

排除ASDM上的ASA连接问题

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[故障排除方法](#)

[ASA 配置](#)

[闪存中的ASDM映像](#)

[正在使用的ASDM映像](#)

[HTTP服务器限制](#)

[其他可能的配置问题](#)

[网络连接](#)

[应用软件](#)

[使用HTTPS运行命令](#)

[相关信息](#)

简介

本文档介绍检查访问/配置带Cisco ASDM的Cisco ASA时遇到的问题所需的故障排除方法。

先决条件

要求

本文档中列出的场景、症状和步骤用于在自适应安全设备(ASA)上设置初始配置后进行故障排除。有关初始配置，请参阅Cisco ASA系列通用操作自适应安全设备管理器(ASDM)配置指南7.1的[为设备配置ASDM访问](#)部分。

本文档使用ASA CLI进行故障排除，需要通过Secure Shell(SSh)/Telnet/控制台访问ASA。

使用的组件

本文档中的信息基于ASA和ASDM。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

ASDM通过图形管理界面为安全设备提供安全管理和监控服务。

故障排除方法

本故障排除文档重点介绍三个主要故障点。如果遵循此顺序的一般故障排除流程，本文档可帮助您确定ASDM使用/访问的准确问题。

- ASA 配置
- 网络连接
- 应用软件

ASA 配置

ASA上存在三个成功访问ASDM所需的基本配置：

- 闪存中的ASDM映像
- 正在使用的ASDM映像
- HTTP服务器限制

闪存中的ASDM映像

确保所需的ASDM版本已上传到闪存。它可以与当前运行的ASDM版本一起上传，也可以使用其它常规文件传输方法上传到ASA，例如TFTP。

在ASA CLI上输入show flash，以帮助您列出ASA闪存上存在的文件。检查ASDM文件是否存在：

```
<#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
```

为进一步验证闪存上的映像是否有效且未损坏，您可以使用verify命令比较软件包中存储的MD5散列和实际文件的MD5散列：

```
<#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
```

此步骤可帮助您验证映像是否存在，以及映像在ASA上的完整性。

正在使用的ASDM映像

此过程在ASA上的ASDM配置下定义。使用的当前映像的示例配置定义如下所示：

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

为了进一步验证，您还可以使用show asdm image命令：

```
<#root>
```

```
ciscoasa# s
```

```
how asdm image
```

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

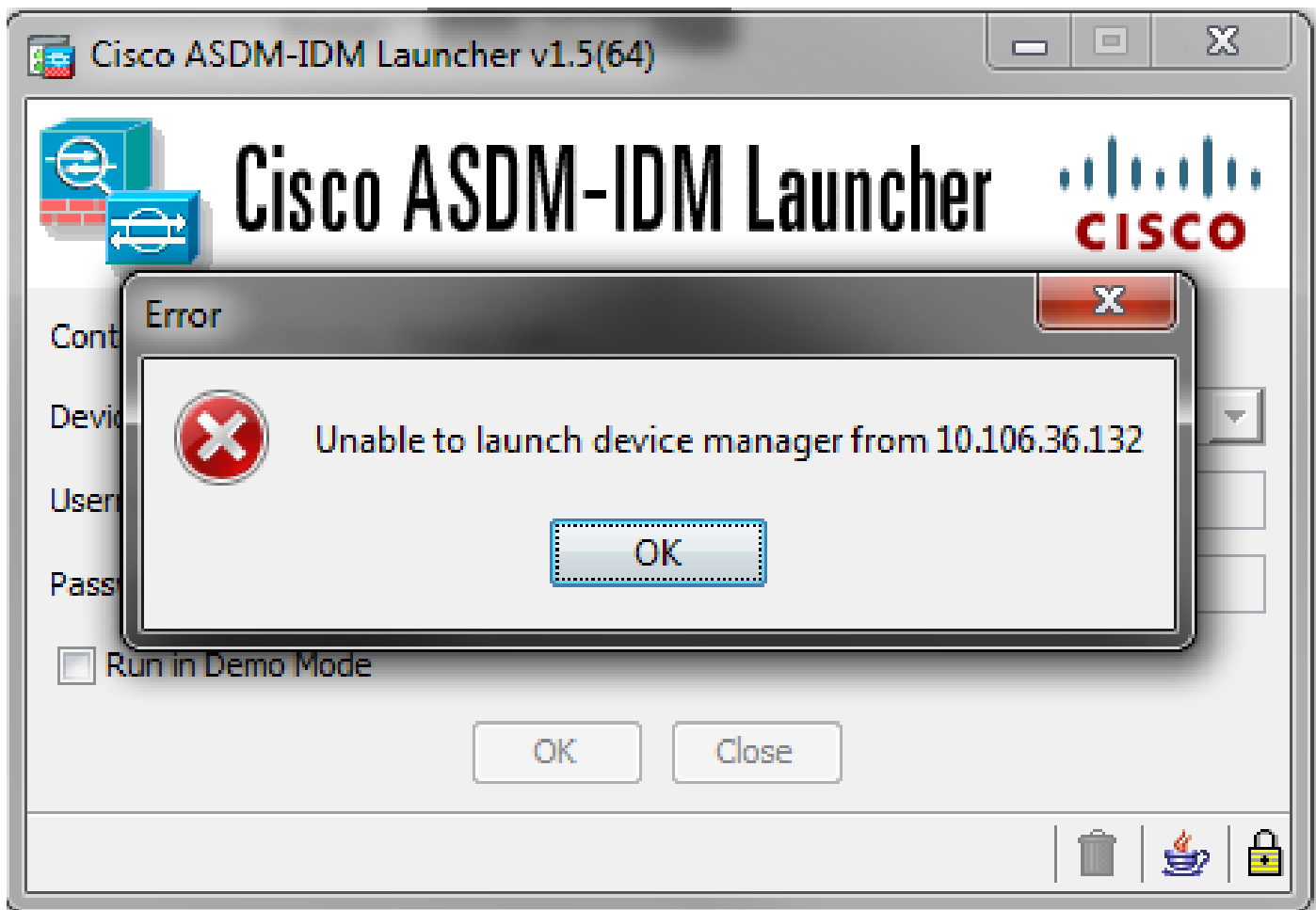
HTTP服务器限制

此步骤在ASDM配置中至关重要，因为它定义了哪些网络可以访问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
```

验证您是否有在前面的配置中定义的必要网络。缺少这些定义会导致ASDM启动程序在连接时超时，并产生以下错误：



ASDM启动页面(<https://<ASA IP地址>/admin>)导致请求超时，且不会显示任何页面。

进一步验证HTTP服务器使用非标准端口进行ASDM连接，例如8443。配置中会突出显示以下内容：

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

如果它使用非标准端口，则需要在连接到ASDM启动程序中的ASA时将端口指定为：

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

当您访问ASDM启动页面时，这也适用：<https://10.106.36.132:8443/admin>

其他可能的配置问题

完成上述步骤后，如果客户端一切正常，则ASDM可以打开。但是，如果仍然遇到问题，请从另一台计算机打开ASDM。如果成功，则问题可能出在应用级别，并且ASA配置正常。但是，如果仍然无法启动，请完成以下步骤以进一步验证ASA端配置：

1. 验证ASA上的安全套接字层(SSL)配置。ASDM在与ASA通信时使用SSL。根据ASDM的启动方式，较新的操作系统软件在协商SSL会话时不允许使用较弱的密码。使用show run all ssl命令验证在ASA上允许哪些密码，以及配置中是否指定了任何特定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启动时存在任何SSL密码协商错误，它们将显示在ASA日志中：

```
%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
```

如果看到特定设置，请将其恢复为默认值。请注意，需要在ASA上启用VPN-3DES-AES许可证，以便ASA在配置中使用3DES和AES密码。这可以通过CLI上的show version命令进行验证。输出显示如下：

```
<#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许可证可以从思科许可网站[免费获取](#)。点击安全产品，然后选择Cisco ASA

3DES/AES许可证。

 注：在随附8.6/9.x代码的新ASA 5500-X平台中，默认情况下，SSL密码设置设置为des-sha1，这会导致ASDM会话无法工作。有关详细信息，请参阅[ASA 5500-x:ASDM和其他SSL功能开箱即用](#)文章。

2. 验证ASA上是否已启用WebVPN。如果已启用，则需使用此URL(<https://10.106.36.132/admin>)才能在访问ASDM Web启动页面时访问它。
3. 在ASA上检查端口443的网络地址转换(NAT)配置。这会导致ASA不处理ASDM请求，而是将其发送到已为其配置NAT的网络/接口。
4. 如果所有内容都已验证并且ASDM仍然超时，请通过ASA CLI上的show asp table socket命令验证ASA是否设置为侦听为ASDM定义的端口。输出可以显示ASA在ASDM端口上侦听：

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

如果此输出未显示，请删除并重新应用ASA上的HTTP服务器配置，以便重置ASA软件上的套接字。

5. 如果在登录/验证ASDM时遇到问题，请验证HTTP的身份验证选项是否设置正确。如果未设置身份验证命令，您可以使用ASA启用密码登录到ASDM。如果要启用基于用户名/密码的身份验证，需要输入此配置以从ASA的用户名/密码数据库对ASA的ASDM/HTTP会话进行身份验证：

```
<#root>
```

```
aaa authentication http console LOCAL
```

请记住，在启用上一个命令时，应创建用户名/密码：

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

如果上述步骤均无帮助，则在ASA上可以使用以下调试选项进行进一步调查：

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

网络连接

如果您已完成上一部分但仍无法访问ASDM，则下一步是验证从要访问ASDM的计算机到ASA的网络连接。要验证ASA是否收到来自客户端计算机的请求，需要执行一些基本的故障排除步骤：

1. 使用互联网控制消息协议(ICMP)进行测试。
对要从中访问ASDM的ASA接口执行ping操作。如果允许ICMP通过您的网络，并且ASA接口

级别没有限制，则ping操作可以成功。如果ping失败，可能是因为在ASA和客户端计算机之间存在通信问题。但是，这还不是确定是否存在此类通信问题的决定性步骤。

2. 确认数据包捕获。

在要访问ASDM的接口上放置数据包捕获。捕获可显示目的地为接口IP地址的TCP数据包到达目的端口号443（默认）。

要配置捕获，请使用以下命令：

```
<#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
```

这会捕获从连接到ASDM的ASA接口上的端口443的所有TCP流量。此时通过ASDM连接或打开ASDM Web启动页面。然后使用show capture asdm_test命令查看捕获的数据包的结果：

```
<#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>
```

此捕获显示从客户端计算机到ASA的同步(SYN)请求，但ASA不发送任何响应。如果您看到类似于前一捕获的捕获，则意味着数据包到达ASA，但ASA不响应这些请求，从而隔离问题到ASA自身。请参阅本文档的第一部分以进一步排除故障。

但是，如果您没有看到与前面类似的输出，并且没有捕获任何数据包，这意味着ASA和ASDM客户端计算机之间存在连接问题。确认没有可以阻止TCP端口443流量的中间设备，并且没有可能阻止流量到达ASA的浏览器设置（如代理设置）。

通常，数据包捕获是确定通往ASA的路径是否清晰，以及是否无需进一步诊断以排除网络连接问题的好方法。

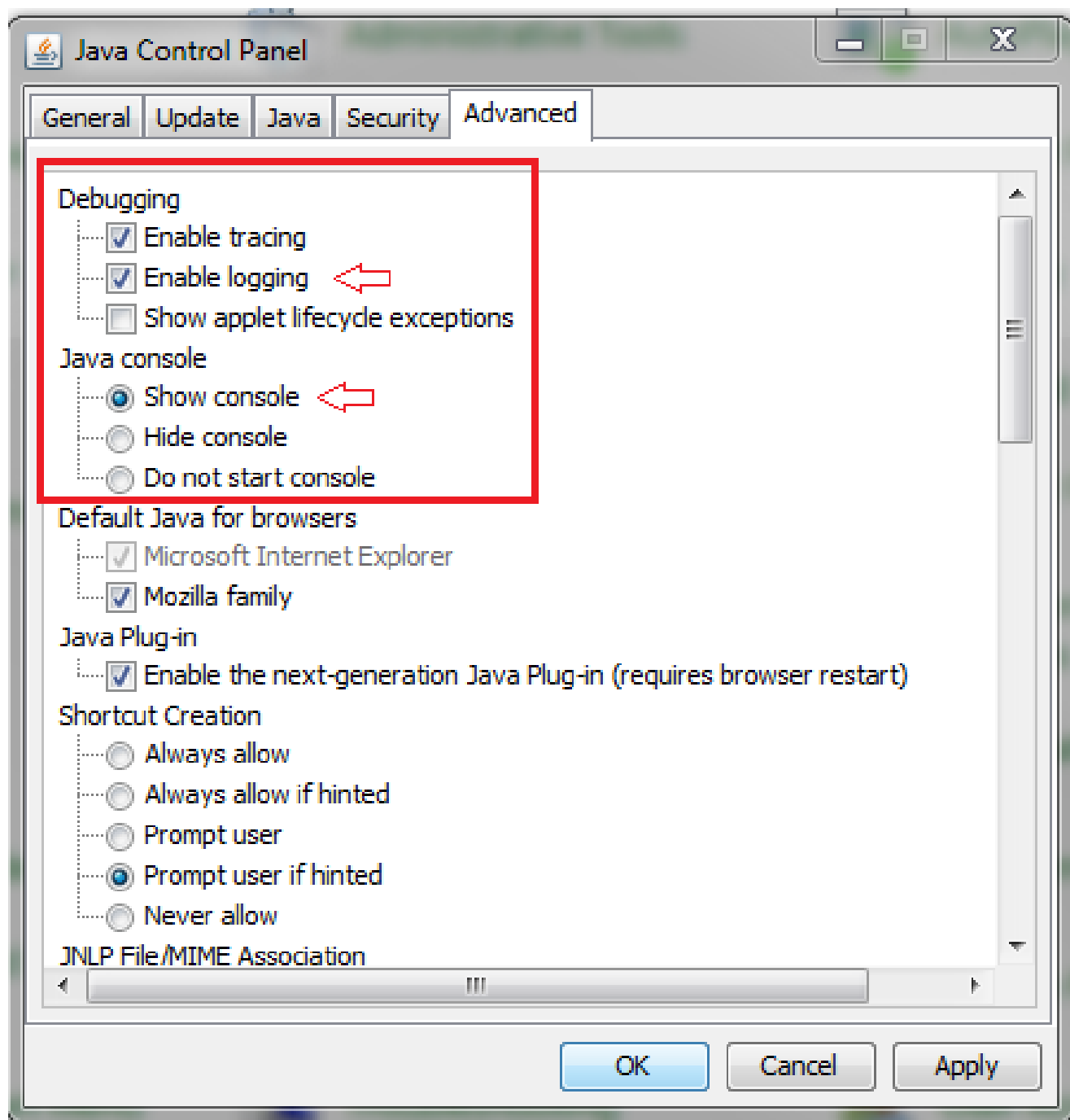
应用软件

本节介绍如何排除在客户端计算机上安装的ASDM启动程序软件无法启动/加载时的故障。ASDM启动程序是驻留在客户端计算机上并连接到ASA以检索ASDM映像的组件。检索后，ASDM映像通常存储在缓存中，并从缓存中获取，直到ASA端发现任何更改（例如ASDM映像更新）。

完成以下基本故障排除步骤以排除客户端计算机上的任何问题：

1. 从其他计算机打开ASDM启动页面。如果启动，则意味着问题出在客户端计算机上。如果它发生故障，请使用故障排除指南从头开始按顺序隔离相关组件。
2. 通过Web启动打开ASDM，并从那里直接启动软件。如果成功，则很可能存在ASDM启动程序安装问题。从客户端计算机上卸载ASDM启动程序，然后从ASA Web启动本身重新安装它。
3. 在用户主目录中清除ASDM的缓存目录。删除整个缓存目录时清除缓存。如果ASDM成功启动，您也可以从ASDM File (ASDM文件) 菜单中清除缓存。
4. 验证已安装正确的Java版本。[Cisco ASDM发行说明](#)列出了已测试Java版本的要求。
5. 清除Java缓存。在Java Control Panel中，选择General > Temporary Internet File。然后，单击View以启动Java Cache Viewer。删除引用或与ASDM相关的所有条目。
6. 如果这些步骤失败，请从客户端收集调试信息以作进一步调查。使用URL为ASDM启用调试：<https://<ASA的IP地址>?debug=5>，例如<https://10.0.0.1?debug=5>。使用Java版本6（也称为1.6版），可从Java Control Panel > Advanced启用Java调试消息。

然后选择调试下的复选框。请勿在Java控制台下选择不启动控制台。在ASDM启动之前，必须启用Java调试。



Java控制台输出记录在用户主目录的.asdm/log目录中。ASDM日志也可以在同一目录中找到。

使用HTTPS运行命令

此过程有助于确定HTTP通道的任何第7层问题。当ASDM应用本身不可访问，并且没有任何可用于管理设备的CLI访问时，此信息非常有用。

用于访问ASDM Web启动页面的URL也可用于在ASA上运行任何配置级别命令。此URL可用于对

ASA进行基本级别的配置更改，包括远程设备重新加载。要输入命令，请使用以下语法：

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

如果命令中有空格，并且浏览器无法分析URL中的空格字符，则可以使用+或%20来指示空格。

例如，[https://10.106.36.137/admin/exec/show ver](https://10.106.36.137/admin/exec/show%20ver)会生成到浏览器的show version输出：

```
https://10.106.36.137/admin/exec/show ver

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
```

此命令执行方法要求在ASA上启用HTTP服务器，并且激活必要的HTTP限制。但是，这不需要在ASA上存在ASDM映像。

相关信息

- [配置设备的ASDM访问](#)
- [ASA 5500-x:ASDM和其他SSL功能开箱即用](#)
- [Cisco ASDM版本说明](#)

- [在ASA上获取3DES/AES许可证的思科许可证页面](#)
- [技术支持和文档 - Cisco Systems](#)

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）。