

ASDMでのASA接続問題のトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[トラブルシューティング手法](#)

[ASA の設定](#)

[フラッシュ内の ASDM イメージ](#)

[使用中の ASDM イメージ](#)

[HTTP サーバの制約](#)

[その他の考えられる設定上の問題](#)

[ネットワーク接続](#)

[アプリケーションソフトウェア](#)

[HTTPS でコマンドを実行する](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco ASDMを使用してCisco ASAにアクセス/設定する際に直面する問題を確認するために必要なトラブルシューティングの方法について説明します。

前提条件

要件

このドキュメントに記載されているシナリオ、症状、および手順は、Adaptive Security Appliance (ASA ; 適応型セキュリティアプライアンス) で初期設定を行った後の問題のトラブルシューティングのために記述されています。初期設定については、『Cisco ASAシリーズ Adaptive Security Device Manager(ASDM)コンフィギュレーションガイド、7.1』の「[アプライアンス用のASDMアクセスの設定](#)」セクションを参照してください。

このドキュメントでは、ASA への Secure Shell (SSH) /Telnet/コンソール アクセスを必要とする ASA CLI をトラブルシューティングに使用します。

使用するコンポーネント

このドキュメントの情報は、ASAおよびASDMに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

ASDM は、グラフィカル管理インターフェイスを介してセキュリティ アプライアンスのセキュリティ管理およびモニタリング サービスを提供します。

トラブルシューティング手法

このトラブルシューティング ドキュメントでは、3 つの主な障害ポイントを取り上げます。この順序で一般的なトラブルシューティングプロセスに従う場合、このドキュメントは ASDM の使用 / アクセスに関する正確な問題を判別するのに役立ちます。

- ASA の設定
- ネットワーク接続
- アプリケーション ソフトウェア

ASA の設定

ASA には、ASDM に正常にアクセスするために必要な 3 つの基本設定があります。

- フラッシュ内の ASDM イメージ
- 使用中の ASDM イメージ
- HTTP サーバの制約

フラッシュ内の ASDM イメージ

ASDM の必要なバージョンがフラッシュにアップロードされていることを確認します。これは、ASDM の現在実行されているバージョンまたはその他の従来のファイル転送方法 (TFTP など) を使って ASA にアップロードできます。

ASA CLI で show flash と入力すると、ASA のフラッシュ メモリに存在するファイルを表示できます。ASDM ファイルが存在することを確認します。

```
<#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
```

さらに、フラッシュに存在するイメージが有効で破損していないことを検証するには、verify コマンドを使用して、ソフトウェア パッケージに保存された MD5 ハッシュと実際に存在するファイルの MD5 ハッシュを比較します。

```
<#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
```

この手順は、ASAにイメージが存在するかどうか、およびイメージの整合性を確認するのに役立ちます。

使用中の ASDM イメージ

このプロセスは、ASA の ASDM 設定で定義されます。使用されている現在イメージの設定例の定義は次のとおりです。

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

さらに検証するため、show asdm image コマンドを使用することもできます。

```
<#root>
```

```
ciscoasa# s
```

```
how asdm image
```

```
Device Manager image file, disk0:/asdm-702.bin
```

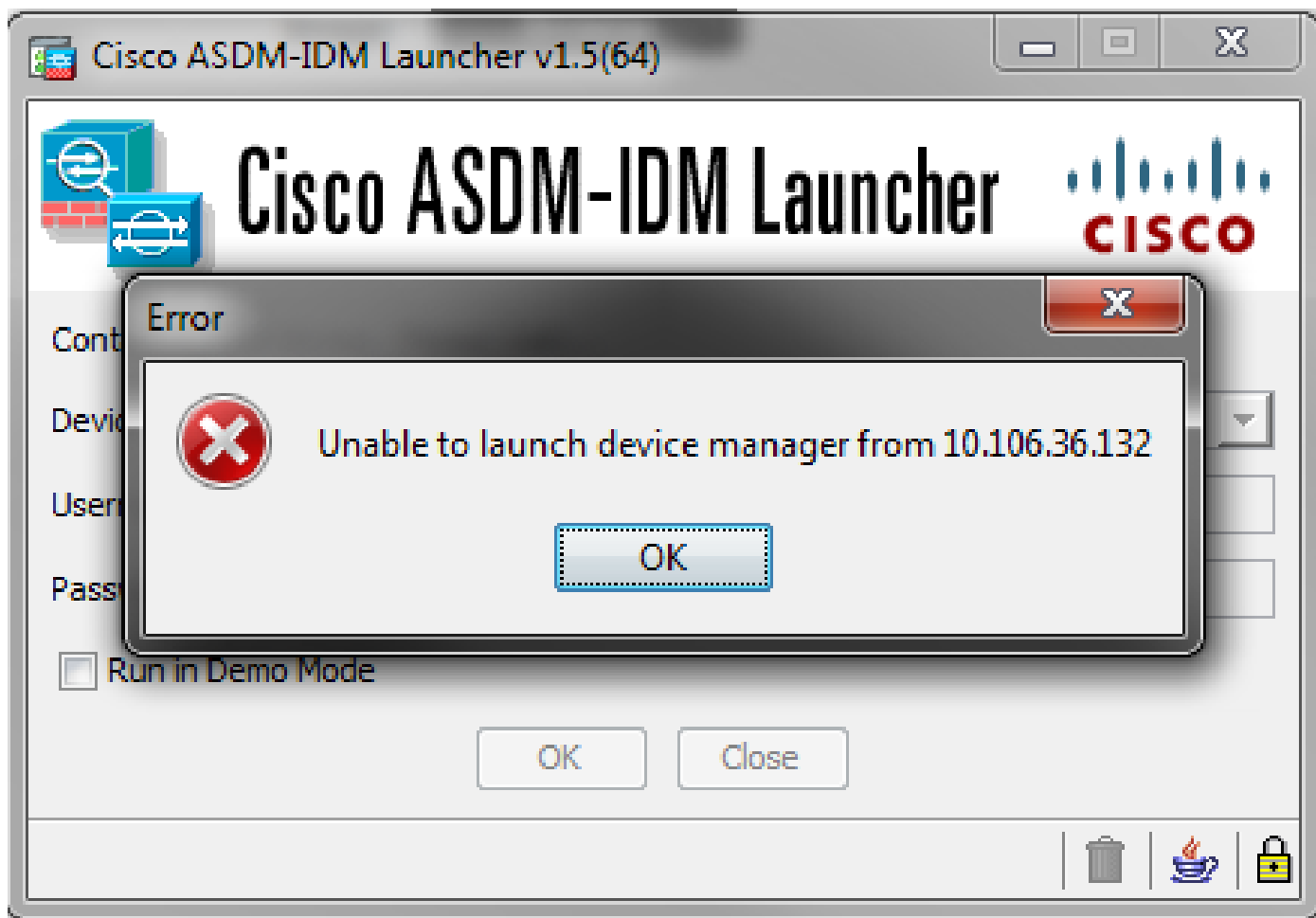
HTTP サーバの制約

この手順は、ASAにアクセスできるネットワークを定義するため、ASDM設定に不可欠です。設定例は次のとおりです。

```
http server enable
http 192.168.1.0 255.255.255.0 inside

http 10.0.0.1 255.0.0.0 outside
```

以前の設定に必要なネットワークが定義されていることを検証します。これらが定義されていない場合は、ASDM Launcher の接続中にタイムアウトし、次のエラーが発生します。



ASDM の起動ページ (<https://<ASAのIPアドレス>/admin>) で要求がタイムアウトし、ページが表示されません。

さらに、HTTP サーバが ASDM の接続に標準以外のポート (8443 など) を使用していることを検証します。これを設定内で強調表示します。

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

標準以外のポートが使用されている場合は、ASDM launcher で ASA に接続するときのポートを次のように指定する必要があります。

Device IP Address / Name: 10.106.36.132:8443

Username: cisco

Password: [masked]

これは、ASDM起動ページにアクセスする場合にも適用されます。

<https://10.106.36.132:8443/admin>

その他の考えられる設定上の問題

上記の手順を完了した後、クライアント側ですべてが機能していれば、ASDMを開くことができます。しかし、引き続き問題が発生する場合は、別のマシンから ASDM を開きます。成功した場合、問題はおそらくアプリケーションレベルであり、ASA の設定に問題はありません。しかし、それでも起動できない場合は、次の手順を実行して、ASA 側の設定をさらに検証します。

1. ASA の Secure Sockets Layer (SSL) 設定を検証します。ASDM は、ASA との通信中に SSL を使用します。ASDMの起動方法に基づいて、新しいOSソフトウェアではSSLセッションのネゴシエーション時に弱い暗号の使用を許可できません。 show run all ssl コマンドを使用して、ASA でどの暗号を使用できるか、および設定に特定の SSL バージョンが指定されているかどうかを検証します。

```
<#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
```

ASDM の起動中に SSL 暗号ネゴシエーションのエラーが発生する場合は、ASA のログに表示されます。

```
%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
```

特別な設定が見つかった場合は、それらをデフォルトに戻します。設定内で ASA が 3DES および AES 暗号を使用できるようにするには、ASA で VPN-3DES-AES ライセンスを有効にする必要があります。これは、CLI の show version コマンドを使用して検証できます。次のような出力が表示されます。


```
<#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 ライセンスは、[シスコのライセンス Web サイト](#)から無料で入手できます。[Security Products] をクリックし、[Cisco ASA 3DES/AES License] を選択します。

 注:8.6/9.xコードが付属する新しいASA 5500-Xプラットフォームでは、SSL暗号設定がデフォルトでdes-sha1に設定されるため、ASDMセッションが機能しません。詳細については、「[ASA 5500-x:ASDMおよびその他のSSL機能が出荷直後の状態で動作しない](#)」の記事を参照してください。

2. WebVPN が ASA で有効になっていることを検証します。有効になっている場合は、ASDM の Web 起動ページにアクセスするときに、この URL (<https://10.106.36.132/admin>) を使用してアクセスする必要があります。
3. ASA のポート 443 のネットワーク アドレス変換 (NAT) 設定を確認します。これによって、ASA は ASDM の要求を処理せずに、NAT が設定されたネットワーク/インターフェイスに送信します。
4. すべてを検証しても ASDM がまだタイムアウトする場合は、ASA CLI で show asp table socket コマンドを使用して、ASDM 用に定義されたポートでリッスンするように ASA が設定されていることを検証します。出力に、ASAがASDMポートでリッスンしていることが示される場合があります。

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

この出力が表示されない場合は、ASA の HTTP サーバ設定を削除してから再度適用し、ASA ソフトウェアのソケットをリセットします。

5. ASDM へのログイン/認証時に問題が発生する場合は、HTTP の認証オプションが正しく設定されていることを検証します。認証コマンドが設定されていない場合は、ASA のイネー

ブル パスワードを使用して ASDM にログインできます。ユーザ名/パスワードベースの認証を有効にするには、次の設定を入力して、ASAのユーザ名/パスワードデータベースからASAへのASDM/HTTPセッションを認証する必要があります。

```
<#root>
```

```
aaa authentication http console LOCAL
```

上記のコマンドを有効にするときは、必ずユーザ名/パスワードを作成してください。

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

これらの手順がいずれも有効でない場合は、ASA で次のデバッグ オプションを使用して詳しい調査を行うことができます。

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

ネットワーク接続

前の項を完了しても、依然として ASDM にアクセスできない場合は、次のステップとして、ASDM へのアクセスに使用するマシンから ASA へのネットワークの接続性を検証します。ASA がクライアント マシンから要求を受信していることを検証するには、いくつかの基本的なトラブルシューティング手順があります。

1. Internet Control Message Protocol (ICMP) を使ってテストする。
ASDM へのアクセスに使用する ASA インターフェイスに対して ping を実行します。ICMPがネットワークを通過することを許可され、ASAインターフェイスレベルに制限がない場合、pingは成功する可能性があります。ping が失敗する場合、その原因はおそらく ASA とクライアント マシン間の通信の問題にあります。ただし、これはそのタイプの通信の問題があることを確認する最終的な手順ではありません。
2. パケット キャプチャを使って確認する。
ASDM へのアクセスに使用するインターフェイスにパケット キャプチャを配置します。キャプチャは、インターフェイスIPアドレス宛てのTCPパケットが宛先ポート番号443 (デフォルト) で到着することを示すことができます。

キャプチャを設定するには、次のコマンドを使用します。

```
<#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`

これで、ASDM に接続する ASA インターフェイスのポート 443 に到着する TCP トラフィックがキャプチャされます。この時点で ASDM を使って接続するか、または ASDM Web 起動ページを開きます。次に、`show capture asdm_test` コマンドを使用して、キャプチャされたパケットの結果を表示します。

```
<#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>

このキャプチャは、クライアント マシンから ASA への同期 (SYN) 要求を示していますが、ASA は応答を送信していません。上記と同じようなキャプチャが表示された場合、パケットは ASA に到着したものの ASA がそれらの要求に応答していないことを示しています。これは問題が ASA 自体に絞り込まれたことを意味します。詳細なトラブルシューティングについては、このドキュメントの最初の項を参照してください。

一方、上記と同じようなキャプチャが表示されず、パケットがキャプチャされていない場合、これは ASA と ASDM クライアント マシンの間に接続の問題があることを意味します。TCPポート 443トラフィックをブロックできる中継デバイスが存在しないこと、およびトラフィックが ASA に到達するのを妨げるブラウザ設定 (プロキシ設定など) が存在しないことを確認します。

通常、パケットキャプチャは、ASA へのパスが明確かどうか、およびネットワーク接続の問題を除外するためにさらなる診断が必要かどうかを判断する優れた方法です。

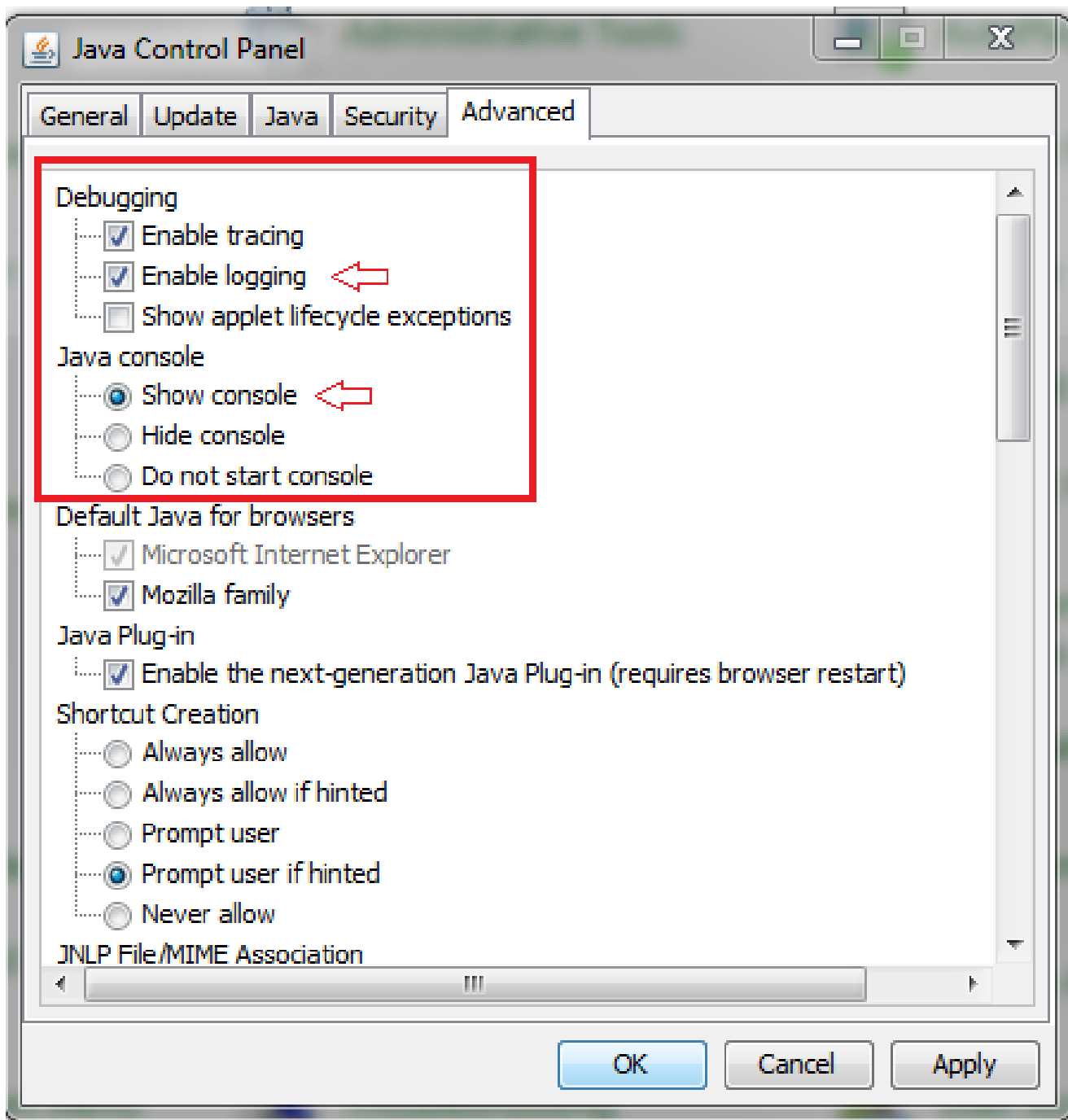
アプリケーション ソフトウェア

ここでは、クライアント マシンにインストールされた ASDM Launcher ソフトウェアを起動/ロードできない場合のトラブルシューティング方法について説明します。ASDM Launcher は、クライアント マシンに存在し、ASA に接続して ASDM イメージを取得するコンポーネントです。取得された ASDM イメージは通常、キャッシュに保存され、ASA 側で変更 (ASDM イメージのアップデートなど) が通知されるまで、そこから取得されます。

クライアント マシン上の問題を排除するには、次の基本的なトラブルシューティング手順を実行します。

1. 別のマシンから ASDM 起動ページを開きます。起動した場合、これは問題となっているクライアント マシンに関連した問題であることを意味します。不合格の場合は、トラブルシューティングガイドを最初から使用して、関係するコンポーネントを順番に切り分けます。
2. Web 起動を使って ASDM を開き、そこからソフトウェアを直接起動します。成功する場合は、ASDM Launcher のインストールに問題がある可能性があります。クライアント マシンから ASDM Launcher をアンインストールし、ASA の Web 起動自体から再インストールします。
3. ユーザのホーム ディレクトリにある ASDM のキャッシュ ディレクトリをクリアします。このキャッシュは、cache ディレクトリ全体を削除するとクリアされます。ASDM が正常に起動する場合は、ASDM の [File] メニューからキャッシュをクリアすることもできます。
4. 適切な Java バージョンがインストールされていることを確認します。『[Cisco ASDM リリースノート](#)』に、[テストされた Java バージョンの要件が記載されています。](#)
5. Java キャッシュをクリアします。[Java Control Panel] で、[General] > [Temporary Internet File] を選択します。次に、[View] をクリックして [Java Cache Viewer] を起動します。ASDM を参照するエントリまたは ASDM に関連するエントリをすべて削除します。
6. これらの手順に失敗した場合は、さらなる調査のためにクライアント マシンからデバッグ情報を収集します。https://<ASAのIPアドレス>?debug=5のURLを使用してASDMのデバッグを有効にします(<https://10.0.0.1?debug=5>など)。Java バージョン 6 (バージョン 1.6 と呼ばれる) で Java のデバッグ メッセージを有効にするには、[Java Control Panel] > [Advanced] を使用します。次に、[Debugging] の下のチ

チェックボックスを選択します。[Java console] の下の [Do not start console] は選択しないでください。ASDM を起動する前に Java のデバッグを有効にする必要があります。



Java コンソールの出力は、ユーザのホーム ディレクトリの `.asdm/log` ディレクトリに記録されます。ASDM ログも同じディレクトリにあります。

HTTPS でコマンドを実行する

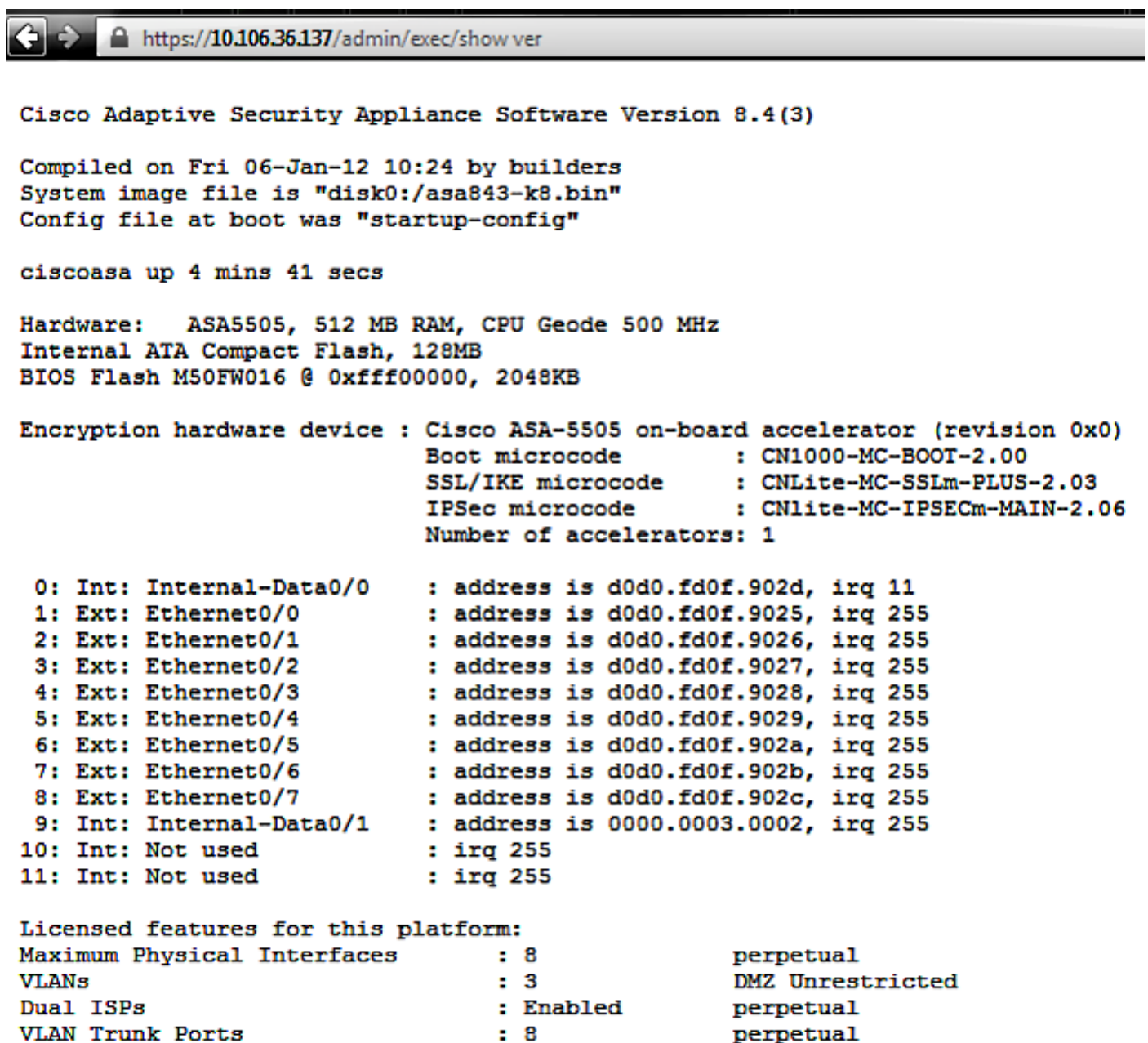
この手順は、HTTP チャンネルのレイヤ 7 に関する問題を特定するのに役立ちます。この情報は、ASDM アプリケーション自体にアクセスできず、デバイスを管理するために CLI アクセスを使用できないような状況で役立ちます。

ASDM Web 起動ページへのアクセスに使用される URL を使用して、ASA のすべての設定レベルのコマンドを実行することもできます。この URL は、リモート デバイスのリロードを含む ASA の基本的なレベルの設定変更を行うために使用できます。コマンドを入力するには、次の構文を使用します。

`https://<ASA の IP アドレス>/admin/exec/<コマンド>`

コマンド内にスペースがあり、ブラウザがURL内のスペース文字を解析できない場合は、+記号または%20を使用してスペースを示すことができます。

たとえば、[https://10.106.36.137/admin/exec/show ver](https://10.106.36.137/admin/exec/show%20ver) と入力すると、ブラウザに `show version` の出力が表示されます。



```
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
```

このコマンド実行方法を使用するには、ASA で HTTP サーバが有効になっており、必要な HTTP の制約がアクティブになっている必要があります。ただし、ASDM イメージは ASA に存在しなくてもかまいません。

関連情報

- [アプライアンス用の ASDM アクセスの設定](#)
- [ASA 5500-x:ASDMおよびその他のSSL機能が出荷直後の状態で動作しない](#)
- [Cisco ASDM リリース ノート](#)
- [ASA の 3DES/AES ライセンスを取得するためのシスコのライセンス ページ](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。