

排除ASDM上的ASA連線問題

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[故障排除方法](#)

[ASA配置](#)

[快閃記憶體中的ASDM映像](#)

[ASDM映像正在使用中](#)

[HTTP伺服器限制](#)

[其他可能的組態問題](#)

[網路連線](#)

[應用程式軟體](#)

[使用HTTPS運行命令](#)

[相關資訊](#)

簡介

本文檔介紹檢查使用Cisco ASDM訪問/配置Cisco ASA時所面臨的問題的必要故障排除方法。

必要條件

需求

在自適應安全裝置(ASA)上設定初始配置後，本文檔中列出的場景、症狀和步驟用於排除故障。有關初始配置，請參閱Cisco ASA系列通用操作自適應安全裝置管理器(ASDM)配置指南7.1中的[為裝置配置ASDM訪問](#)部分。

本文檔使用ASA CLI進行故障排除，需要通過Secure Shell(SSH)/Telnet/控制檯訪問ASA。

採用元件

本文檔中的資訊基於ASA和ASDM。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

ASDM通過圖形管理介面為安全裝置提供安全管理和監控服務。

故障排除方法

本故障排除文檔主要針對三個主要故障點。如果按照此順序遵循常規故障排除流程，本文檔可幫助您確定ASDM使用/訪問的準確問題。

- ASA配置
- 網路連線
- 應用程式軟體

ASA配置

為了成功訪問ASDM，ASA上需要三個基本配置：

- 快閃記憶體中的ASDM映像
- ASDM映像正在使用中
- HTTP伺服器限制

快閃記憶體中的ASDM映像

確保將所需的ASDM版本上傳到快閃記憶體。它可以與當前運行的ASDM版本一起上傳，也可以使用其它常規檔案傳輸方法（如TFTP）上傳到ASA。

在ASA CLI上輸入show flash，以幫助您列出ASA快閃記憶體上存在的檔案。檢查ASDM檔案是否存在：

```
<#root>
ciscoasa#
show flash
--#--  --length--  -----date/time-----  path
249  76267      Feb 28 2013 19:58:18  startup-config.cfg
250  4096        May 12 2013 20:26:12  sdesktop
251  15243264    May 08 2013 21:59:10  asa823-k8.bin
252  25196544    Mar 11 2013 22:43:40  asa845-k8.bin
253  17738924    Mar 28 2013 00:12:12  asdm-702.bin      ---- ASDM Image
```

為了進一步驗證快閃記憶體上存在的映像是否有效且未損壞，可以使用verify命令比較軟體包中儲存的MD5雜湊和實際檔案存在的MD5雜湊：

```
<#root>
ciscoasa#
verify flash:/asdm-702.bin
```

```
Verifying file integrity of disk0:/asdm-702.bin
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
Done!  
Embedded Hash MD5: e441a5723505b8753624243c03a40980  
Computed Hash MD5: e441a5723505b8753624243c03a40980  
CCO Hash MD5: c305760ec1b7f19d910c4ea5fa7d1cf1  
Signature Verified  
Verified disk0:/asdm-702.bin
```

此步驟可幫助您驗證映像是否存在，以及映像是否在ASA上完整。

ASDM映像正在使用中

此過程在ASA上的ASDM配置下定義。使用的當前映像的示例配置定義如下所示：

```
asdm image disk0:/asdm-702.bin
```

若要進一步驗證，您還可以使用show asdm image 指令：

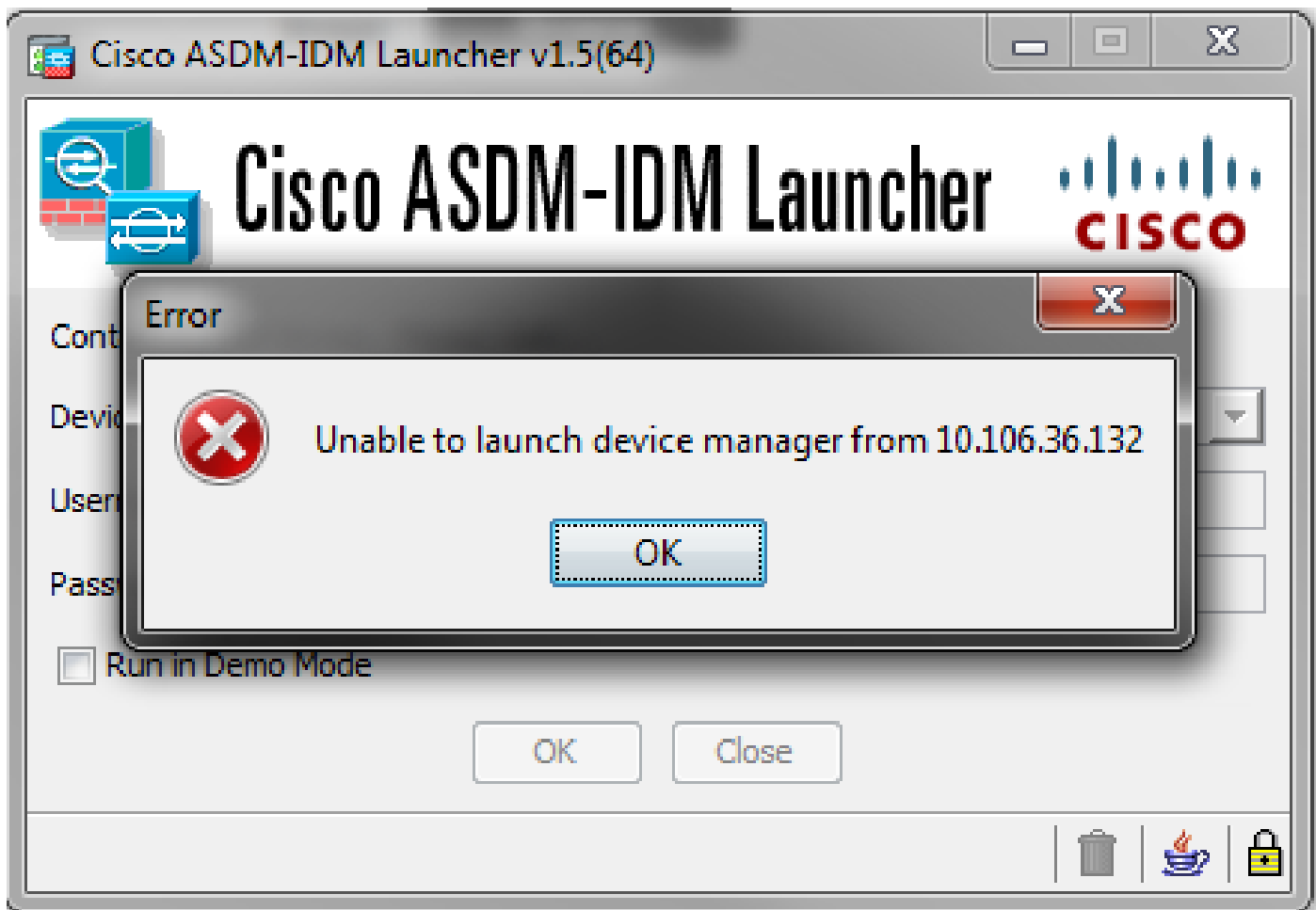
```
<#root>  
ciscoasa# s  
how asdm image  
  
Device Manager image file, disk0:/asdm-702.bin
```

HTTP伺服器限制

此步驟在ASDM配置中至關重要，因為它定義了哪些網路可以訪問ASA。示例配置如下所示：

```
http server enable  
http 192.168.1.0 255.255.255.0 inside  
  
http 10.0.0.1 255.0.0.0 outside
```

確認您具有在先前配置中定義的必要網路。缺少這些定義會導致ASDM啟動器在連線時超時，並產生以下錯誤：



ASDM啟動頁面(<https://<ASA IP地址>/admin>)導致請求超時，並且不顯示頁面。

進一步驗證HTTP伺服器是否使用非標準埠進行ASDM連線，例如8443。以下內容在配置中突出顯示：

```
ciscoasa(config)# show run http  
http server enable 8443
```

如果它使用非標準埠，則當您連線到ASDM啟動器中的ASA時，需要將該埠指定為：

Device IP Address / Name:	10.106.36.132:8443
Username:	cisco
Password:	•••••

當您訪問ASDM啟動頁面時，這也適用：<https://10.106.36.132:8443/admin>

其他可能的組態問題

完成上述步驟後，如果客戶端的所有裝置都正常，ASDM即可開啟。但是，如果仍然遇到問題，請從另一台電腦開啟ASDM。如果成功，則問題可能出在應用程式級別，並且ASA配置正常。但是，如果仍然無法啟動，請完成以下步驟以進一步驗證ASA端配置：

1. 驗證ASA上的安全套接字層(SSL)配置。ASDM在與ASA通訊時使用SSL。根據ASDM的啟動方式，較新的作業系統軟體在協商SSL會話時不允許使用較弱密碼。驗證在ASA上允許哪些密碼，以及配置中是否使用show run all ssl命令指定了任何特定SSL版本：

```
<#root>

ciscoasa#

  show run all ssl

ssl server-version any <--- Check SSL Version restriction configured on the ASA
ssl client-version any
ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1 <--- Check SSL ciphers
permitted on the ASA
```

如果ASDM啟動時出現任何SSL密碼協商錯誤，則這些錯誤將顯示在ASA日誌中：

```
%ASA-7-725014: SSL lib error. Function: SSL3_GET_CLIENT_HELLO Reason:
no shared cipher
%ASA-6-302014: Teardown TCP connection 3 for mgmt:10.103.236.189/52501 to
identity:10.106.36.132/443 duration 0:00:00 bytes 7 TCP Reset by appliance
```

如果您看到特定設定，請將其還原為預設值。請注意，需要在ASA上啟用VPN-3DES-AES許可證，以使ASA在配置中使用3DES和AES密碼。這可透過CLI上的show version指令驗證。輸出顯示如下：

```
<#root>


ciscoasa#

show version

Hardware: ASA5510, 256 MB RAM, CPU Pentium 4 Celeron 1600 MHz
Internal ATA Compact Flash, 64MB
Slot 1: ATA Compact Flash, 32MB
BIOS Flash M50FW080 @ 0xffe00000, 1024KB
<snip>
Failover           : Active/Active
VPN-DES            : Enabled
VPN-3DES-AES      : Enabled
<snip>
```

VPN-3DES-AES許可證可以從思科許可網站免費獲取，[無需付費](#)。按一下Security

Products，然後選擇Cisco ASA 3DES/AES License。

 註：在隨附8.6/9.x代碼的新ASA 5500-X平台中，SSL密碼設定預設設定為des-sha1，這導致ASDM會話無法工作。有關詳細資訊，請參閱[ASA 5500-x:ASDM和其他SSL功能無法開箱即用的文章](#)。

2. 驗證ASA上是否已啟用WebVPN。如果啟用，則需使用此URL(<https://10.106.36.132/admin>)才能在訪問ASDM Web啟動頁面時訪問它。
3. 在ASA上檢查埠443的網路地址轉換(NAT)配置。這會導致ASA不處理ASDM請求，而是將其傳送到已為其配置NAT的網路/介面。
4. 如果所有內容都經過驗證且ASDM仍然超時，請通過ASA CLI上的show asp table socket命令驗證ASA是否設定為偵聽為ASDM定義的埠。輸出可以顯示ASA在ASDM埠上偵聽：

Protocol	Socket	Local Address	Foreign Address	State
SSL	0001b91f	10.106.36.132:443	0.0.0.0:*	LISTEN

如果此輸出未顯示，請刪除並重新應用ASA上的HTTP伺服器配置，以便重置ASA軟體上的套接字。

5. 如果在登入/驗證ASDM時遇到問題，請驗證HTTP的身份驗證選項是否設定正確。如果未設定身份驗證命令，您可以使用ASA啟用密碼登入到ASDM。如果要啟用基於使用者名稱/密碼的身份驗證，需要輸入此配置以從ASA的使用者名稱/密碼資料庫對ASA的ASDM/HTTP會話進行身份驗證：

```
<#root>
```

```
aaa authentication http console LOCAL
```

請記得在啟用前面的命令時建立使用者名稱/密碼：

```
username <username> password <password> priv <Priv level>
```

如果上述步驟均無幫助，則在ASA上可以使用以下調試選項進行進一步調查：

```
debug http 255  
debug asdm history 255
```

網路連線

如果您已完成上一部分，但仍無法訪問ASDM，則下一步是驗證從要訪問ASDM的電腦到ASA的網路連線。以下幾個基本故障排除步驟用於驗證ASA是否收到來自客戶端電腦的請求：

1. 使用網際網路控制訊息通訊協定(ICMP)進行測試。
Ping要從中訪問ASDM的ASA介面。如果允許ICMP在網路中傳輸，並且ASA介面級別沒有限

制，ping操作可以成功。如果ping失敗，可能是因為在ASA和客戶端電腦之間存在通訊問題。但是，這不是確定是否存在這種通訊問題一個結論性步驟。

2. 確認資料包捕獲。

在要訪問ASDM的介面上放置資料包捕獲。捕獲可以顯示，目的地為介面IP地址的TCP資料包到達的目的埠號為443（預設）。

要配置捕獲，請使用以下命令：

```
<#root>
```

```
capture asdm_test interface
```

```
match tcp host
```

```
eq 443 host
```

For example, cap asdm_test interface mgmt match tcp host 10.106.36.132
eq 443 host 10.106.36.13

該命令會捕獲從其中連線到ASDM的ASA介面上的埠443的所有TCP流量。此時通過ASDM連線或開啟ASDM網路啟動頁面。然後使用show capture asdm_test命令檢視捕獲的資料包的結果：

```
<#root>
```

```
ciscoasa#
```

```
show capture asdm_test
```

Three packets captured

```
1: 21:38:11.658855 10.106.36.13.54604 > 10.106.36.132.443:
  S 807913260:807913260(0) win 8192 <mss 1260,nop,wscale 2,nop,nop,sackOK>

2: 21:38:14.659252 10.106.36.13.54604 > 10.106.36.132.443:
  S 807913260:807913260(0) win 8192 <mss 1260,nop,wscale 2,nop,nop,sackOK>

3: 21:38:20.662166 10.106.36.13.54604 > 10.106.36.132.443:
  S 807913260:807913260(0) win 8192 <mss 1260,nop,nop,sackOK>
```

此捕獲顯示從客戶端電腦到ASA的同步(SYN)請求，但ASA未傳送響應。如果您看到與上一個捕獲類似的捕獲，則意味著資料包到達ASA，但ASA不響應這些請求，這將隔離問題至ASA本身。請參閱本檔案的第一節，以進一步進行疑難排解。

但是，如果您沒有看到與前面類似的輸出，並且沒有捕獲任何資料包，則這意味著ASA和ASDM客戶端電腦之間存在連線問題。確認沒有中間裝置可以阻止TCP埠443流量，並且沒有瀏覽器設定（如代理設定）可以阻止流量到達ASA。

通常，資料包捕獲是確定通往ASA的路徑是否清晰，以及是否需要進一步診斷以排除網路連線問題的好方法。

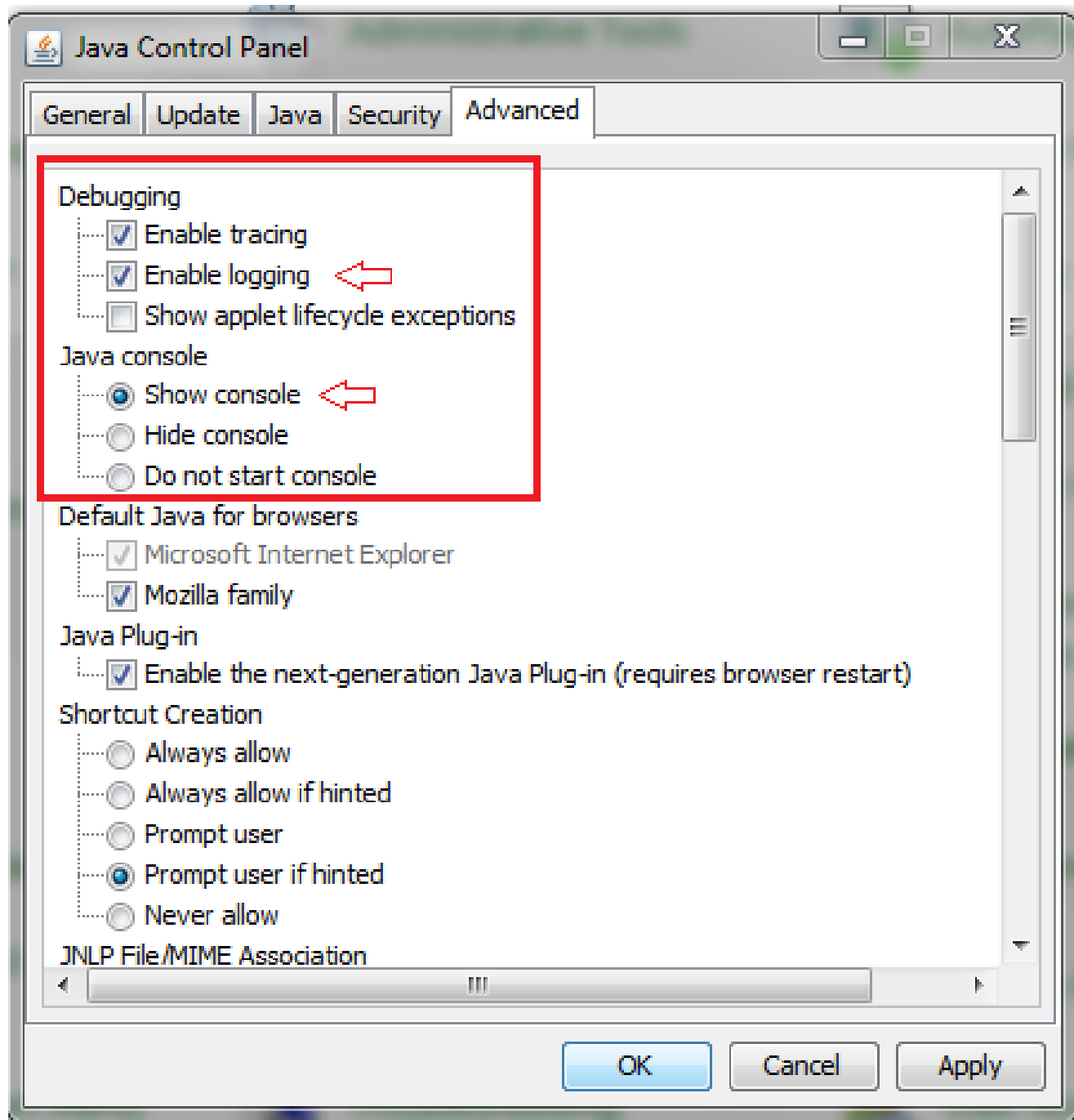
應用程式軟體

本節介紹當客戶端電腦上安裝的ASDM啟動程式軟體無法啟動/載入時，如何對其進行故障排除。ASDM啟動程式是駐留在客戶機上並連線到ASA以檢索ASDM映像的元件。檢索後，ASDM映像通常儲存在快取中，並從快取中獲取，直到ASA端發現任何更改（例如ASDM映像更新）。

完成以下基本故障排除步驟，以排除客戶端電腦上的任何問題：

1. 從其他電腦開啟ASDM啟動頁面。如果啟動，則表示問題出在客戶端電腦上。如果發生故障，請使用故障排除指南從頭開始按順序隔離相關元件。
2. 通過Web啟動開啟ASDM，然後從那裡直接啟動軟體。如果成功，則很可能存在ASDM啟動程式安裝問題。從客戶端電腦上解除安裝ASDM啟動程式，然後從ASA Web啟動本身重新安裝它。
3. 清除使用者主目錄中的ASDM快取目錄。刪除整個快取目錄時，快取將被清除。如果ASDM成功啟動，您還可以從ASDM File選單中清除快取。
4. 驗證是否安裝了正確的Java版本。[Cisco ASDM發行說明](#)列出了已測試Java版本的要求。
5. 清除Java快取。在「Java Control Panel」中，選擇「General > Temporary Internet File」。然後，按一下檢視以啟動Java Cache Viewer。刪除所有引用或與ASDM相關的條目。
6. 如果這些步驟失敗，請從客戶端電腦收集調試資訊以進行進一步調查。使用URL：
`https://<ASA的IP地址>?debug=5`啟用ASDM調試，例如<https://10.0.0.1?debug=5>。

在Java版本6（也稱為1.6版）中，從Java控制面板>高級啟用Java調試消息。然後選擇調試下的覈取方塊。請勿在Java控制台下選擇不啟動控制檯。在ASDM啟動之前，必須啟用Java調試。



Java控制檯輸出記錄在使用者主目錄的.asdm/log目錄中。也可以在同一個目錄中找到ASDM日誌。

使用HTTPS運行命令

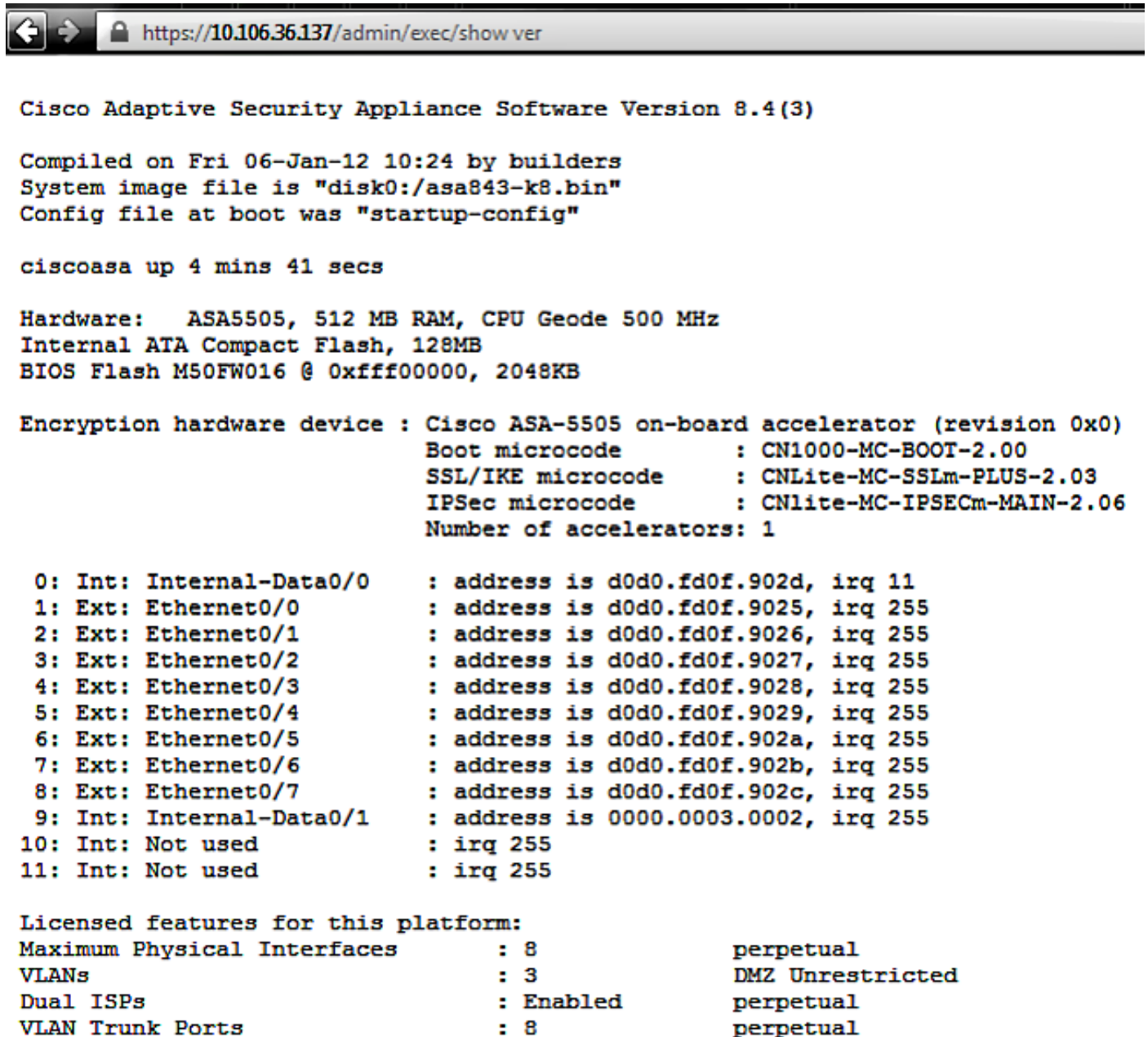
此過程有助於確定HTTP通道的任何第7層問題。當您遇到ASDM應用程式本身不可訪問，並且沒有可用於管理裝置的CLI訪問時，此資訊非常有用。

用於訪問ASDM Web啟動頁面的URL也可用於在ASA上運行任何配置級命令。此URL可用於在基本級別對ASA進行配置更改，包括遠端裝置重新載入。若要輸入命令，請使用以下語法：

```
https://<ASA的IP地址>/admin/exec/<command>
```

如果命令中有空格，並且瀏覽器無法分析URL中的空格字元，則可以使用+或%20來指示空格。

例如，[https://10.106.36.137/admin/exec/show ver](https://10.106.36.137/admin/exec/show%20ver)會產生到瀏覽器的show version輸出：



```
Cisco Adaptive Security Appliance Software Version 8.4(3)

Compiled on Fri 06-Jan-12 10:24 by builders
System image file is "disk0:/asa843-k8.bin"
Config file at boot was "startup-config"

ciscoasa up 4 mins 41 secs

Hardware:   ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 128MB
BIOS Flash M50FW016 @ 0xffff00000, 2048KB

Encryption hardware device : Cisco ASA-5505 on-board accelerator (revision 0x0)
                          Boot microcode       : CN1000-MC-BOOT-2.00
                          SSL/IKE microcode    : CNLite-MC-SSLm-PLUS-2.03
                          IPSec microcode      : CNlite-MC-IPSECm-MAIN-2.06
                          Number of accelerators: 1

0: Int: Internal-Data0/0   : address is d0d0.fd0f.902d, irq 11
1: Ext: Ethernet0/0       : address is d0d0.fd0f.9025, irq 255
2: Ext: Ethernet0/1       : address is d0d0.fd0f.9026, irq 255
3: Ext: Ethernet0/2       : address is d0d0.fd0f.9027, irq 255
4: Ext: Ethernet0/3       : address is d0d0.fd0f.9028, irq 255
5: Ext: Ethernet0/4       : address is d0d0.fd0f.9029, irq 255
6: Ext: Ethernet0/5       : address is d0d0.fd0f.902a, irq 255
7: Ext: Ethernet0/6       : address is d0d0.fd0f.902b, irq 255
8: Ext: Ethernet0/7       : address is d0d0.fd0f.902c, irq 255
9: Int: Internal-Data0/1   : address is 0000.0003.0002, irq 255
10: Int: Not used         : irq 255
11: Int: Not used         : irq 255

Licensed features for this platform:
Maximum Physical Interfaces   : 8           perpetual
VLANs                         : 3           DMZ Unrestricted
Dual ISPs                     : Enabled      perpetual
VLAN Trunk Ports              : 8           perpetual
```

此命令執行方法要求在ASA上啟用HTTP伺服器並且啟用必要的HTTP限制。但是，這不需要在ASA上存在ASDM映像。

相關資訊

- [為裝置配置ASDM訪問](#)
- [ASA 5500-x:ASDM和其他SSL功能無法開箱使用](#)

- [Cisco ASDM版本說明](#)
- [在ASA上獲取3DES/AES許可證的思科許可證頁面](#)
- [技術支援與文件 - Cisco Systems](#)

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）。