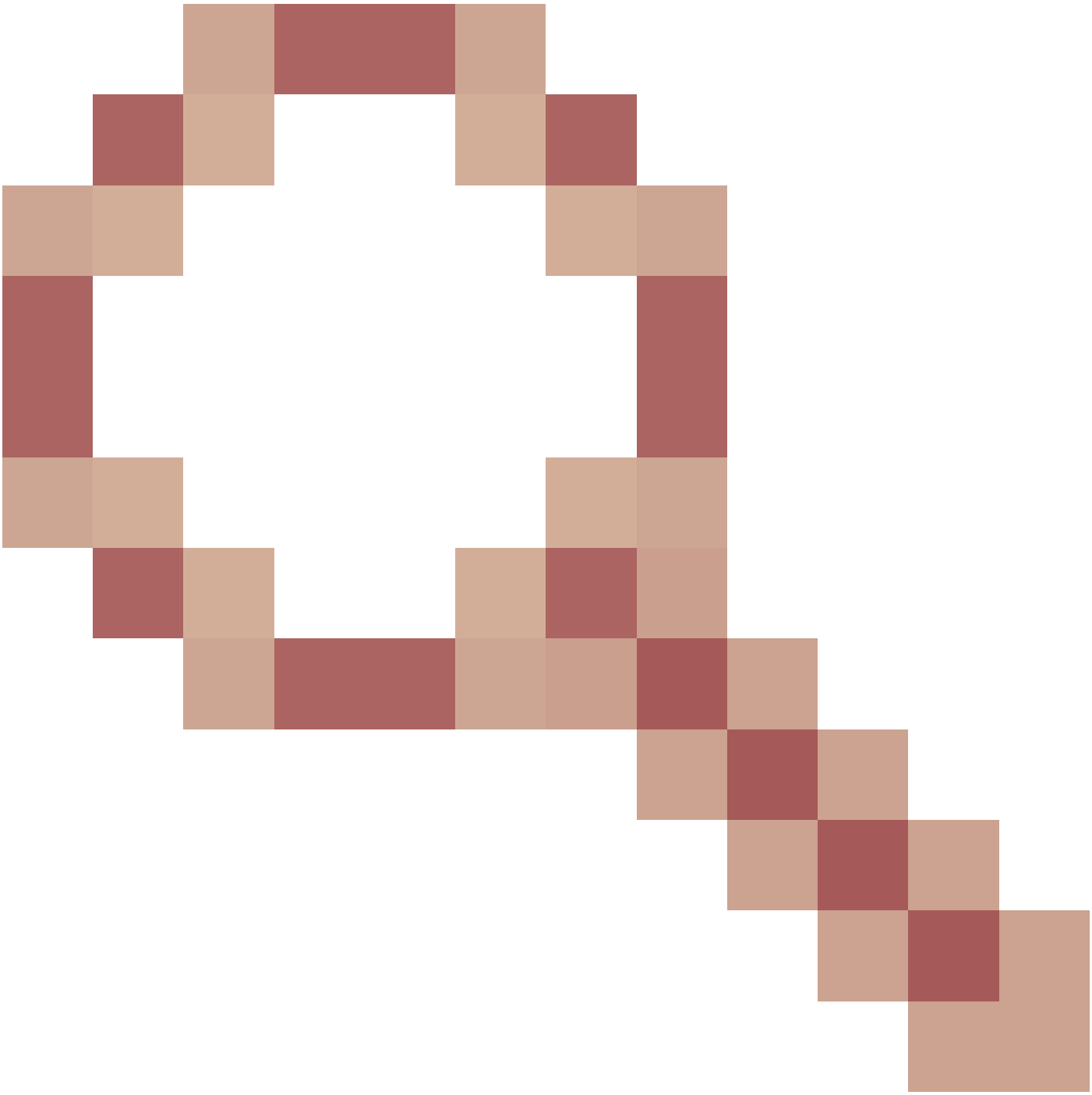
問題9. ASDM會話未超時

症狀是未考慮ASDM GUI會話超時。

疑難排解 — 建議步驟

當在託管ASA上未設定aaa authentication http console LOCAL命令時，會發生這種情況。

請參閱思科錯誤ID CSCwj70826



ENH:新增警告：設定會話超時，需要「aaa authentication http console LOCAL」

因應措施

在託管ASA上配置命令「aaa authentication http console LOCAL」。

問題10. ASDM LDAP身份驗證失敗

疑難排解 — 建議步驟

步驟 1

確保配置到位，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

步驟 2

檢查LDAP伺服器狀態：

<#root>

asa#

show aaa-server

好方案：

<#root>

Server status:

ACTIVE

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

壞情況：

<#root>

Server status:

FAILED

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

步驟 3

通過暫時禁用LDAP身份驗證，檢查LOCAL身份驗證是否正常工作。

步驟 4

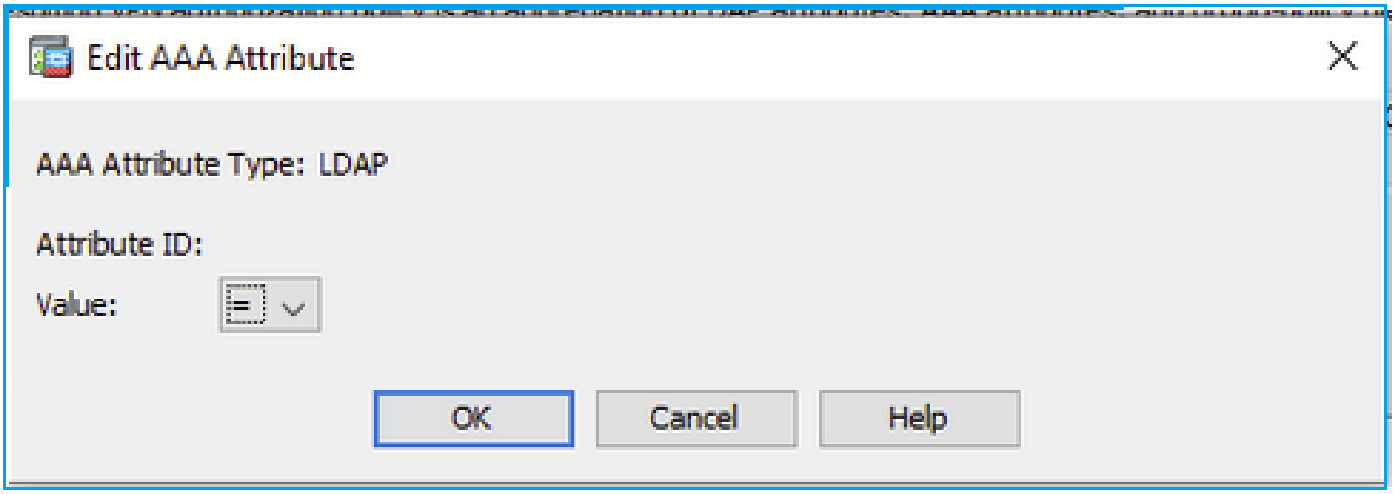
在ASA上運行LDAP調試並嘗試驗證使用者：

```
<#root>
#
debug ldap 255
```

在調試中，查詢包含「失敗」等提示的行。

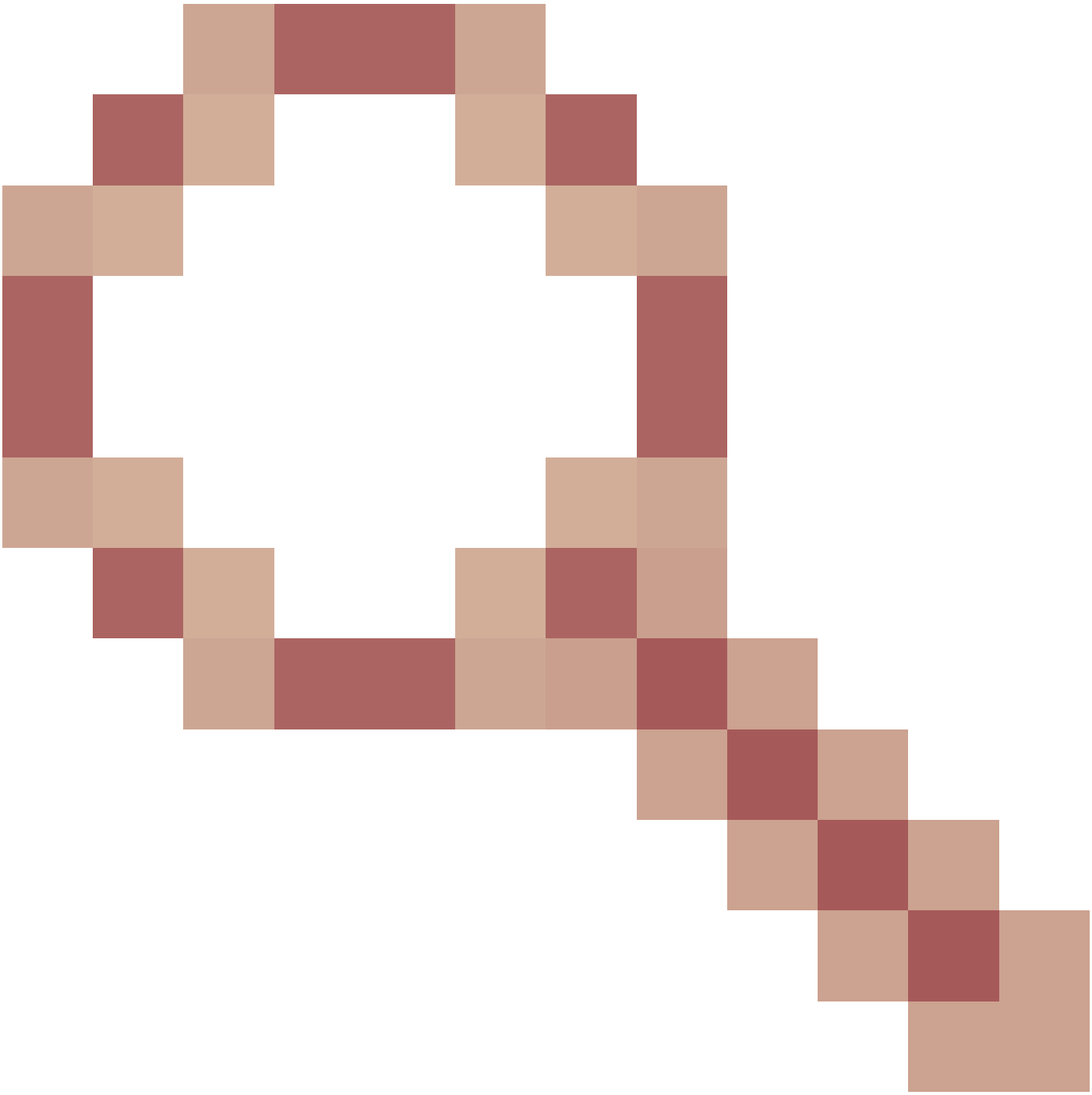
問題11.缺少ASDM Webvpn DAP配置

在ASDM AAA屬性的DAP配置下，型別(Radius/LDAP)不可見，僅檢視=和!= on下拉選單：

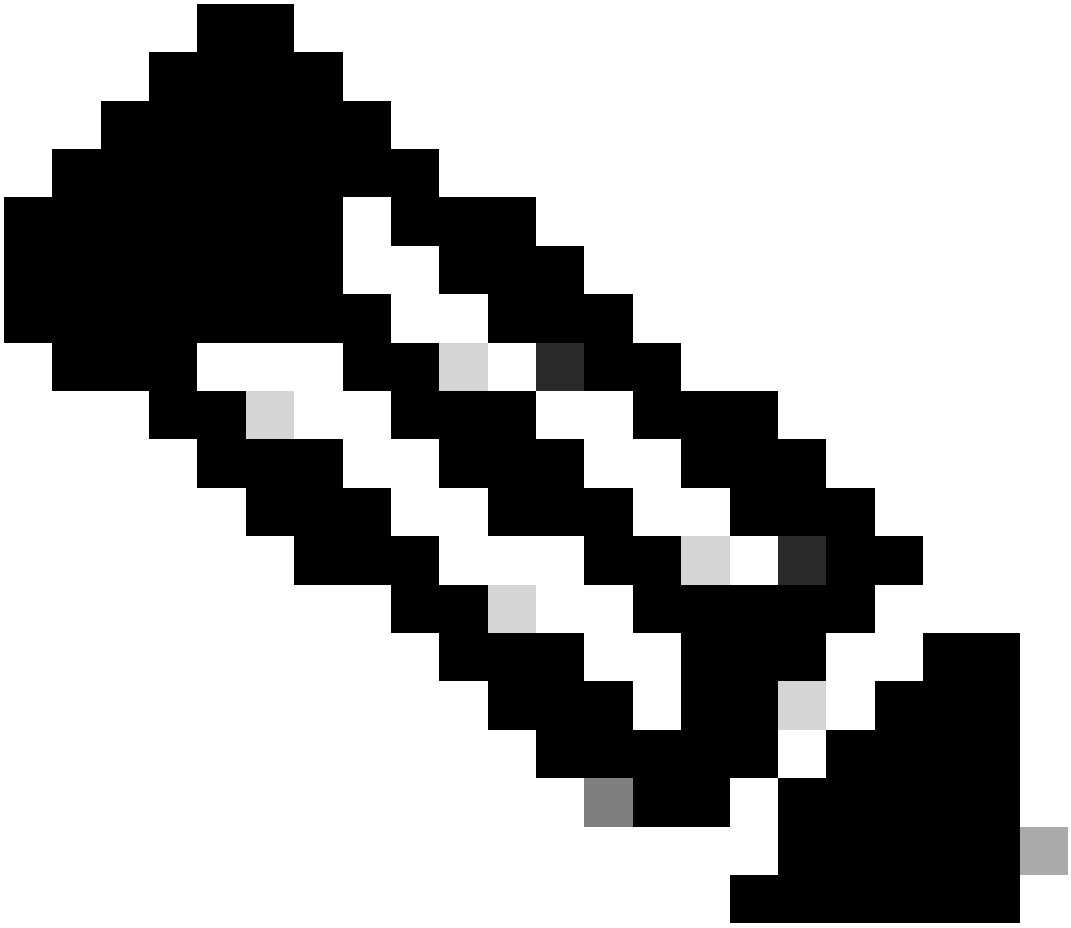


疑難排解 — 建議步驟

這是思科錯誤id CSCwa追蹤到的軟體缺陷99370



ASDM:DAP配置缺少AAA屬性型別(Radius/LDAP)

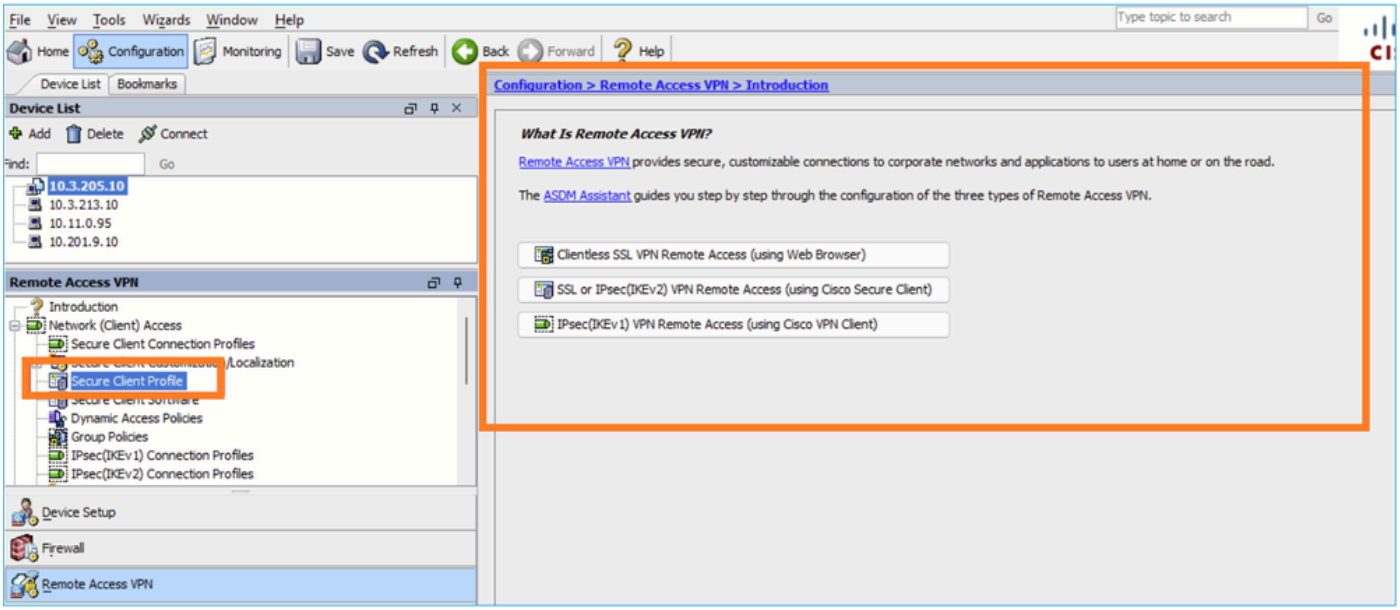


附註：此缺陷已在最近的ASDM軟體版本中修復。有關詳細資訊，請檢視缺陷詳細資訊。

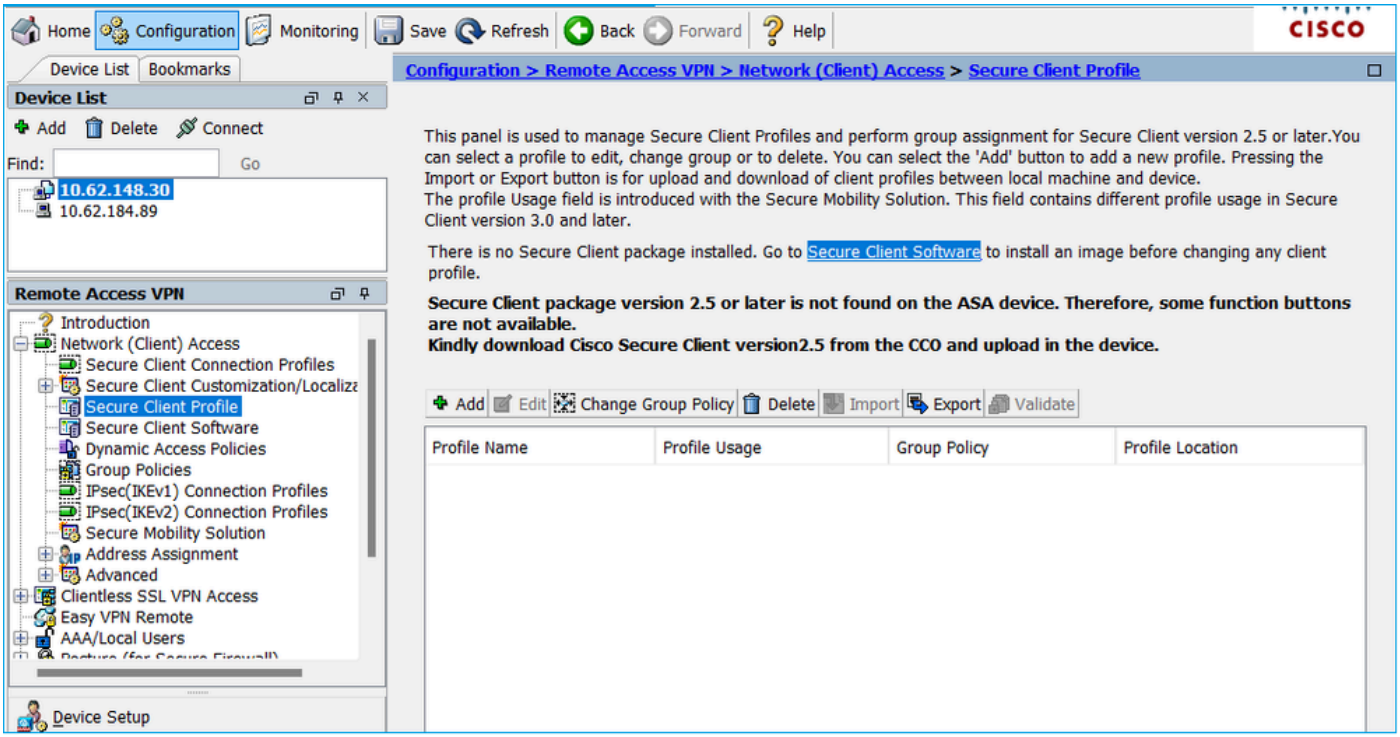
排除ASDM的其他問題

問題1.無法訪問ASDM上的安全客戶端配置檔案

ASDM UI顯示以下內容：



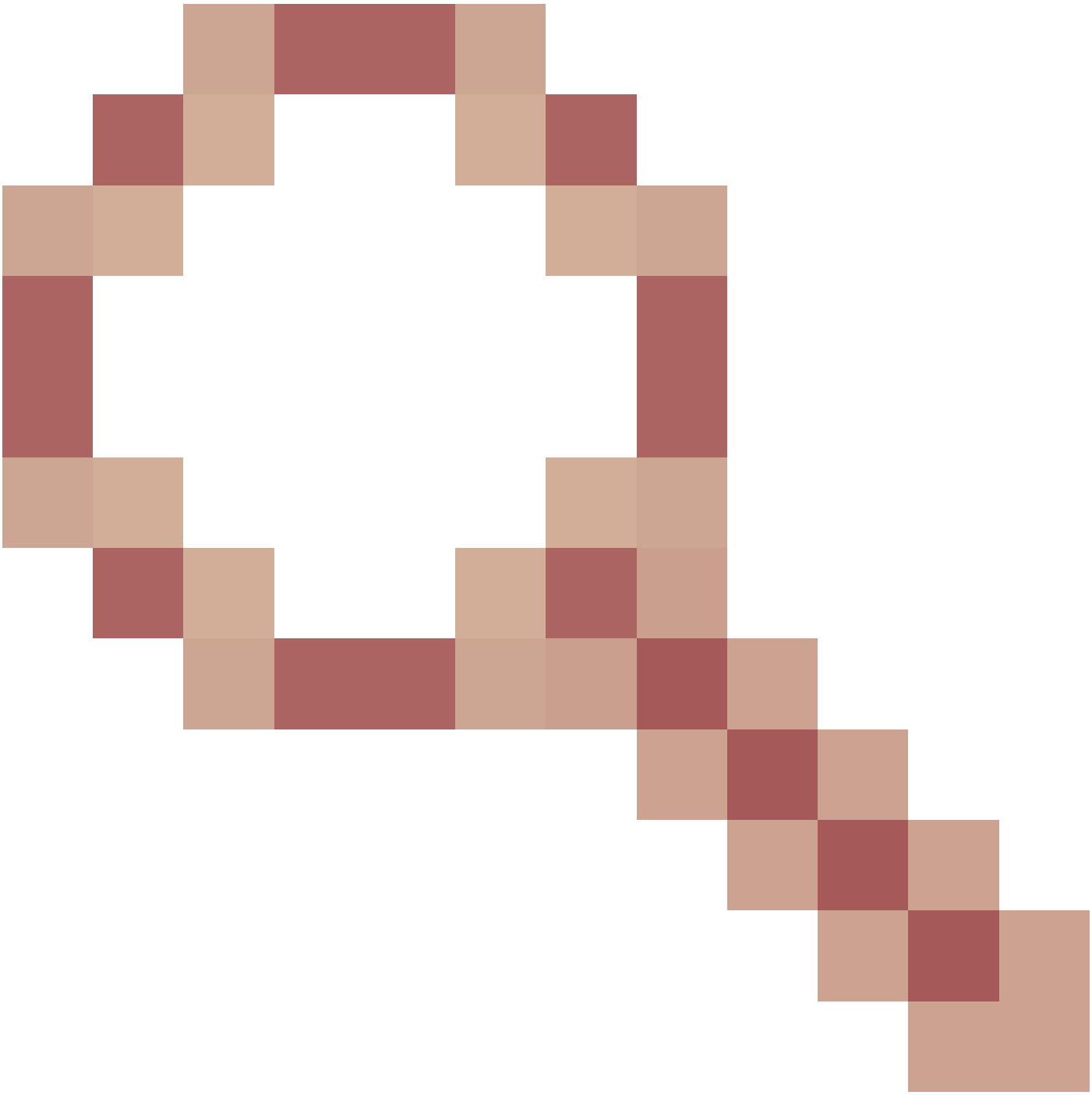
預期的UI輸出為：



疑難排解 — 建議步驟

這是一個已知的缺陷：

思科錯誤ID CSCwi56155



無法訪問ASDM上的安全客戶端配置檔案

因應措施:

降級AnyConnect

或

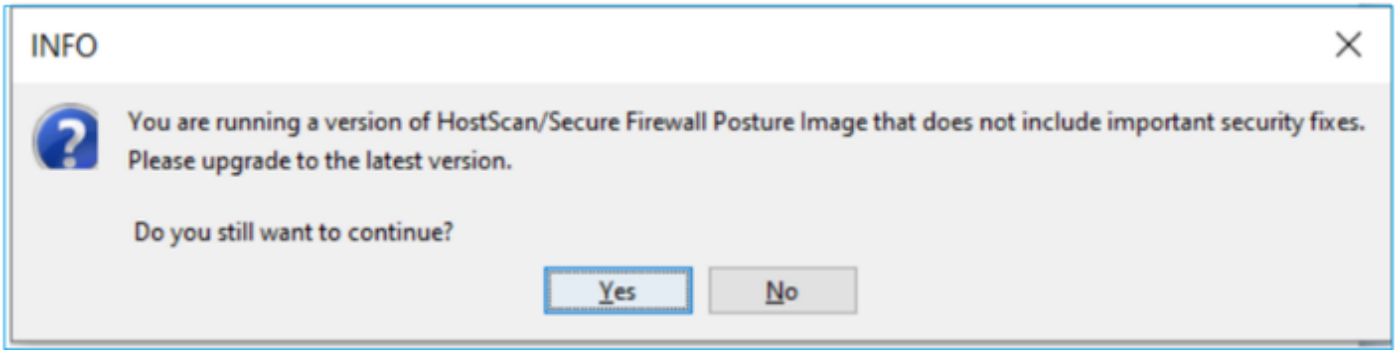
將ASDM升級到7.20.2版

檢視缺陷註釋以瞭解更多詳細資訊。此外，您可以訂購缺陷，因此您將收到有關缺陷更新的通知。

問題2. ASDM顯示hostscan的彈出視窗 — 映像不包括重要的安全修復

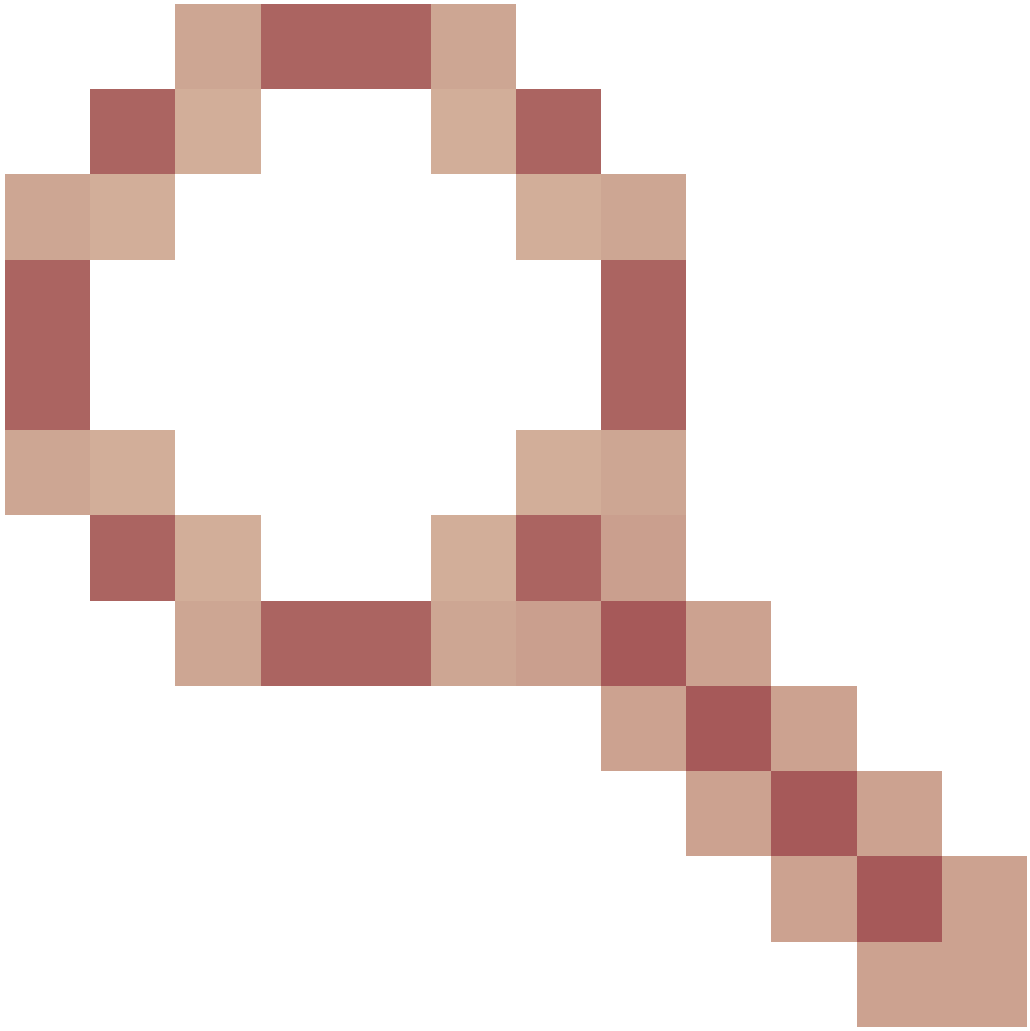
ASDM UI顯示：

「您運行的HostScan/SecureFirewall狀態映像版本不包括重要的安全修復。請升級到最新版本。是否仍要繼續？」

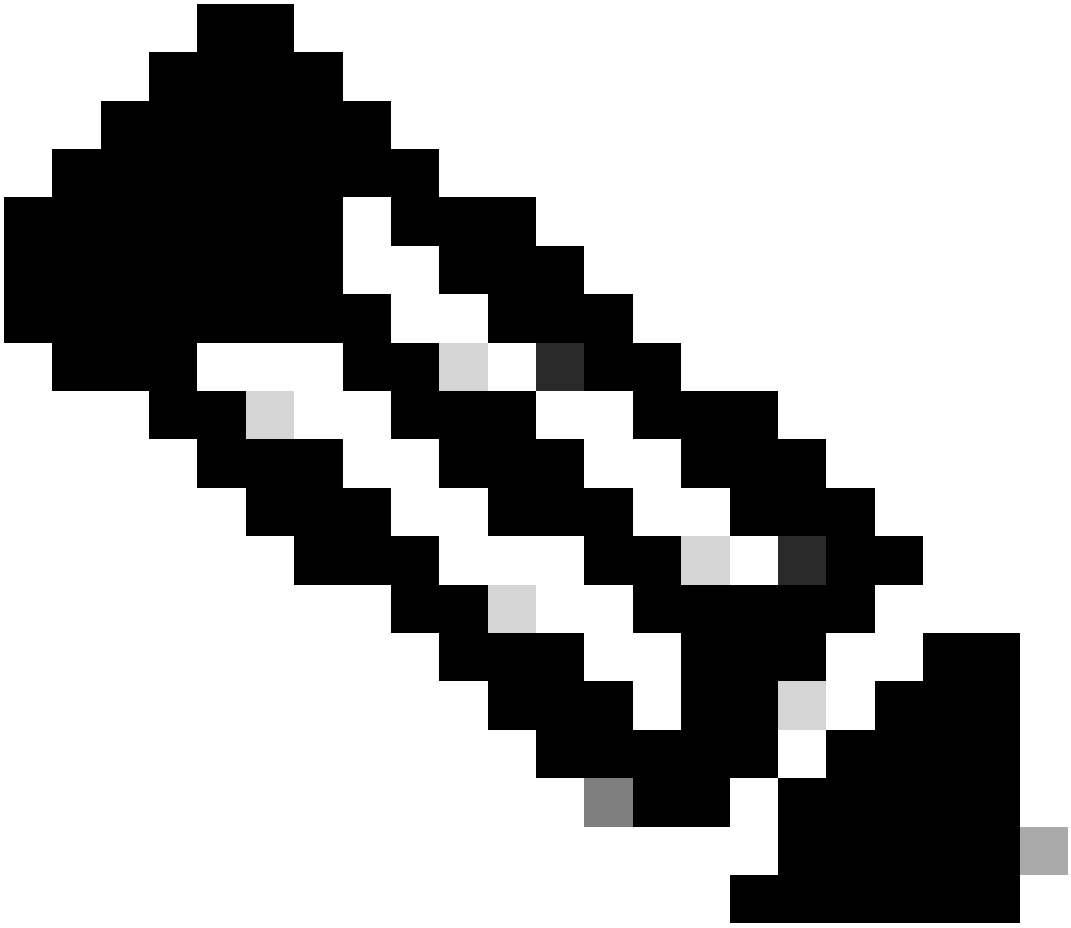


疑難排解 — 建議步驟

這是一個已知的缺陷：



思科錯誤ID CSCwc62461
當登入ASDM彈出以進行hostscan時 — 映像不包含重要的安全修復



附註：此缺陷已在最近的ASDM軟體版本中修復。有關詳細資訊，請檢視缺陷詳細資訊。

因應措施：

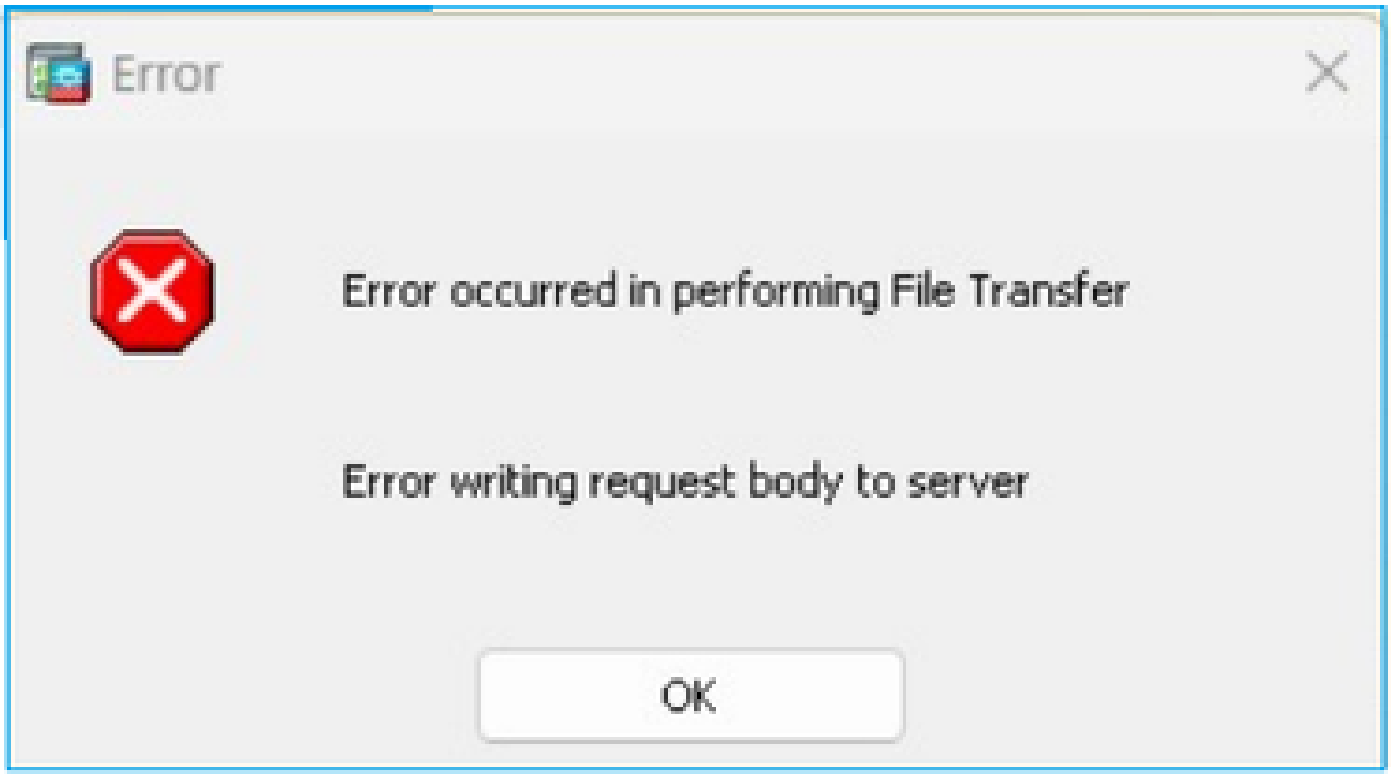
按一下彈出消息框中的「是」繼續。

問題3.通過ASDM複製映像時，ASDM「將請求正文寫入伺服器時出錯」

ASDM UI顯示：

執行檔案傳輸時出錯

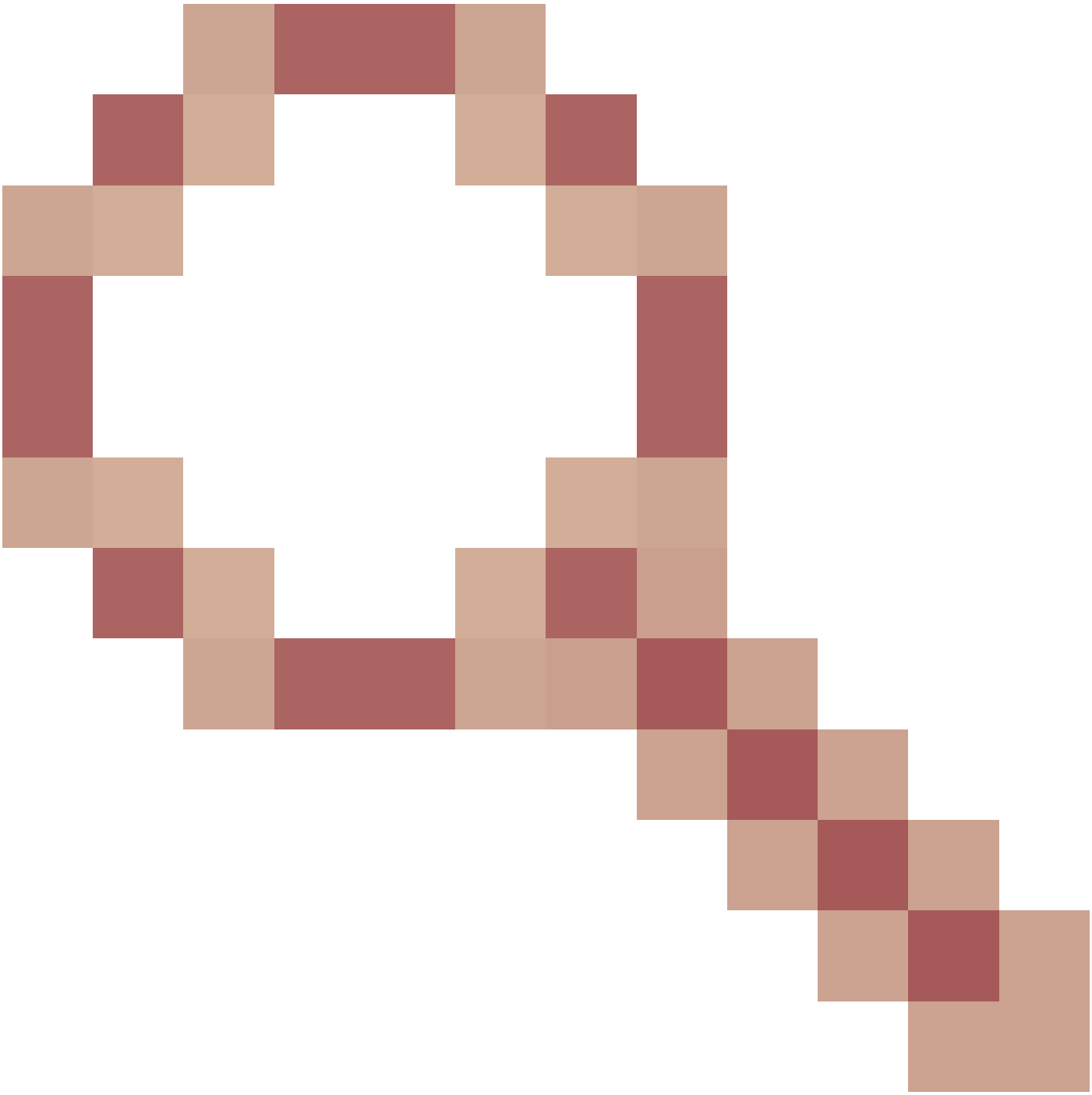
將請求正文寫入伺服器時出錯



疑難排解 — 建議動作

這是一個已知的缺陷，跟蹤者：

思科錯誤ID CSCtf74236



複製映像時ASDM「向伺服器寫入請求正文時出錯」

因應措施

使用SCP/TFTP傳輸檔案。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。