# 故障排除

本章涵盖以下部分：


- Secure Firewall ASA 设备故障排除， 第 1 页
- 对安全设备连接器进行故障排除， 第 12 页
- 安全事件连接器故障排除, on page 20
- 对思科防御协调器进行故障排除, on page 31
- 设备连接状态, on page 39


# Secure Firewall ASA 设备故障排除

## 重新启动后，ASA 无法重新连接到 CDO

如果 CDO 和您的 ASA 在 ASA 重新启动后不连接，可能是因为 ASA 已回退到使用 CDO 的安全设备连接器 (SDC) 不支持的 OpenSSL 密码套件。此故障排除主题针对该案例进行测试，并提供补救步骤。

### 现象

- ASA 重新启动，CDO 和 ASA 无法重新连接。CDO 显示消息“重新连接失败”。
- 尝试载入 ASA 时，CDO 显示消息：无法检索以下项的证书：<ASA_IP_Address> 。

## 由于证书错误而无法载入 ASA

**环境**：ASA 配置了客户端证书身份验证。

**解决方案**：禁用客户端证书身份验证。

**详细信息**：ASA 支持基于凭证的身份验证以及客户端证书身份验证。CDO 无法连接到使用客户端证书身份验证的 ASA。在将 ASA 载入 CDO 之前，请使用以下程序来确保其未启用客户端证书身份验证：

**步骤 1** 打开终端窗口并使用 SSH 连接到 ASA。

**步骤 2** 进入全局配置 模式。

**步骤 3** 在 hostname (config)# 提示符处输入以下命令：

```
no ssl certificate-authentication interface interface-name port 443
```

接口名称是 CDO 连接到的接口的名称。

## 确定 ASA 使用的 OpenSSL 密码套件

使用此程序可识别 ASA 使用的 OpenSSL 密码套件。如果命令输出中指定的密码套件不在支持的密码套件列表中，则 SDC 不支持该密码套件，您需要在 ASA 上更新密码套件。CDO 的安全设备连接器支持的密码套件, on page 2

**步骤 1** 在可以访问 SDC 的计算机上打开控制台窗口。

**步骤 2** 使用 SSH 连接到 SDC。您可以以常规用户（例如 CDO 或 SDC）或您创建的其他用户身份登录。您无需以 root 用户身份登录。

**Tip** 要查找 SDC IP 地址，请执行以下操作：

a. 打开 CDO。

b. 从用户菜单中，选择“安全设备连接器”(Secure Device Connectors)。

c. 点击表中显示的 SDC。SDC 的 IP 地址显示在设备的详细信息窗格中。

**步骤 3** 在命令提示符后输入：openssl s_client -showcerts -connect ASA_IP_Address :443

**步骤 4** 在命令输出中查找这些行。

```
New, TLSV1/SSLv3, Cipher is DES-CB3-SHA
or
SSL-Session:
            Protocol: TLSv1.2
            Cipher: DES-CB3-SHA
```

在本示例中，ASA 使用的密码套件是 DES-CB3-SHA。

## CDO 的安全设备连接器支持的密码套件

CDO 的安全设备连接器使用仅接受最新和最安全密码的 node.js。因此，CDO 的 SDC 仅支持以下密码列表：

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA256
- DHE-RSA-AES256-SHA256

如果您在 ASA 上使用的密码套件不在此列表中，则 SDC 不支持该密码套件，您需要更新 ASA 的密码套件。

## 更新 ASA 的密码套件

**要更新 ASA 上的 TLS 密码套件，请执行以下操作：**

**步骤 1** 使用 SSH 连接到 ASA。

**步骤 2** 连接到 ASA 后，将权限提升到全局配置模式。您的提示符应如下所示：asaname(config)#

**步骤 3** 在提示符后，输入与此类似的命令：

```
ssl cipher tlsv1.2 custom "ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384 DHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256
 DHE-RSA-AES128-SHA256 ECDHE-RSA-AES256-SHA384 DHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA256
DHE-RSA-AES256-SHA256"
```

**Note** 此命令配置 ASA 支持的密码套件包含在引号之间和单词 custom 之后。在此命令中，指定的密码套件以 `ECDHE-RSA-AES128-GCM-SHA256` 开头，以 `DHE-RSA-AES256-SHA256`结尾。当您在 ASA 上输入 命令时，请删除您知道 ASA 不支持的任何密码套件。

**步骤 4** 提交命令后，在提示符后输入 write memory 以保存本地配置。例如：`asaname(config)#write memory`

# 使用 CLI 命令对 ASA 进行故障排除

本节讨论您可能希望用于对 ASA 进行故障排除和测试基本连接的一些重要命令。请参阅《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》，了解其他故障排除场景和 CLI 命令。在“系统管理”部分，导航至“测试和故障排除”一章。

您可以使用每个 ASA 设备可用的 CDO CLI 界面来执行这些命令。请参阅使用 CDO 命令行界面，了解如何在 CDO 中使用 CLI 界面。

### NAT 策略设置

确定 NAT 设置的一些重要命令如下：

- 要确定 NAT 策略统计信息，请使用 show nat。
- 要确定 NAT 池，包括已分配的地址和端口，及其分配次数，请使用 **show nat pool**。

有关与 NAT 相关的更多命令，请参阅《CLI 手册 2：思科 ASA 系列防火墙 CLI 配置指南》，并导航至“网络地址转换 (NAT)”一章。

### 测试基本连接：Ping 通地址

您可以使用 ping 命令对 ASA 设备执行 ping 操作<IP address>命令。了解有关

### 显示路由表

使用 **show route** 命令来查看路由表中的条目。

**ciscoasa# show route**

ASA 路由表的输出示例：

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - 静态 InterVRF
Gateway of last resort is 192.168.0.254 to network 0.0.0.0
S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.0.254, management
C 10.0.0.0 255.0.0.0 is directly connected, outside
L 10.10.10.1 255.255.255.255 is directly connected, Outside
C 192.168.0.0 255.255.255.0 is directly connected, management
L 192.168.0.118 255.255.255.255 is directly connected, management
```

### 监控交换机端口

- **show interface**

  显示接口统计信息。

- **show interface ip brief**

  显示接口的 IP 地址和状态。

- **show arp**

显示动态、静态和代理 ARP 条目。动态 ARP 条目包括 ARP 条目时限（秒）。

ARP 条目输出示例：

```
management 10.10.32.129 0050.568a.977b 0
management 10.10.32.136 0050.568a.5387 21
LANFAIL 20.20.21.1 0050.568a.4d70 96
outsi 10.10.16.6 0050.568a.e6d3 3881
outsi 10.10.16.1 0050.568a.977b 5551
```

# ASA 远程访问 VPN 故障排除

本节讨论在 ASA 设备上配置远程访问 VPN 时可能出现的一些故障排除问题。

### “RA VPN 监控”页面上缺少信息

如果未为 Webvpn 启用外部接口，则可能会出现此问题。

**解决方法：**

1. 在导航窗格中，点击 **设备和服务**。
2. 点击**设备 (Devices)** 选项卡，然后点击 **ASA** 选项卡。
3. 选择存在问题的 RA VPN 头端 ASA 设备。
4. 在右侧的 **管理 (Management)** 窗格中，点击**配置 (Configuration)**。
5. 点击“编辑”并搜索“webvpn”。
6. 按 Enter 键并添加 enable interface_name。这里，interface_name 是用户在进行远程访问 VPN 连接时所连接的外部接口的名称。请选择您使用此连接配置文件支持的设备与最终用户之间的任何接口，虽然这通常是外部（面向互联网的）接口。

   例如：

   ```
   webvpn
   enable outside
   ```
7. 点击**保存 (Save)**。
8. 预览配置并将其部署到设备。预览和部署所有设备的配置更改

# 无法将 ASA 添加到现有 RA VPN 配置

-

开始之前

- 

**SUMMARY STEPS**

**1.**

**DETAILED STEPS**

| | 命令或操作 | 目的 |
|---|---|---|
| 步骤 1 | 示例： | |

示例

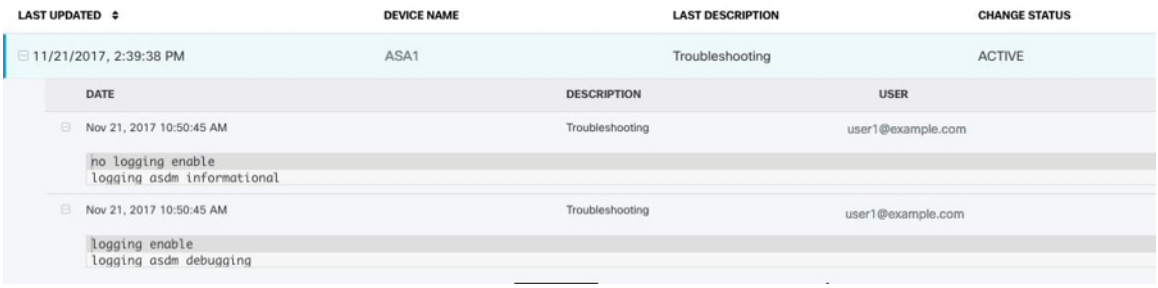
下一步做什么

- 

# ASA 实时日志记录

使用实时日志记录显示最近 20 秒记录的数据或最后 10 KB 的记录数据，以先达到的限制为准。当 CDO 检索实时数据时，它会查看 ASDM 上的现有日志记录配置，将其更改为请求调试级别的数据，然后将日志记录配置返回到您的配置。日志记录 CDO 显示反映您在 ASDM 中设置的任何日志记录过滤器。

您可以通过查看更改日志来查看 CDO 发送的用于执行日志记录的命令。以下是更改日志条目的示例。第一个条目（位于底部）表示 CDO 使用 logging enable 命令“打开”日志记录，并将 ASDM 日志记录级别更改为调试。第二个条目（位于顶部）显示日志记录配置已恢复到之前的状态。已使用 no logging enable 命令“关闭”日志记录，并且 ASDM 日志记录级别已恢复为 informational。




## 查看 ASA 实时日志

**步骤 1** 在 **设备和服务** 页面上，点击 **设备** 选项卡。

**步骤 2** 点击相应的设备类型选项卡，然后选择要查看其实时数据的设备。

**步骤 3** 点击**故障排除 (Troubleshoot)** Troubleshoot 。

**步骤 4** （可选）在点击查看实时日志之前，您可以在左侧窗格中定义过滤器，以优化日志记录搜索的结果。

**步骤 5** 点击查看实时日志。CDO 根据您的过滤条件检索实时日志记录数据并显示该数据。

**步骤 6** 查看额外的 20 秒记录的数据或最后 10 KB 的记录数据。再次点击查看实时日志。

# ASA 数据包跟踪器

数据包跟踪器允许您将合成数据包发送到网络中，并评估现有路由配置、NAT 规则和策略配置如何影响该数据包。使用此工具可对以下类型的问题进行故障排除：

- 用户报告他们无法访问他们应该能够访问的资源。
- 用户报告他们可以访问他们不应该能够访问的资源。
- 测试策略以确定其是否按预期工作。

数据包跟踪器可用于物理或虚拟的实时在线 ASA 设备。Packet Tracer 在 ASA 型号设备上不起作用。数据包跟踪器根据 ASA 上保存的配置评估数据包。数据包跟踪器不会评估 CDO 上的暂存更改。

我们认为最佳做法是在处于同步状态的 ASA 上运行数据包跟踪器。虽然如果设备未同步，数据包跟踪器将运行，但您可能会遇到一些意外结果。例如，如果您在 CDO 上删除了暂存配置中的规则，并且在数据包跟踪期间在 ASA 上触发了同一规则，则 CDO 将无法显示数据包与该规则的交互结果。

### 使用 ASA Packet Tracer 进行故障排除

当数据包跟踪器通过 ASA 的路由配置、NAT 规则和安全策略发送数据包时，它会在每个步骤显示数据包的状态。如果策略允许该数据包，则会显示绿色复选标记。如果数据包被拒绝并丢弃，CDO 会显示一个红色的 X。

数据包跟踪器还会显示数据包跟踪结果的实时日志。在下面的示例中，您可以看到规则拒绝 tcp 数据包的位置。


## 对 ASA 设备安全策略进行故障排除

**步骤 1** 在设备和服务页面中，选择您的 ASA，然后点击操作窗格中的故障排除。 Troubleshoot

**步骤 2** 在 Values 窗格中，选择要通过 ASA 虚拟发送的接口和数据包类型。

**步骤 3** （可选）如果要跟踪将安全组标签值嵌入第 2 层 CMD 报头 (Trustse) 的数据包，请选中 SGT 编号，然后输入安全组标签编号 0-65535。

**步骤 4** 指定源和目标。如果使用思科 Trustsec，可以指定 IPv4 或 IPv6 地址、完全限定域名 (FQDN) 或安全组名称或标记。对于源地址，您还可以指定 Domain\username 格式的用户名。

**步骤 5** 指定其他协议特征：

- ICMP - 输入 ICMP 类型、ICMP 代码 (0-255)，并且可以选择键入 ICMP 标识符。
- TCP/UDP/SCTP - 通过从列表中选择源和目标端口或在端口组合框中输入值来输入它们。
- IP - 输入协议编号 0-255。

**步骤 6** 点击**运行 Packet Tracer (Run Packet Tracer)**。

**步骤 7** 继续分析 Packet Tracer 结果。分析 Packet Tracer 结果, on page 9

## 对访问规则进行故障排除

**步骤 1** 选择**策略 (Policies)** > **网络策略 (Network Policies)** > 。

**步骤 2** 选择与您的 ASA 关联的策略。

**步骤 3** 在网络策略中选择要进行故障排除的规则，然后点击详细信息窗格中的**故障排除** Troubleshoot 。请注意，在故障排除页面的“值”面板中，许多字段已预填充了您选择的规则的属性。

**步骤 4** 在其余必填字段中输入信息。完成所有必填字段后，“运行 Packet Tracer”按钮变为活动状态。

**步骤 5** 点击**运行 Packet Tracer (Run Packet Tracer)**。

**步骤 6** 继续分析 Packet Tracer 结果。分析 Packet Tracer 结果, on page 9

## 对 NAT 规则进行故障排除

**步骤 1** 在**设备和服务** 页面中，选择您的 ASA，然后点击操作窗格中的**查看 NAT 规则** View NAT Rules 。

**步骤 2** 从NAT规则表中选择要进行故障排除的规则，然后点击详细信息窗格中的**故障排除** Troubleshoot 。请注意，在“故障排除”(Troubleshoot) 页面的“值”(values) 面板中，许多字段都预填充了您选择的规则的属性。

**步骤 3** 在其余必填字段中输入信息。完成所有必填字段后，Run Packet Tracer 将变为活动状态。

**步骤 4** 点击**运行 Packet Tracer (Run Packet Tracer)**。

**步骤 5** 继续分析 Packet Tracer 结果。分析 Packet Tracer 结果, on page 9

## 对两次 NAT 规则进行故障排除

**步骤 1** 在设备和服务页面中，选择您的 ASA，然后点击操作窗格中的查看 NAT 规则。 View NAT Rules

**步骤 2** 从 NAT 规则表中选择要进行故障排除的规则，然后点击详细信息窗格中的故障排除。 Troubleshoot 对于双向 Twice NAT 规则，这将打开一个下拉列表，您可以在其中选择对源数据包转换或目标数据包转换进行故障排除。

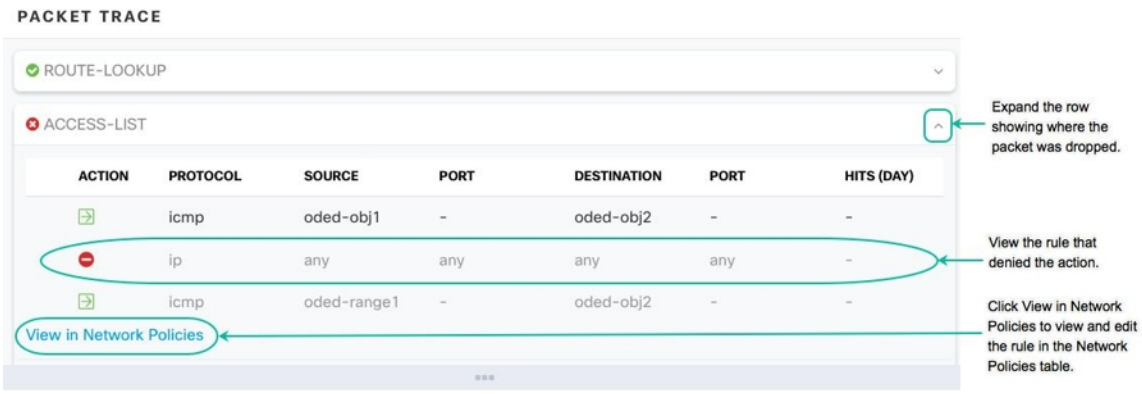
**步骤 3** 在其余必填字段中输入信息。完成所有必填字段后，Run Packet Tracer 将变为活动状态。

**步骤 4** 点击**运行 Packet Tracer (Run Packet Tracer)**。

## 分析 Packet Tracer 结果

无论数据包被丢弃还是被允许，您都可以通过展开数据包跟踪表中的一行并读取与该操作相关的规则或日志记录信息来了解原因。在下面的示例中，数据包跟踪器识别了一个访问列表策略，该策略包含一条拒绝来自任何源并发往任何目的地的 IP 数据包的规则。如果这不是您想要的操作，您可以点击**在网络策略中查看**链接并立即编辑该规则。编辑规则后，请务必将该配置更改部署到 ASA，然后重新运行数据包跟踪器，以确保获得预期的访问结果。

除数据包跟踪器结果外，CDO 还会显示来自 ASA 的ASA 实时日志记录。




# 思科 ASA 公告 cisco-sa-20180129-asa1

思科产品安全事件响应团队 (PSIRT) 发布了安全公告 cisco-sa-20180129-asa1，其中描述了严重性为 ASA 和 Firepower 的安全漏洞。 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1有关受影响的 ASA 和 Firepower 硬件、软件和配置的完整说明，请阅读整个 PSIRT 团队公告。https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1

如果您确定您的 ASA 受到公告的影响，您可以使用 CDO 将您的 ASA 升级到补丁版本。使用此过程：

**步骤 1** 在每个受影响的 ASA 上配置 DNS 服务器。在 ASA 上配置 DNS

**步骤 2** 返回到公告，确定您需要的软件补丁。https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1

**步骤 3** 有关介绍如何使用 CDO 将 ASA 升级到 ASA 公告中列出的固定版本的主题，请参阅在单个 ASA 上升级 ASA 和 ASDM 映像。从升级必备条件开始，然后阅读有关升级单个 ASA、在主用-备用配置中升级 ASA 或批量升级 ASA 的信息。ASA 和 ASDM 升级必备条件

为方便起见，以下是思科报告的安全公告的摘要：

2018 年 2 月 5 日更新：经过进一步调查，思科已确定受此漏洞影响的其他攻击媒介和功能。此外，还发现原始修复不完整，因此现在可以使用新的修复代码版本。有关详细信息，请参阅固定软件部分。思科自适应安全设备 (ASA) 软件的 XML 解析器中存在允许未经身份验证的远程攻击者重新加载受影响系统或远程执行代码的漏洞。由于内存不足，ASA 也可能停止处理传入的虚拟专用网络 (VPN) 身份验证请求。该漏洞是由处理恶意 XML 负载时分配和释放内存的问题引起的。攻击者可以通过将特制的 XML 数据包发送到受影响系统上的易受攻击的接口来利用此漏洞。通过利用该漏洞，攻击者可执行任意代码并获得系统的完全控制，导致受影响设备重新加载或停止处理传入的 VPN 身份验证请求。要受到攻击，ASA 必须在接口上启用安全套接字层 (SSL) 服务或 IKEv2 远程访问 VPN 服务。漏洞被利用的风险还取决于接口对攻击者的可访问性。有关易受攻击的 ASA 功能的完整列表，请参阅易受攻击的产品部分中的表格。思科已发布解决此漏洞的软件更新。目前还没有解决受此漏洞影响的所有功能的变通方法。此公告位于以下链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1

# 确认 ASA 运行配置大小

要确认运行配置文件的大小，请执行以下程序：

**步骤 1** 通过以下方式之一访问 ASA 的命令行界面：

- 打开终端窗口并使用 SSH 登录 ASA。将您的权限提升到“特权 EXEC”模式，以便您看到带有 `hostname#` 的提示符。
- 如果您已成功载入 ASA，请打开**清单 (Inventory)** 页面，选择要连接的设备，然后点击“设备操作”(Device Actions) 窗格中的 **>_ 命令行接口 (>_ Command Line Interface)** 按钮。

**步骤 2** 在提示符后键入 `copy running-config flash`

**步骤 3** 当系统提示输入源文件名时，请勿输入任何内容并按 <Enter>

**步骤 4** 当提示输入目标文件名时，请输入输出文件的名称。在 ASA 复制您指定的文件的运行配置后，它会返回到特权 EXEC 提示符。

**步骤 5** 在提示符后键入 `show flash`。

**步骤 6** 查看长度列。如果文件超过 4718592 字节，则大于 4.5 MB。

以下是一组命令和输出示例：

```
asa1# copy running-config flash
Source filename [running-config]?
Destination filename [running-config]? running-config-output
Cryptochecksum: 725f4c1c 4adfb8a9 8b3e7a6d 49e3420d
23648 bytes copied in 1.380 secs (23648 bytes/sec)
asa1# show flash
--#-- --length-- -----date/time------ path
 107 110325428 Feb 28 2019 15:41:42 asdm-8826067.bin
 122 5018592 Apr 30 2019 21:00:59 running-config-output
 111 102647808 Mar 12 2019 14:26:10 asa9-12-1-smp-k8.bin
```

# 影响安全设备连接器的容器权限升级漏洞：cisco-sa-20190215-runc

思科产品安全事件响应团队 (PSIRT) 发布了安全公告 cisco-sa-20190215-runc，其中描述了 Docker 中的一个高严重性漏洞。阅读整个 PSIRT 团队公告，了解漏洞的完整说明。https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190215-runc

此漏洞会影响所有 CDO 客户：

- 使用 CDO 云部署的安全设备连接器 (SDC) 的客户无需执行任何操作，因为 CDO 运营团队已执行补救步骤。
- 使用本地部署的 SDC 的客户需要升级其 SDC 主机才能使用最新的 Docker 版本。他们可以按照以下说明执行此操作：

## 更新 CDO 标准 SDC 主机

如果您使用 CDO 映像部署了 SDC，请使用以下说明。 使用 CDO 的 VM 映像部署安全设备连接器

**步骤 1** 使用 SSH 或虚拟机监控程序控制台连接到 SDC 主机。

**步骤 2** 运行以下命令检查 Docker 服务的版本：

```
docker version
```

**步骤 3** 如果您运行的是最新的虚拟机 (VM)，您应该会看到如下输出：

```
 > docker version
Client:
     Version: 18.06.1-ce
     API version: 1.38
     Go version: go1.10.3
     Git commit: e68fc7a
     Built: Tue Aug 21 17:23:03 2018
     OS/Arch: linux/amd64
     Experimental: false
```

您可能会在这里看到旧版本。

**步骤 4** 运行以下命令以更新 Docker 并重新启动服务：

```
> sudo yum update docker-ce
> sudo service docker restart
```

**注释** 当 Docker 服务重新启动时，CDO 和您的设备之间会出现短暂的连接中断。

**步骤 5** 再次运行 docker version 命令。您应该会看到以下输出：

```
> docker version
Client:
    Version: 18.09.2
    API version: 1.39
    Go version: go1.10.6
    Git commit: 6247962
    Built: Sun Feb XX 04:13:27 2019
    OS/Arch: linux/amd64
    Experimental: false
```

**步骤 6** 大功告成。您现在已升级到 Docker 的最新版本并安装了补丁。

## 更新自定义 SDC 主机

如果您已创建自己的 SDC 主机，则需要按照说明根据 Docker 的安装方式进行更新。如果您使用的是 CentOS、yum 和 Docker-ce（社区版），则前面的程序将起作用。

如果您已安装 Docker-ee（企业版）或使用其他方法安装 Docker，则 Docker 的固定版本可能不同。您可以查看 Docker 页面以确定要安装的正确版本：Docker 安全更新和容器安全最佳实践。
https://blog.docker.com/2019/02/docker-security-update-cve-2018-5736-and-container-security-best-practices/

## 缺陷跟踪

思科将继续评估此漏洞，并将在获得更多信息时更新公告。公告被标记为最终版本后，您可以参考相关的思科漏洞了解更多详细信息：

CSCvo33929-CVE-2019-5736: runc container breakout

# 大型 ASA 运行配置文件

### CDO 中的行为

您可能会看到 ASA 无法载入、CDO 未显示 ASA 运行配置文件中定义的所有配置或 CDO 无法写入更改日志等行为。

### 可能的原因

ASA 的运行配置文件对于 CDO 而言可能“过大”。

当您将 ASA 载入 CDO 时，CDO 会在其数据库中存储 ASA 的运行配置文件的副本。通常，如果该运行配置文件过大（4.5 MB 或更大），或者包含的行过多（大约 22,000 行），或者单个访问组的访问列表条目过多，则 CDO 将无法可预测地管理该设备。

要确认运行配置文件的大小，请参阅确认 ASA 运行配置大小。

### 解决方法或解决方案

请联系您的思科客户团队寻求帮助，以在不中断安全策略的情况下安全地减小配置文件的大小。

# 对安全设备连接器进行故障排除

使用这些主题对现场安全设备连接器 (SDC) 进行故障排除。

如果这些场景都不符合您的情况，请通过思科技术支持中心提交支持案例。

# SDC 无法接通

如果 SDC 未能连续响应来自 CDO 的两个心跳请求，则该 SDC 处于“无法访问”状态。如果您的 SDC 无法访问，您的租户将无法与您已载入的任何设备通信。

CDO 表示无法通过以下方式访问 SDC：

- 您会看到消息“某些安全设备连接器 (SDC) 无法访问。您将无法与与这些 SDC 关联的设备进行通信。”在 CDO 主页上。
- “服务”(Services) 页面中的 SDC 状态为“无法访问”(Unreachable)。

首先，尝试将 SDC 重新连接到租户以解决此问题：

1. 检查 SDC 虚拟机是否正在运行，并且可以访问您所在地区的 CDO IP 地址。请参阅将 思科防御协调器 连接到托管设备。
2. 尝试通过手动请求心跳来重新连接 CDO 和 SDC。如果 SDC 响应心跳请求，它将返回“活动”状态。要手动请求心跳，请执行以下操作：
   1. 从 CDO 菜单中，选择**工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。
   2. 点击无法访问的 SDC。
   3. 在“操作”(Actions) 窗格中，点击**请求检测信号 (Request Heartbeat)**。
   4. 点击**重新连接 (Reconnect)**。
3. 如果在手动尝试将 SDC 重新连接到租户后，SDC 未返回到主用状态，请按照中的说明进行操作。部署后，SDC 状态在 CDO 上未变为活动状态 ，第 13 页

   。

# 部署后，SDC 状态在 CDO 上未变为活动状态

如果 CDO 在部署后约 10 分钟内未指示您的 SDC 处于活动状态，请使用您在部署 SDC 时创建的 cdo 用户和密码，通过 SSH 连接到 SDC VM。

---

**步骤 1** 查看 /opt/cdo/configure.log。它会显示您为 SDC 输入的配置设置，以及这些设置是否已成功应用。如果设置过程中出现任何故障，或者值输入不正确，请再次运行 sdc-onboard 设置：

a) 在 [cdo@localhost cdo]$ 提示符后，输入 sudo sdc-onboard setup。
b) 输入 `cdo` 用户的密码。
c) 按照提示操作。设置脚本将指导您完成在设置向导中执行的所有配置步骤，并为您提供更改输入的值的机会。

**步骤 2** 如果在查看日志并运行 sudo sdc-onboard setup 后，CDO 仍不指示 SDC 处于活动状态，请联系 CDO 支持。联系思科威胁防御支持

---

# 更改后的 SDC IP 地址未反映在 CDO 中

如果您更改了 SDC 的 IP 地址，则在格林威治标准时间上午 3:00 之前，它不会反映在 CDO 中。

# 排除设备与 SDC 的连接故障

使用此工具可测试从CDO通过安全设备连接器(SDC)到您的设备的连接。如果您的设备未能载入，或者您想在载入之前确定 CDO 是否可以访问您的设备，则可能需要测试此连接。

**步骤 1** 从 CDO 菜单中，选择**工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)**。

**步骤 2** 选择 SDC。

**步骤 3** 在右侧的**故障排除 (Troubleshooting)** 窗格中，点击**设备连接 (Device Connectivity)**。

**步骤 4** 输入您尝试进行故障排除或尝试连接的设备的有效 IP 地址或 FQDN 和端口号，然后点击**开始 (Go)**。CDO 执行以下验证：

a) **DNS 解析 (DNS Resolution)** - 如果您提供 FQDN 而不是 IP 地址，这将验证 SDC 可以解析域名并获取 IP 地址。

b) **连接测试 (Connection Test)** - 验证设备是否可访问。

c) **TLS 支持 (TLS Support)** - 检测设备和 SDC 支持的 TLS 版本和密码。

- **不支持的密码 (Unsupported Cipher)** - 如果没有设备和 SDC 都支持的 TLS 版本，则 CDO 还会测试设备（而不是 SDC）支持的 TLS 版本和密码。

d) “SSL 证书”(SSL Certificate) - 故障排除提供证书信息。

**步骤 5** 如果在载入或连接设备方面仍有问题，请联系防御协调器支持。

# 与 SDC 间歇性连接或无连接

本节中讨论的解决方案仅适用于本地安全设备连接器 (SDC)。

症状：与 SDC 的连接断断续续或无连接。

诊断：如果磁盘空间几乎已满（80% 以上），可能会出现此问题。

执行以下步骤以检查磁盘空间使用情况。

1. 打开 Secure Device Connector (SDC) VM 的控制台。
2. 使用用户名 **cdo** 登录。
3. 输入初始登录时创建的密码。
4. 首先，通过键入 df -h 确认没有可用磁盘空间，以检查可用磁盘空间量。

   您可以确认磁盘空间已被 Docker 占用。正常磁盘使用量应低于 2 GB。
5. 要查看 Docker 文件夹的磁盘使用情况，

执行 sudo du -h /var/lib/docker | sort -h.

您可以看到 Docker 文件夹的磁盘空间使用情况。

### 操作步骤

如果 Docker 文件夹的磁盘空间使用量快要满了，请在 Docker 配置文件中定义以下内容：

- 最大大小：在当前文件达到最大大小后强制执行日志轮换。
- 最大文件：在达到最大限制时删除多余的轮换日志文件。

请执行以下操作：

1. 执行 sudo vi /etc/docker/daemon.json。
2. 将以下行插入文件。

```
{
"log-driver": "json-file",
"log-opts": {"max-size": "100m", "max-file": "5" }
}
```

3. 按 ESC，然后键入 :wq!写入更改并关闭文件。

**注释** 您可以执行 sudo cat /etc/docker/daemon.json 来验证对文件所做的更改。

4. 执行 sudo systemctl restart docker 以重新启动 docker 文件。

   更改需要几分钟才能生效。您可以执行 sudo du -h /var/lib/docker | sort -h 以查看 docker 文件夹的更新磁盘使用情况。

5. 执行 df -h 以验证可用磁盘大小是否已增加。
6. 在 SDC 状态从“无法连通”(Unreachable) 变成“活动”(Active) 之前，您必须从 CDO 转到**服务 (Services)**页面中的“安全连接器”(Secure Connectors) 选项卡，然后从“操作”(Actions) 菜单中点击请求**重新连接 (Request Reconnect)**。

# 影响安全设备连接器的容器权限升级漏洞：cisco-sa-20190215-runc

思科产品安全事件响应团队 (PSIRT) 发布了安全公告 **cisco-sa-20190215-runc**，其中描述了 Docker 中的一个高严重性漏洞。阅读整个 PSIRT 团队公告，了解漏洞的完整说明。https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190215-runc

此漏洞会影响所有 CDO 客户：

- 使用 CDO 云部署的安全设备连接器 (SDC) 的客户无需执行任何操作，因为 CDO 运营团队已执行补救步骤。

- 使用本地部署的 SDC 的客户需要升级其 SDC 主机才能使用最新的 Docker 版本。他们可以按照以下说明执行此操作：
  - 更新 CDO 标准 SDC 主机，第 11 页
  - 更新自定义 SDC 主机，第 12 页
  - 缺陷跟踪，第 12 页

## 更新 CDO 标准 SDC 主机

如果您使用 CDO 映像部署了 SDC，请使用以下说明。 使用 CDO 的 VM 映像部署安全设备连接器

**步骤 1** 使用 SSH 或虚拟机监控程序控制台连接到 SDC 主机。

**步骤 2** 运行以下命令检查 Docker 服务的版本：

```
docker version
```

**步骤 3** 如果您运行的是最新的虚拟机 (VM)，您应该会看到如下输出：

```
 > docker version
Client:
     Version: 18.06.1-ce
     API version: 1.38
     Go version: go1.10.3
     Git commit: e68fc7a
     Built: Tue Aug 21 17:23:03 2018
     OS/Arch: linux/amd64
     Experimental: false
```

您可能会在这里看到旧版本。

**步骤 4** 运行以下命令以更新 Docker 并重新启动服务：

```
> sudo yum update docker-ce
> sudo service docker restart
```

**注释** 当 Docker 服务重新启动时，CDO 和您的设备之间会出现短暂的连接中断。

**步骤 5** 再次运行 docker version 命令。您应该会看到以下输出：

```
> docker version
Client:
    Version: 18.09.2
    API version: 1.39
    Go version: go1.10.6
    Git commit: 6247962
    Built: Sun Feb XX 04:13:27 2019
    OS/Arch: linux/amd64
    Experimental: false
```

**步骤 6** 大功告成。您现在已升级到 Docker 的最新版本并安装了补丁。

## 更新自定义 SDC 主机

如果您已创建自己的 SDC 主机，则需要按照说明根据 Docker 的安装方式进行更新。如果您使用的是 CentOS、yum 和 Docker-ce（社区版），则前面的程序将起作用。

如果您已安装 Docker-ee（企业版）或使用其他方法安装 Docker，则 Docker 的固定版本可能不同。您可以查看 Docker 页面以确定要安装的正确版本：Docker 安全更新和容器安全最佳实践。
https://blog.docker.com/2019/02/docker-security-update-cve-2018-5736-and-container-security-best-practices/

## 缺陷跟踪

思科将继续评估此漏洞，并将在获得更多信息时更新公告。公告被标记为最终版本后，您可以参考相关的思科漏洞了解更多详细信息：

CSCvo33929-CVE-2019-5736: runc container breakout

# 无效系统时间

Cisco Defense Orchestrator (CDO) 正在采用一种与安全设备连接器 (SDC) 进行通信的新方式。为此，CDO 必须在 2024 年 2 月 1 日之前将您现有的 SDC 迁移到新的通信方式。

**注释** 如果您的 SDC 在 2024 年 2 月 1 日之前未迁移，则 CDO 将无法再通过 SDC 与您的设备通信。

CDO 的运营团队尝试迁移您的 SDC 但未成功，因为您的 SDC 系统时间比 AWS 系统时间早或晚 15 分钟。

请按照以下步骤来更正系统时间问题。解决此问题后，我们将能够继续进行迁移。

**步骤 1** 通过 VM 终端或通过 SSH 连接登录到 SDC VM。

**步骤 2** 在提示符后，输入 `sudo sdc-onboard setup` 并进行身份验证。

**步骤 3** 现在，您将像第一次设置 SDC 一样回答 SDC 设置问题。重新输入与之前相同的所有密码和网络信息，但要特别注意 NTP 服务器地址：

a) 使用用于设置 SDC 的相同密码重置 root 和 cdo 用户密码。
b) 当系统提示时，输入 **y** 以重新配置网络。
c) 输入您之前输入的 IP 地址/CIDR 值。
d) 像以前一样输入网络网关的值。
e) 像以前一样输入 DNS 服务器的值。
f) 当系统提示您输入 NTP 服务器时，请务必提供有效的 NTP 服务器地址，例如 `time.aws.com`。
g) 查看您提供的值，如果正确，请输入 **y** 。

**步骤 4** 通过在提示符后输入 `date`，验证您的时间服务器是否可访问并与您的 SDC 同步。系统将显示 UTC 日期和时间，您可以将其与 SDC 时间进行比较。

### 下一步做什么

完成这些步骤后或遇到任何错误时，请联系思科技术支持中心 (TAC)。在成功完成这些步骤后，CDO 运营团队即可完成向新通信方法的 SDC 迁移。

# SDC 版本低于 202311****

Cisco Defense Orchestrator (CDO) 正在采用一种与安全设备连接器 (SDC) 进行通信的新方式。为此，CDO 必须在 2024 年 2 月 1 日之前将您现有的 SDC 迁移到新的通信方式。

**注释** 如果您的 SDC 在 2024 年 2 月 1 日之前未迁移，则 CDO 将无法再通过 SDC 与您的设备通信。

CDO 的运营团队尝试迁移您的 SDC 但未成功，因为您的租户运行的版本低于 202311****。

通过从 CDO 菜单栏**工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)** 导航，“安全连接器”(Secure Connectors) 页面上会列出 SDC 的当前版本。选择 SDC 后，可在屏幕右侧的**详细信息 (Details)** 窗格中找到其版本号。

请按照以下步骤升级 SDC 版本。问题一旦解决，CDO 操作人员将能够再次运行迁移过程。

**步骤 1** 登录到 SDC VM 并进行身份验证。

**步骤 2** 在提示符后，输入 `sudo su - sdc` 并进行身份验证。

**步骤 3** 在提示符处输入 `crontab -r`。

如果收到消息 `no crontab for sdc`，则可以将其忽略并移至下一步。

**步骤 4** 在提示符处输入 `./toolkit/toolkit.sh upgrade`。CDO 将确定您是否需要升级并对工具包进行升级。确保控制台中未报告任何错误。

**步骤 5** 验证 SDC 的新版本：

a) 登录 CDO。

b) 通过 CDO 菜单栏**工具和服务 (Tools & Services)** > **安全连接器 (Secure Connectors)** 导航到“安全连接器”(Secure Connectors) 页面。

c) 选择您的 SDC，然后点击**操作 (Actions)** 窗格中的**请求检测信号 (Request Heartbeat)**。

d) 验证 SDC 版本是否为 202311**** 或更高版本。

### 下一步做什么

完成这些步骤后或遇到任何错误时，请联系思科技术支持中心 (TAC)。成功完成这些步骤后，CDO 运营团队可以再次运行迁移过程。

# AWS 服务器的证书或连接错误

Cisco Defense Orchestrator (CDO) 正在采用一种与安全设备连接器 (SDC) 进行通信的新方式。为此，CDO 必须在 2024 年 2 月 1 日之前将您现有的 SDC 迁移到新的通信方式。

**注释** 如果您的 SDC 在 2024 年 2 月 1 日之前未迁移，则 CDO 将无法再通过 SDC 与您的设备通信。

CDO 的运营团队尝试迁移您的 SDC，但未成功，因为他们遇到了连接问题。

请按照以下步骤纠正连接问题。解决此问题后，我们将能够继续进行迁移。

**步骤 1** 创建允许在端口 443 上连接到您所在区域的域的防火墙规则：

- 美国地区的生产租户：
  - cognito-identity.us-west-2.amazonaws.com
  - cognito-idp.us-west-2.amazonaws.com
  - sns.us-west-2.amazonaws.com
  - sqs.us-west-2.amazonaws.com
- 欧盟地区的生产租户：
  - cognito-identity.eu-central-1.amazonaws.com
  - cognito-idp.eu-central-1.amazonaws.com
  - sns.eu-central-1.amazonaws.com
  - sqs.eu-central-1.amazonaws.com
- 亚太地区的生产租户：
  - cognito-identity.ap-northeast-1.amazonaws.com
  - cognito-idp.ap-northeast-1.amazonaws.com
  - sqs.ap-northeast-1.amazonaws.com
  - sns.ap-northeast-1.amazonaws.com

**步骤 2** 您可以使用以下命令之一确定需要添加到防火墙“允许列表”(allow list) 的 IP 地址的完整列表。

**注释** 以下命令适用于已安装 **jq** 的用户。IP 地址将显示在一个列表中。

- 美国地区的生产租户：

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select( (.service ==
"AMAZON" ) and .region == "us-west-2") | .ip_prefix'
```

- 欧盟地区的生产租户：

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select( (.service == "AMAZON" ) and .region == "eu-central-1") | .ip_prefix'
```

- 亚太地区的生产租户：

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] | select( (.service == "AMAZON" ) and .region == "ap-northeast-1") | .ip_prefix'
```

**注释** 如果您没有安装 **jq**，则可以使用此命令的简化版本：

```
curl -s https://ip-ranges.amazonaws.com/ip-ranges.json
```

---

### 下一步做什么

完成这些步骤后或遇到任何错误时，请联系思科技术支持中心 (TAC)。在成功完成这些步骤后，CDO 运营团队即可完成向新通信方法的 SDC 迁移。

# 安全事件连接器故障排除

如果这些场景都不符合您的情况，请通过思科技术支持中心提交支持案例。

# 安全事件连接器载入故障排除

这些故障排除主题介绍了与安全事件连接器 (SEC) 载入失败相关的许多不同症状。

### SEC 载入失败

**症状**：SEC 载入失败。

**修复**：删除 SEC 并重新载入。

如果收到此错误：

1. 从虚拟机容器中删除安全事件连接器及其文件。
2. 更新您的安全设备连接器。通常，SDC 会自动更新，您不必使用此程序，但此程序在故障排除的情况下非常有用。
3. 在 SDC 虚拟机上安装安全事件连接器。

**提示** 激活 SEC 时，请始终使用复制链接复制引导程序数据。

注释 如果此程序无法解决问题，请事件日志记录故障排除日志文件并联系您的托管服务提供商或思科技术支持中心。

### 未提供 SEC Bootstrap 数据

**消息**：错误，无法引导程序安全事件连接器，不提供引导程序数据，正在退出。(ERROR cannot bootstrap Secure Event Connector, bootstrap data not provided, exiting.)

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
Please input the bootstrap data from Setup Secure Event Connector page of CDO:
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector, bootstrap data not
provided, exiting.
```

**诊断**：系统提示时，Boostrap 数据未输入到设置脚本中。

**修复**：在载入时，如果提示输入引导程序数据，提供在 CDO UI 中生成的 SEC 引导程序数据。

### 引导程序配置文件不存在

**消息**：错误，无法为租户引导安全事件连接器：<tenant_name>，引导程序配置文件（“/usr/local/cdo/es_bootstrapdata”）不存在，正在退出。(ERROR Cannot bootstrap Secure Event Connector for tenant: <tenant_name>, bootstrap config file ("/usr/local/cdo/es_bootstrapdata") does not exist, exiting.)

**诊断**：SEC 引导程序数据文件（“/usr/local/cdo/es_bootstrapdata”）不存在。

**修复**：将 CDO UI 中生成的 SEC 引导程序数据放到文件 **/usr/local/cdo/es_bootstrapdata** 中，然后再次尝试载入。

1. 重复载入程序。
2. 复制引导程序日期。
3. 以“sdc”用户身份登录 SEC VM。
4. 将 CDO UI 中生成的 SEC 引导程序数据放到文件 **/usr/local/cdo/es_bootstrapdata** 中，然后再次尝试载入。

### 解码引导程序数据失败

**消息**：错误无法为租户引导安全事件连接器：<tenant_name>，未能解码 SEC Boostrap 数据，正在退出。(ERROR cannot bootstrap Secure Event Connector for tenant: <tenant_name>, faile to decode SEC boostrap data, exiting.)

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
base64: invalid input
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: tenant_XYZ,
 failed to decode SEC bootstrap data, exiting.
```

**诊断**：解码引导程序数据失败

**修复**：重新生成 SEC 引导程序数据，然后再次尝试载入。

### 引导程序数据没有载入 SEC 所需的信息

**消息：**

- 错误，无法为租户引导安全事件连接器容器，安全服务交换 FQDN 未设置，正在退出。
- 错误，无法为租户引导安全事件连接器容器，安全服务交换 OTP 未设置，正在退出。

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: 安全服务交换
 FQDN not set, exiting.
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: 安全服务交换
 FQDN not set, exiting.
```

**诊断：**引导程序数据没有载入 SEC 所需的信息

**修复：**重新生成 bootstrapdata，然后再次尝试载入。

### 当前正在运行的工具包 Cron

**消息：**错误，SEC 工具包已在运行，正在退出。(ERROR SEC toolkit already running, exiting.)

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
 [2020-06-10 04:37:26] ERROR SEC toolkit already running.
```

**诊断：** 工具包 cron 当前正在运行。

**修复：**再次重试载入命令。

### 没有足够的 CPU 和内存

**消息：**错误，无法设置安全事件连接器，需要至少 4 个 CPU 和 8 GB 内存，正在退出。(ERROR unable to setup Secure Event Connector, minimum 4 cpus and 8 GB ram required, exiting.)

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR unable to setup Secure Event Connector, minimum 4 cpus and 8
GB ram required, exiting.
```

**诊断：**没有足够的 CPU 和内存。

**修复：**确保至少为虚拟机上的 SEC 调配了 4 个 CPU 和 8 GB RAM，然后再次尝试载入。

### SEC 已在运行

**消息：**错误安全事件连接器已在运行，在载入新的安全事件连接器并退出之前执行“cleanup”。

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR Secure Event Connector already running, execute 'cleanup' before
 onboarding a new Secure Event Connector, exiting.
```

**诊断：**SEC 已在运行。

**修复：**在载入新的 SEC 之前运行 SEC 清理命令。

### SEC 域无法访问

**消息：**

- 未能连接到 api-sse.cisco.com:443；连接被拒绝 (Failed connect to api-sse.cisco.com:443; Connection refused)
- 错误，无法设置安全事件连接器，无法访问域 api-sse.cisco.com，正在退出。(ERROR unable to setup Secure Event Connector, domain api-sse.cisco.com unreachable, exiting.)

```
 [sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
curl: (7) Failed connect to api-sse.cisco.com:443; Connection refused
[2020-06-10 04:37:26] ERROR unable to setup Secure Event Connector, domain api-sse.cisco.com
 unreachable, exiting.
```

**诊断**：SEC 域不可达

**修复**：确保本地 SDC 具有互联网连接，然后再次尝试载入。

#### 载入 SEC 命令成功且未出错，但 SEC docker 容器未启动

**症状**：载入 SEC 命令成功且未出错，但 SEC docker 容器未启动

**诊断**：载入 SEC 命令成功且未出错，但 SEC docker 容器未启动

**修复**：

1. 以“sdc”用户身份登录 SEC。
2. 检查 SEC docker 容器启动日志中是否存在任何错误 (/usr/local/cdo/data/<tenantDir>/event_streamer/logs/startup.log)。
3. 如果是，请运行 SEC 清理命令，然后再次尝试载入。

#### 联系 CDO 支持人员

如果这些场景都不符合您的情况，请通过思科技术支持中心提交支持案例。

# 安全事件连接器注册失败故障排除

**症状**：向云事件服务注册思科安全事件连接器失败。

**诊断**：这些是 SEC 无法注册到事件云服务的最常见原因。

- **SEC 无法从 SEC 访问 Eventing 云服务**

  修复：确保可在端口 443 上访问互联网，并且 DNS 配置正确。

- **由于 SEC bootstrapdata 中的一次性密码无效或过期，注册失败**

  修复：

---

**步骤 1** 以“sdc”用户身份登录 SDC。

**步骤 2** 查看连接器日志：( /usr/local/cdo/data/<tenantDir>/event_streamer/logs/connector.log ) 以检查注册状态。

如果注册因令牌无效而失败，您将在日志文件中看到类似于以下内容的错误消息。

**context:(*contextImpl).handleFailed] registration - CE2001：注册失败 - 因无效令牌，注册设备失败。请使用新的有效令牌重试。- 失败"**

**步骤 3** 在 SDC VM 上运行 SEC 清理命令步骤，从“安全连接器”(Secure Connectors) 页面删除 SEC。

**步骤 4** 生成新的 SEC 引导程序数据，然后重试 SEC 激活步骤。

# 使用安全和分析日志记录事件排除网络问题

以下是使用事件查看器排除网络问题的基本框架。

此场景假设您的网络运营团队收到报告，指出用户无法访问网络上的资源。根据报告问题的用户及其位置，网络运营团队可以合理地了解哪个防火墙控制其对资源的访问。

**Note** 此场景还假设 FDM 管理 设备是管理网络流量的防火墙。安全分析和日志记录不会从其他设备类型收集日志记录信息。

**步骤 1** 在导航窗格中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。

**步骤 2** 点击**历史 (Historical)** 选项卡。

**步骤 3** 按**时间范围 (Time Range)** 开始过滤事件。默认情况下，“历史”(Historical) 选项卡显示最近一小时的事件。如果这是正确的时间范围，请输入当前日期和时间作为**结束**时间。如果该时间范围不正确，请输入包含所报告问题时间的开始和结束时间。

**步骤 4** 在**传感器 ID (Sensor ID)** 字段中输入您怀疑控制用户访问的防火墙的 IP 地址。如果可能是多个防火墙，请使用搜索栏中的 **attribute:value** 对过滤事件。输入两个条目并将其与 OR 语句组合在一起。例如：`SensorID:192.168.10.2 OR SensorID:192.168.20.2`。

**步骤 5** 在事件过滤器栏中的**源 IP (Source IP)** 字段中输入用户的 IP 地址。

**步骤 6** 如果用户无法访问资源，请尝试在**目标 IP (Destination IP)** 字段中输入该资源的 IP 地址。

**步骤 7** 展开结果中的事件并查看其详细信息。以下是一些需要查看的详细信息：

- **AC_RuleAction** - 触发规则时采取的操作（允许、信任、阻止）。
- **FirewallPolicy** - 触发事件的规则所在的策略。
- **FirewallRule** - 触发事件的关联规则的名称。如果值为“默认操作”(Default Action)，则触发事件的是策略的默认操作，而不是策略中的某个规则。
- **UserName** - 与发起方 IP 地址关联的用户。发起方 IP 地址与源 IP 地址相同。

**步骤 8** 如果规则操作阻止访问，请查看 FirewallRule 和 FirewallPolicy 字段，以确定策略中阻止访问的规则。

# NSEL 数据流故障排除

配置 Netflow 安全事件日志记录 (NSEL) 后，请使用以下程序验证 NSEL 事件是否从 ASA 发送到思科云以及思科云是否正在接收这些事件。

请注意，一旦 ASA 被配置为将 NSEL 事件发送到安全事件连接器 (SEC)，然后再发送到思科云，数据不会立即流动。假设 ASA 上生成了与 NSEL 相关的流量，第一个 NSEL 数据包可能需要几分钟才能到达。

**Note** 此工作流程向您展示如何直接使用“flow-export counters”命令和“capture”命令对 NSEL 数据流进行故障排除。有关这些命令用法的更详细讨论，请参阅《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》中的“数据包捕获”和《思科 ASA NetFlow 实施指南》中的“监控 NSEL”。

执行这些任务：

- 验证 NetFlow 数据包是否正在发送到 SEC
- 验证思科云是否正在接收 NetFlow 数据包

# 事件日志记录故障排除日志文件

安全事件连接器 (SEC) troubleshoot.sh 收集所有事件流传输器日志，并将其压缩到单个 .tar.gz 文件中。

使用以下程序创建 comparessed.tar.gz 文件并解压缩该文件：

1. 运行故障排除脚本，第 25 页。
2. 解压缩 sec_troubleshoot.tar.gz 文件，第 26 页。

## 运行故障排除脚本

安全事件连接器 (SEC) troubleshoot.sh 收集所有事件流传输器日志，并将其压缩到单个 .tar.gz 文件中。请按照以下程序运行 Troubleshooting.sh 脚本：

**步骤 1** 打开 VM 虚拟机监控程序并启动安全设备连接器 (SDC) 的控制台会话。

**步骤 2** 登录并切换到 **root** 用户：

```
[cdo@localhost ~]$sudo su root
```

**Note** 您也可以切换到 sdc 用户，但作为根用户，您还将收到 IP 表信息。IP 表信息显示防火墙正在设备上运行，并且所有防火墙路由。如果防火墙阻止安全事件连接器 TCP 或 UDP 端口，事件将不会显示在事件日志记录表中。IP 表将帮助您确定是否属于这种情况。

**步骤 3** 在提示符后，运行故障排除脚本并指定租户名称。以下是命令语法：

```
[root@localhost ~]$ /usr/local/cdo/toolkit/troubleshoot.sh --app sec --tenant CDO_[tenant_name]
```

以下为输出示例：

```
[root@localhost ~]$ /usr/local/cdo/toolkit/troubleshoot.sh --app sec --tenant CDO_example_tenant
```

在命令输出中，您会看到 sec_troubleshoot 文件存储在 SDC 上的 **/tmp/troubleshoot** 目录中。文件名遵循约定 **sec_troubleshoot-*timestamp*.tar.gz.**

**步骤 4** 要检索文件，请以 CDO 用户身份登录并使用 SCP 或 SFTP 下载文件。

以下为输出示例：

```
[root@localhost troubleshoot]# scp sec_troubleshoot-timestamp.tar.gz
root@server-ip:/scp/sec_troubleshoot-timestamp.tar.gz
```

### What to do next

请继续解压缩 sec_troubleshoot.tar.gz 文件, on page 26。

## 解压缩 sec_troubleshoot.tar.gz 文件

安全事件连接器 (SEC) 运行故障排除脚本 脚本收集所有事件流传输器日志，并将其压缩到一个 sec_troubleshoot.tar.gz 文件中。按照此程序解压缩 sec_troubleshoot.tar.gz 文件。

1. 打开 VM 虚拟机监控程序并启动安全设备连接器 (SDC) 的控制台会话。
2. 登录并切换到 **root** 用户：

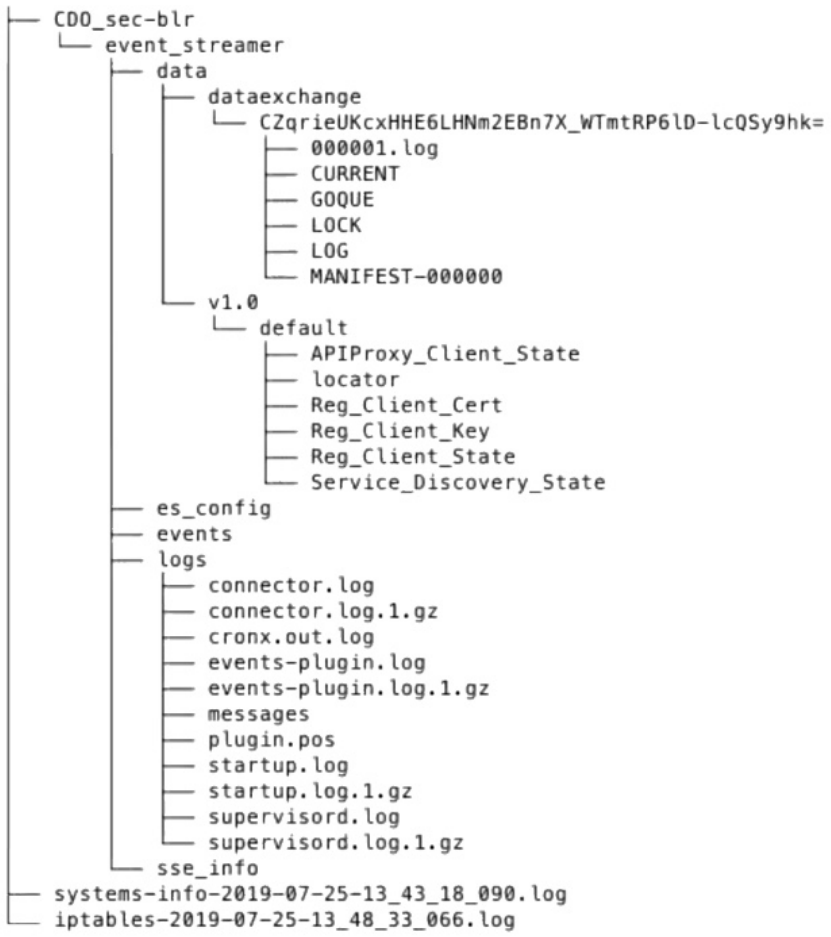
   ```
   [cdo@localhost ~]$sudo su root
   ```

**Note** 您也可以切换到 **sdc** 用户，但作为根用户，您还将收到 IP 表信息。IP 表信息显示防火墙正在设备上运行，并且所有防火墙路由。如果防火墙阻止安全事件连接器 TCP 或 UDP 端口，事件将不会显示在事件日志记录表中。IP 表将帮助您确定是否属于这种情况。

3. 在提示符后，键入以下命令：

   ```
   [root@localhost ~]$ tar xvf sec_troubleshoot-timestamp.tar.gz
   ```

日志文件存储在以租户命名的目录中。这些是存储在 sec_troubelshoot-timestamp.tar.gz 文件中的日志类型。如果您以 root 用户身份收集所有日志文件，则包括 iptables 文件。




# 生成 SEC 引导程序数据失败。

症状：在 CDO 中生成 SEC 引导程序数据时，“引导程序生成”步骤失败并显示错误：“获取引导程序数据时出错。请重试。"

修复：再次重试引导程序数据生成。如果仍然失败，请联系 CDO 支持。CDO 客户如何通过 TAC 提交支持请求

# 载入后，CDO 安全连接器页面中的 SEC 状态为“非活动”

症状：由于以下原因之一，CDO 安全连接器页面中的安全事件连接器状态显示为“非活动”：

- 心跳失败
- 连接器注册失败

**修复：**

- 心跳失败：请求 SEC 心跳并刷新“安全连接器”页面，以查看状态是否更改为“活动”，如果未更改，请检查安全设备连接器注册是否失败。

- **连接器注册失败**：请参阅问题 安全事件连接器注册失败故障排除。

# SEC 处于“在线”状态，但 CDO 事件日志记录页面中没有事件

症状：安全事件连接器在 CDO 安全连接器页面中显示“活动”，但在 CDO 事件查看器中看不到事件。

解决方案或解决方法：

**步骤 1** 以“sdc”用户身份登录到本地 SDC 的虚拟机。在提示符后，键入 **sudo su - sdc**。

**步骤 2** 执行以下检查：

- 查看 SEC 连接器日志 ( /usr/local/cdo/data/<tenantDir>/event_streamer/logs/connector.log ) 并确保 SEC 注册已成功。如未成功，请参阅问题“安全事件连接器注册失败故障排除”。
- 检查 SEC 事件日志 ( /usr/local/cdo/data/<tenantDir> /event_streamer/logs/events-plugin.log）并确保事件正在处理。否则，请联系 CDO 支持。
- 登录到 SEC docker 容器并执行命令“supervisorctl -c /opt/cssp/data/conf/supervisord.conf”，并确保输出如下所示，并且所有进程都处于 RUNNING 状态。否则，请联系 CDO 支持。

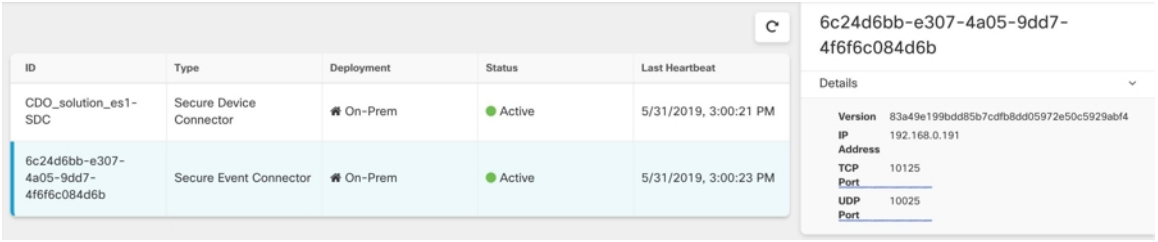
**estreamer-connector RUNNING pid 36, uptime 5:25:17**

**estreamer-cron RUNNING pid 39, uptime 5:25:17**

**estreamer-plugin RUNNING pid 37, uptime 5:25:17**

**estreamer-rsyslog RUNNING pid 38, uptime 5:25:17**

- 确保本地 SDC 上的防火墙规则未阻止“安全连接器”(Secure Connectors) 页面上为 SEC 显示的 UDP 和 TCP 端口。要确定需要打开的端口，请参阅查找用于思科安全分析和日志记录的设备 TCP、UDP 和 NSEL 端口。




- 如果您使用自己的 CentOS 7 虚拟机手动设置了 SDC，并将防火墙配置为阻止传入请求，则可以执行以下命令来取消阻止 UDP 和 TCP 端口：

**firewall-cmd --zone=public --add-port=<udp_port> /udp --permanent**

**firewall-cmd --zone=public --add-port=<tcp_port> /tcp --permanent**

**firewall-cmd --reload**

- 使用您选择的 Linux 网络工具，检查是否在这些端口上接收数据包。如果未收到，请重新检查 FTD 日志记录配置。

如果上述修复方法均无效，请向 CDO 支持人员提交支持请求。 CDO 客户如何通过 TAC 提交支持请求。

# SEC 清理命令

安全事件连接器 (SEC) 清理命令可从安全设备连接器 (SDC) 虚拟机中删除 SEC 容器及其关联的文件。您可以在 安全事件连接器注册失败故障排除, on page 23 或载入失败的情况下运行此命令。

运行命令：

### Before you begin

要执行此任务，您需要知道租户的名称。要查找租户名称，请在CDO中打开用户菜单，然后点击**设置 (Settings)**。向下滚动页面以找到您的**租户名称 (Tenant Name)**。

**步骤 1** 以 `sdc` 用户身份登录 SDC。在提示符后，键入 `sudo su - sdc`。

**步骤 2** 连接到 `/usr/local/cdo/toolkit` 目录。

**步骤 3** 运行 `sec.sh remove`*`tenant_name`* 并确认您打算删除 SEC。

示例：

```
 [sdc@localhost~]$ /usr/local/cdo/toolkit/sec.sh remove tenant_XYZ
Are you sure you want to remove Secure Event Connector for tenant tenant_XYZ? (y/n): y
```

### What to do next

如果此命令无法删除 SEC，请继续执行 SEC 清理命令失败, on page 29：

# SEC 清理命令失败

如果 SEC 清理命令, on page 29 失败，请使用此程序。

**消息**：找不到 SEC，正在退出。

**症状**：清理 SEC 命令无法清理现有 SEC。

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh remove tenant_XYZ Are you sure you want
to remove Secure Event Connector for tenant tenant_XYZ? (y/n): y [2020-06-10 04:50:42] SEC
 not found, exiting.
```

**修复**： 当清理命令失败时，手动清理安全事件连接器。

删除已在运行的 SEC docker 容器：

**步骤 1** 以“sdc”用户身份登录 SDC。在提示符后，键入 `sudo su - sdc`。

**步骤 2** 运行 **docker ps** 命令以查找 SEC 容器的名称。SEC 名称的格式为“es_ *name*”。

**步骤 3** 运行 **docker stop** 命令以停止 SEC 容器。

**步骤 4** 运行 **rm** 命令以删除 SEC 容器。

**例如：**

```
$ docker stop <SEC_docker_container_name>
$ docker rm <SEC_docker_container_name>
```

# 使用运行状况检查了解安全事件连接器的状态

安全事件连接器 (SEC) 运行状况检查脚本提供有关 SEC 状态的信息。

请按照以下程序运行运行状况检查：

**步骤 1** 打开 VM 监控程序并启动安全设备连接器 (SDC) 的控制台会话。

**步骤 2** 以“cdo”用户身份登录 SDC。

**步骤 3** 切换到“sdc”用户：

```
[cdo@tenant]$sudo su sdc
```

**步骤 4** 在提示符后，运行 healthcheck.sh 脚本并指定租户名称：

```
[sdc@host ~]$ /usr/local/cdo/toolkit/healthcheck.sh --app sec --tenant CDO_[tenant_name]
```

例如：

```
[sdc@host ~]$ /usr/local/cdo/toolkit/healthcheck.sh --app sec --tenant CDO_example_tenant
```

脚本的输出提供以下信息：

```
================================================
Running SEC health check for tenant [redacted]
------------------------------------------------
SEC cloud URL [redacted] is: Reachable
------------------------------------------------
SEC Connector status: Active
------------------------------------------------
SEC Events Plugin is: Running
SEC UDP syslog server is: Running
SEC TCP syslog server is: Running
------------------------------------------------
SEC send sample event: Success. Please search with filter "sensorID:127.0.0.1" to locate the event in CDO events viewer page.
================================================
```

运行状况检查输出的值：

- **SEC 云 URL**：显示 CDO 云 URL 以及 SEC 是否可以访问 CDO。
- **SEC 连接器**：如果 SEC 连接器已正确载入并启动，则会显示“正在运行”(Running)。
- **SEC UDP 系统日志服务器**：如果 UDP 系统日志服务器已准备好发送 UDP 事件，则显示“正在运行”。
- **SEC TCP 系统日志服务器**：如果 TCP 系统日志服务器已准备好发送 TCP 事件，将显示“正在运行”。
- **SEC 连接器状态**：如果 SEC 正在运行并已载入到 CDO，则会显示为“活动”(Active)。

- **SEC 发送示例事件**：如果在运行状况检查结束时，所有状态检查均为“绿色”，则该工具会发送示例事件。（如果有任何进程“关闭”，则工具会跳过发送测试事件。）示例事件在事件日志中显示为名为“sec-health-check” 的策略。

# 对思科防御协调器进行故障排除

## 登录失败故障排除

**登录失败，因为您无意中登录到错误的 CDO 区域**

请确保您登录的是适当的 CDO 区域。登录 https://sign-on.security.cisco.com 后，您可以选择要访问的区域。点击 **CDO** 磁贴访问 Defenseorchestrator.com 或点击 **CDO (EU)** 访问 Defenseorchestrator.eu。

## 迁移后的登录失败故障排除

**由于用户名或密码不正确，CDO 登录失败**

**解决方法** 如果您尝试登录 CDO，并且知道您使用的是正确的用户名和密码，但登录失败，或者您尝试“忘记密码”无法恢复有效的密码，则您可能已尝试在未创建新 Cisco Security Cloud Sign On 帐户的情况下进行登录，则您需要按照创建新的 Cisco Security Cloud Sign On 账户并配置 Duo 多因素身份验证中的说明注册新的 Cisco Security Cloud Sign On 帐户。

**登录到 Cisco Security Cloud Sign On 控制面板成功，但您无法启动 CDO**

**解决方法** 您可能使用与 CDO 租户不同的用户名创建了 Cisco Security Cloud Sign On 账户。请联系思科技术支持中心 (TAC)，以规范 CDO 和 Cisco Secure Sign-On 之间的用户信息。

**使用保存的书签登录失败**

**解决方法** 您可能正在尝试使用浏览器中保存的旧书签登录。书签可能指向 https://cdo.onelogin.com。https://cdo.onelogin.com/

**解决方法** 登录 https://sign-on.security.cisco.com。

- **解决方法** 如果您尚未创建 Cisco Secure Sign-On 账户，请创建一个账户。创建新的 Cisco Security Cloud Sign On 账户并配置 Duo 多因素身份验证
- **解决方法** 如果您已创建新账户，请点击控制面板上与 思科防御协调器（美国）、思科防御协调器（欧盟）或 思科防御协调器（亚太地区）对应的 CDO 磁贴
- **解决方法** 将书签更新为指向 https://sign-on.security.cisco.com。https://sign-on.security.cisco.com/

# 访问和证书故障排除

## 使用 CDO 排除用户访问故障

考虑用户被拒绝访问他们应该有权访问的资源的情况。以下是您可以用来诊断和补救该问题的方法。

**步骤 1** 用户通知您的安全团队其对资源的访问已被阻止。确定通常如何访问该资源。它的 IP 地址是什么？您是否在特定端口上访问它？使用哪种协议向资源发送信息？

**步骤 2** 在**设备和服务 (Devices & Services)** 页面上，点击**设备 (Devices)** 选项卡。

**步骤 3** 点击 FTD 选项卡，选择 ASA 并运行数据包跟踪器。有关详细说明，请参阅 ASA 数据包跟踪器。

**步骤 4** 检查数据包跟踪表，了解可能已拒绝访问资源的规则。

**步骤 5** 确定拒绝访问的规则后，在CDO中创建一个更改请求标签并启用它。请参阅更改请求管理。这将帮助您在更改日志中识别您为允许访问资源所做的更改。

**步骤 6** 从 CDO 编辑规则以更正行为。您的 ASA 现在与 CDO 不同步。

**步骤 7** 从设备和服务页面将更改部署到 ASA。CDO 通过保存在 ASA 上的配置来跟踪数据包，而不是在 CDO 上暂存的配置。请注意，您还会将在 CDO 上暂存的任何其他配置更改部署到 ASA。

**步骤 8** 重新运行数据包跟踪器，以确定策略更改是否提供所需的结果。确认您的用户现在有权访问资源。

**步骤 9** 假设您的用户现在具有访问权限，请清除CDO中的更改请求标签。这可以防止不相关的活动与此修复程序关联。

**Note** 如果您所做的更改不能解决问题或产生了一些新问题，并且您想要恢复到以前的配置，则可以恢复ASA配置。请参阅恢复 ASA 配置。

## 解析检测到的新指纹状态

**步骤 1** 在导航栏中，点击 **设备和服务**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击适当的设备类型选项卡。

**步骤 4** 选择处于检测到**新指纹状态**的设备。

**步骤 5** 点击检测到的新指纹窗格中的**查看指纹**。

**步骤 6** 当系统提示您查看并接受指纹时：

**a.** 点击**下载指纹**并进行查看。

**b.** 如果您对指纹满意，请点击**接受**。如果不是，请点击**取消**。

**步骤 7** 解决新的指纹问题后，设备的连接状态可能会显示为**在线**，而配置状态可能会显示“未同步”或“检测到冲突”。回顾解决配置冲突 (Resolve Configuration Conflicts) 以查看和解决 CDO 与设备之间的配置差异。

## 使用安全和分析日志记录事件排除网络问题

以下是使用事件查看器排除网络问题的基本框架。

此场景假设您的网络运营团队收到报告，指出用户无法访问网络上的资源。根据报告问题的用户及其位置，网络运营团队可以合理地了解哪个防火墙控制其对资源的访问。

**Note** 此场景还假设 FDM 管理 设备是管理网络流量的防火墙。安全分析和日志记录不会从其他设备类型收集日志记录信息。

**步骤 1** 在导航窗格中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。

**步骤 2** 点击**历史 (Historical)** 选项卡。

**步骤 3** 按**时间范围 (Time Range)** 开始过滤事件。默认情况下，“历史”(Historical) 选项卡显示最近一小时的事件。如果这是正确的时间范围，请输入当前日期和时间作为**结束**时间。如果该时间范围不正确，请输入包含所报告问题时间的开始和结束时间。

**步骤 4** 在**传感器 ID (Sensor ID)** 字段中输入您怀疑控制用户访问的防火墙的 IP 地址。如果可能是多个防火墙，请使用搜索栏中的 **attribute:value** 对过滤事件。输入两个条目并将其与 OR 语句组合在一起。例如：`SensorID:192.168.10.2 OR SensorID:192.168.20.2`。

**步骤 5** 在事件过滤器栏中的**源 IP (Source IP)** 字段中输入用户的 IP 地址。

**步骤 6** 如果用户无法访问资源，请尝试在**目标 IP (Destination IP)** 字段中输入该资源的 IP 地址。

**步骤 7** 展开结果中的事件并查看其详细信息。以下是一些需要查看的详细信息：

- **AC_RuleAction** - 触发规则时采取的操作（允许、信任、阻止）。
- **FirewallPolicy** - 触发事件的规则所在的策略。
- **FirewallRule** - 触发事件的关联规则的名称。如果值为“默认操作”(Default Action)，则触发事件的是策略的默认操作，而不是策略中的某个规则。
- **UserName** - 与发起方 IP 地址关联的用户。发起方 IP 地址与源 IP 地址相同。

**步骤 8** 如果规则操作阻止访问，请查看 FirewallRule 和 FirewallPolicy 字段，以确定策略中阻止访问的规则。

## SSL 解密问题故障排除

### 处理解密重签名适用于浏览器而非应用的 Web 站点（SSL 或证书颁发机构锁定）

智能手机和其他设备的某些应用使用 SSL（或证书颁发机构）锁定技术。SSL 锁定技术将原始服务器证书的散列值嵌入到应用本身内部。因此，当应用收到来自 Firepower Threat Defense设备的重签证书时，散列验证会失败并中止连接。

主要表现是，用户使用站点应用无法连接到网站，但可以使用网络浏览器连接，即使在应用无法正常工作的同一台设备上使用浏览器也可以连接。例如，用户不能使用 Facebook iOS 或 Android 应用，但可以通过 https://www.facebook.com 转至 Safari 或 Chrome，进行成功连接。

由于 SSL 锁定专用于避免中间人攻击，因此此问题无法解决。必须从以下选项中选择一项：

**更多详细信息**

如果站点在浏览器中可用，但不能在同一设备的应用中使用，几乎可以肯定这是一个 SSL 锁定实例。但是，如果您想要更深入地挖掘，除了浏览器测试之外，还可以使用连接事件确定 SSL 锁定。

应用可能会通过两种方式处理散列验证失败：

- 第 1 组应用，例如 Facebook，从服务器收到 SH、CERT、SHD 消息后立即发送 SSL 警告消息。警告通常是一个表示 SSL 锁定的“Unknown CA (48)” 警告。紧接着警告消息发送 TCP 重置。在事件详细信息中，您应看到以下现象：
  - SSL 流标志包括 ALERT_SEEN。
  - SSL 流标志不包括 APP_DATA_C2S 或 APP_DATA_S2C。
  - SSL 流消息通常是：CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE。
- 第 2 组应用，例如 Dropbox，不会发送任何警告。而是，等到完成握手后发送 TCP 重置。在事件中，您应看到以下现象：
  - SSL 流标志不包括 ALERT_SEEN、APP_DATA_C2S 或 APP_DATA_S2C。
  - SSL 流消息通常是：CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE、CLIENT_KEY_EXCHANGE、CLIENT_CHANGE_CIPHER_SPEC、CLIENT_FINISHED、SERVER_CHANGE_CIPHER_SPEC、SERVER_FINISHED。

# 迁移后的登录失败故障排除

**由于用户名或密码不正确，CDO 登录失败**

**解决方法** 如果您尝试登录 CDO，并且知道您使用的是正确的用户名和密码，但登录失败，或者您尝试“忘记密码”无法恢复有效的密码，则您可能已尝试在未创建新 Cisco Security Cloud Sign On 帐户的情况下进行登录，则您需要按照创建新的 Cisco Security Cloud Sign On 账户并配置 Duo 多因素身份验证中的说明注册新的 Cisco Security Cloud Sign On 帐户。

**登录到 Cisco Security Cloud Sign On 控制面板成功，但您无法启动 CDO**

**解决方法** 您可能使用与 CDO 租户不同的用户名创建了 Cisco Security Cloud Sign On 账户。请联系思科技术支持中心 (TAC)，以规范 CDO 和 Cisco Secure Sign-On 之间的用户信息。

**使用保存的书签登录失败**

**解决方法** 您可能正在尝试使用浏览器中保存的旧书签登录。书签可能指向 https://cdo.onelogin.com。https://cdo.onelogin.com/

**解决方法** 登录 https://sign-on.security.cisco.com。

- **解决方法** 如果您尚未创建 Cisco Secure Sign-On 账户，请创建一个账户。创建新的 Cisco Security Cloud Sign On 账户并配置 Duo 多因素身份验证
- **解决方法** 如果您已创建新账户，请点击控制面板上与 思科防御协调器（美国）、思科防御协调器（欧盟）或 思科防御协调器（亚太地区）对应的 CDO 磁贴
- **解决方法** 将书签更新为指向 https://sign-on.security.cisco.com。https://sign-on.security.cisco.com/

# 对象故障排除

## 解决重复对象问题

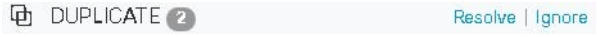
重复对象 是指同一设备上具有不同名称但值相同的两个或多个对象。这些对象通常是意外创建的，可用于类似的目的，并供不同的策略使用。解决重复对象问题后，CDO 会使用保留的对象名称来更新所有受影响的对象引用。

要解决重复对象问题，请执行以下操作：

**步骤 1** 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

**步骤 2** 然后过滤对象以查找重复的对象问题。

**步骤 3** 选择其中一个结果。在对象详细信息面板中，您将看到“重复”(DUPLICATE) 字段以及受影响的重复项数：




**步骤 4** 点击**解决**。CDO 会显示要比较的重复对象。

**步骤 5** 选择两个要比较的对象。

**步骤 6** 您现在有以下选项：

- 如果要将其中一个对象替换为另一个对象，请点击要保留的对象的**选择 (Pick)**，点击**解决 (Resolve)** 以查看将受到影响的设备和网络策略，如果对更改满意，请点击**确认 (Confirm)**。CDO 会保留您选择替换的对象，同时删除重复项。
- 如果列表中有要忽略的对象，请点击**忽略 (Ignore)**。如果您忽略某个对象，它就会从 CDO 显示的重复对象列表中删除。
- 如果要保留对象，但又不希望 CDO 在搜索重复对象时找到该对象，请点击**全部忽略 (Ignore All)**。

**步骤 7** 一旦解决重复对象问题，请查看并部署您现在所做的更改，或者等待并一次部署多个更改。

## 解决未使用的对象问题

未使用的对象 是设备配置中存在但未被其他对象、访问列表或 NAT 规则引用的对象。

**相关信息：**

- 导出设备和服务列表

- 将设备批量重新连接到 CDO

## 解决未使用的对象问题

**步骤 1** 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

**步骤 2** 然后过滤对象以查找未使用的对象问题。

**步骤 3** 选择一个或多个未使用的对象。

**步骤 4** 您现在有以下选项：

- 在操作窗格中，点击**删除 (Remove)** 以从 CDO 中删除未使用的对象。
- 在问题窗格中，点击**忽略 (Ignore)**。如果您忽略某个对象，CDO 将停止在未使用的对象的结果中显示该对象。

**步骤 5** 如果您删除了未使用的对象、 预览和部署所有设备的配置更改 您现在所做的更改，或者等待并一次部署多个更改。

**Note** 要批量解决未使用的对象问题，请参阅批量解决对象问题。

## 批量删除未使用的对象

**步骤 1** 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

**步骤 2** 然后过滤对象以查找未使用的对象问题。

**步骤 3** 选择要删除的未使用对象：

- 点击对象表头行中的复选框，以便选择页面上的所有对象。
- 在对象表中选择单个未使用的对象。

**步骤 4** 在“操作”(Actions) 窗格中，点击**删除 (Remove)** 以删除在 CDO 中选定的所有未使用的对象。一次可以删除 99 个对象。

**步骤 5** 点击**确定 (OK)** 以确认您要删除未使用的对象。

**步骤 6** 您有两种选择来部署这些更改：

- 查看并部署您现在所做的更改，或者等待并一次部署多个更改。
- 打开**清单 (Inventory)** 页面并查找受更改影响的设备。选择受更改影响的所有设备，然后在管理窗格中点击**全部部署**。阅读警告并采取适当的措施。

# 解决不一致的对象问题

不一致对象  是指两台或多台设备上具有相同名称但值不同的对象。有时，用户会在不同的配置中创建具有相同名称和内容的对象，但随着时间的推移，这些对象的值会出现分歧，从而造成不一致。

**注意**：要批量解决不一致的对象问题，请参阅批量解决对象问题。

您可以对不一致的对象执行以下操作：

- **忽略**：CDO 忽略对象之间的不一致并保留其值。对象将不再列在不一致类别下。
- **合并**：CDO 将所有选定对象及其值合并到一个对象组中。
- **重命名**：CDO 允许您重命名其中一个不一致的对象并为其指定新名称。
- **将共享网络对象转换为覆盖**：CDO 允许您将不一致的共享对象（有或没有覆盖）合并为一个具有覆盖的共享对象。不一致对象中最常见的默认值设置为新形成的对象中的默认值。

**Note** 如果有多个通用默认值，则选择其中一个作为默认值。其余默认值和覆盖值设置为该对象的覆盖。

- **将共享网络组转换为其他值**： - CDO 允许您将不一致的共享网络组合并为具有其他值的单个共享网络组。此功能的条件是，要转换的不一致网络组必须至少有一个具有相同值的通用对象。与此条件匹配的所有默认值都将成为默认值，其余对象将作为新形成的网络组的其他值进行分配。

  例如，请考虑两个不一致的共享网络组。第一个网络组“shared_network_group”由“object_1”（192.0.2.x）和“object_2”（192.0.2.y）组成。它还包含附加值“object_3”(192.0.2.a)。第二个网络组“shared_network_group”由“object_1”(192.0.2.x) 和附加值“object_4”(192.0.2.b) 组成。将共享网络组转换为其他值时，新形成的组“shared_network_group”包含默认值“object_1”(192.0.2.x) 和“object_3”(192.0.2.y)”。 2.a) 和 'object_4' (192.0.2.b) 作为附加值。

**Note** 当您创建新的网络对象时，CDO 会自动将其值作为覆盖分配给具有相同名称的现有共享网络对象。这也适用于将新设备载入 CDO 的情况。

仅当满足以下条件时才会进行自动分配：

1. 必须将新网络对象分配给设备。
2. 租户中只能存在一个具有相同名称和类型的共享对象。
3. 共享对象必须已包含覆盖。

要解决不一致的对象问题，请执行以下操作：

**步骤 1** 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

**步骤 2** 然后过滤对象以查找不一致的对象问题。

**步骤 3** 选择不一致的对象。在对象详细信息面板中，您将看到包含受影响对象数量的不一致字段：

**步骤 4** 点击**解决**。CDO 显示不一致的对象以供比较。

**步骤 5** 您现在有以下选项：

- **全部忽略**：
  a. 比较显示的对象，然后在其中一个对象上点击**忽略 (Ignore)**。或者，要忽略所有对象，请点击**全部忽略 (Ignore All)**。
  b. 点击**确定 (OK)**以进行确认。
- **通过合并对象来解决**：
  a. 点击**通过合并 X 对象来解决 (Resolve by Merging X Objects)**。
  b. 点击**确认 (Confirm)**。
- **重命名**：
  a. 点击**重命名**。
  b. 保存对受影响的网络策略和设备所做的更改，然后点击**确认 (Confirm)**。
- **转换为覆盖（对于不一致的共享对象）**：将共享对象与覆盖进行比较时，比较面板仅显示**不一致的值 (Inconsistent Values)** 字段中的默认值。
  a. 点击**转换为覆盖 (Convert to Overrides)**。所有不一致的对象都将转换为具有覆盖的单个共享对象。
  b. 点击**确认 (Confirm)**。您可以点击**编辑共享对象 (Edit Shared Object)** 以查看新创建的对象的详细信息。您可以使用向上和向下箭头在默认值和覆盖之间移动值。
- **转换为其他值（对于不一致的网络组）**：
  a. 点击**转换为其他值 (Convert to Additional Values)**。所有不一致的对象都将转换为具有其他值的单个共享对象。
  b. 保存对受影响的网络策略和设备所做的更改，然后点击**确认 (Confirm)**。

**步骤 6** 解决不一致问题后，请立即查看并部署所做的更改，或者等待并立即部署多个更改。

## 批量解决对象问题

解决具有解决未使用的对象问题、解决重复对象问题或 解决不一致的对象问题, on page 37 问题的对象的方法之一是忽略它们。您可以选择并忽略多个对象，即使对象表现出多个问题也是如此。例如，如果对象既不一致又未使用，则一次只能忽略一种问题类型。

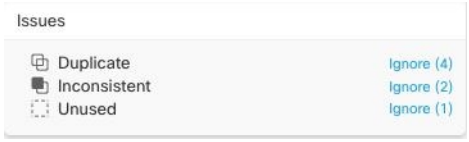
**Important** 如果该对象稍后与其他问题类型关联，则您提交的忽略操作仅影响您当时选择的问题。例如，如果您忽略某个对象，因为它是重复的，并且该对象后来被标记为不一致，则将其忽略为重复对象并不意味着它将作为不一致的对象被忽略。

要批量忽略问题，请执行以下程序：

**步骤 1** 在左侧的 CDO 导航栏中，点击**对象 (Objects)**并选择一个选项。

**步骤 2** 要缩小搜索范围，您可以过滤对象问题。

**步骤 3** 在对象表中，选择要忽略的所有适用对象。“问题”窗格按问题类型对对象进行分组。




**步骤 4** 点击**忽略 (Ignore)** 可按类型忽略问题。您必须单独**忽略**每种问题。

**步骤 5** 点击**确定 (OK)** 以确认要忽略这些对象。

# 设备连接状态

您可以查看 CDO 租户中载入的设备的连接状态。本主题可帮助您了解各种连接状态。在**清单 (Inventory)** 页面上，**连接 (Connectivity)** 列显示设备连接状态。

当设备连接状态为“在线”时，表示设备已通电并连接到CDO。当设备由于各种原因遇到问题时，通常会出现下表中所述的其他状态。下表提供了从此类问题中恢复的方法。可能有多个问题导致连接失败。当您尝试重新连接时，CDO 会提示您先解决所有这些问题，然后再执行重新连接。

| 设备连接状态 | 可能的原因 | 解决方法 |
|---|---|---|
| 在线 | 设备已通电并连接到 CDO。 | 不适用 |
| 离线 | 设备已关闭或丢失网络连接。 | 检查设备是否处于离线状态。 |
| 许可证不足 | 设备没有足够的许可证。 | 许可证不足故障排除, on page 40 |
| 凭证无效 | CDO 用于连接到设备的用户名和密码组合不正确。 | 对无效凭证进行故障排除, on page 40 |

| 设备连接状态 | 可能的原因 | 解决方法 |
| --- | --- | --- |
| 载入 | 设备载入已启动，但尚未完成。 | 检查设备的连接并确保完成设备注册。 |
| 检测到新证书 | 设备上的证书已更改。如果设备使用自签名证书，则可能是由于设备重新启动而导致的。 | 新证书问题故障排除, on page 41 |
| 载入错误 | 在载入设备时，CDO 可能已失去与设备的连接。 | 对载入错误进行故障排除, on page 49 |

# 许可证不足故障排除

如果设备连接状态显示“许可证不足”(Insufficient License)，请执行以下操作：

- 等待一段时间，直到设备获得许可证。通常，思科智能软件管理器需要一些时间才能将新许可证应用于设备。
- 如果设备状态未更改，请从 CDO 注销并重新签名，以刷新 CDO 门户，以解决许可证服务器和设备之间的任何网络通信故障。
- 如果门户刷新未更改设备状态，请执行以下操作：

**步骤 1** 从思科智能软件管理器生成新的令牌并进行复制。您可以观看生成智能许可视频了解详细信息。

**步骤 2** 在 CDO 导航栏中，点击**设备和服务 (Devices & Services)** 页面。

**步骤 3** 点击**设备**选项卡。

**步骤 4** 点击相应的设备类型选项卡，然后选择状态为**许可证不足**的设备。

**步骤 5** 在**设备详细信息 (Device Details)** 窗格中，点击**许可证不足 (Insufficient Licenses)**中出现的**管理许可证 (Manage Licenses)**。此时将出现**管理许可证 (Manage Licenses)** 窗口。

**步骤 6** 在**激活 (Activate)** 字段中，粘贴新的令牌，然后点击**注册设备 (Register Device)**。

将令牌成功应用于设备后，其连接状态将变为**在线 (Online)**。

# 对无效凭证进行故障排除

执行以下操作以解决由于凭证无效而导致设备断开连接的问题：

**步骤 1** 打开**清单 (Inventory)** 页面。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击相应的设备类型选项卡，然后选择具有**无效凭证 (Invalid Credentials)** 状态的设备。

**步骤 4** 在**设备详细信息 (Device Details)** 窗格中，点击**无效凭证 (Invalid Credentials)** 中显示的 **重新连接 (Reconnect)**。CDO 尝试与您的设备重新连接。

**步骤 5** 出现提示时，输入设备的用户名和密码。

**步骤 6** 点击**继续**。

**步骤 7** 设备在线并准备好使用后，点击**关闭 (Close)**。

**步骤 8** 可能是因为 CDO 尝试使用错误的凭证连接到设备，因此直接在设备上更改了 CDO 用于连接到设备的用户名和密码组合。您现在可能会看到设备处于“在线”(Online) 状态，但配置状态为“检测到冲突”(Conflict Detected)。使用解决配置冲突 (Resolve Configuration Conflicts) 以查看和解决 CDO 与设备之间的配置差异。

# 新证书问题故障排除

### CDO 对证书的使用

CDO 在连接到设备时检查证书的有效性。具体而言，CDO 要求：

1. 设备使用 TLS 版本 1.0 或更高版本。
2. 设备提供的证书未过期，并且其颁发日期是过去的日期（即，它已经有效，未计划在以后生效）。
3. 证书必须是 SHA-256 证书。不接受 SHA-1 证书。
4. 以下条件之一成立：
   - 设备使用自签名证书，并且与授权用户信任的最新证书相同。
   - 设备使用受信任证书颁发机构 (CA) 签名的证书，并提供将所提供的枝叶证书链接到相关 CA 的证书链。

以下是 CDO 使用与浏览器不同的证书的方式：

- 如果是自签名证书，则 CDO 会覆盖域名检查，而不会在设备载入或重新连接期间检查证书是否与授权用户信任的证书完全匹配。
- CDO 尚不支持内部 CA。目前无法检查由内部 CA 签名的证书。

  可以按设备禁用 ASA 设备的证书检查。当 CDO 无法信任 ASA 的证书时，您可以选择禁用该设备的证书检查。如果您已尝试禁用设备的证书检查，但仍无法将其载入，则可能是您为设备指定的 IP 地址和端口不正确或无法访问。无法全局禁用证书检查，也无法对具有受支持证书的设备禁用证书检查。无法禁用非 ASA 设备的证书检查。

  当您禁用设备的证书检查时，CDO 仍将使用 TLS 连接到设备，但不会验证用于建立连接的证书。这意味着被动的中间人攻击者将无法窃听连接，但主动的中间人可以通过提供具有无效证书的 CDO 来拦截连接。

### 确定证书问题

CDO 可能无法载入设备的原因有很多种。当 UI 显示消息“CDO 无法使用提供的证书连接到设备”时，表示证书存在问题。当UI不显示此消息时，问题更有可能与连接问题（设备无法访问）或其他网络错误有关。

要确定 CDO 拒绝给定证书的原因，您可以在 SDC 主机或可访问相关设备的其他主机上使用 openssl 命令行工具。使用以下命令创建显示设备提供的证书的文件：

```
openssl s_client -showcerts -connect <host>:<port> &> <filename>.txt
```

此命令将启动交互式会话，因此您需要在几秒钟后使用 Ctrl-c 退出。

您现在应该有一个包含如下输出的文件：

```
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify return:1
depth=1 C = US, O = Google Inc, CN = Google Internet Authority G2
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google Inc, CN = *.google.com
verify return:1 CONNECTED(00000003)
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
  i:/C=US/O=Google Inc/CN=Google Internet Authority G2
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
  i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
  i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE-----
---
Server certificate
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits

---
SSL handshake has read 4575 bytes and written 434 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1.2
```

```
    Cipher : ECDHE-RSA-AES128-GCM-SHA256
    Session-ID: 48F046F3360225D51BE3362B50CE4FE8DB6D6B80B871C2A6DD5461850C4CF5AB
    Session-ID-ctx:
    Master-Key:
9A9CCBAA4F5A25B95C37EF7C6870F8C5DD3755A9A7B4CCE4535190B793DEFF53F94203AB0A62F9F70B9099FBFEBAB1B6

    Key-Arg : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 100800 (seconds)
    TLS session ticket:
    0000 - 7a eb 54 dd ac 48 7e 76-30 73 b2 97 95 40 5b de z.T..H~v0s...@[.
    0010 - f3 53 bf c8 41 36 66 3e-5b 35 a3 03 85 6f 7d 0c .S..A6f>[5...o}.
    0020 - 4b a6 90 6f 95 e2 ec 03-31 5b 08 ca 65 6f 8f a6 K..o....1[..eo..
    0030 - 71 3d c1 53 b1 29 41 fc-d3 cb 03 bc a4 a9 33 28 q=.S.)A.......3(
    0040 - f8 c8 6e 0a dc b3 e1 63-0e 8f f2 63 e6 64 0a 36 ..n....c...c.d.6
    0050 - 22 cb 00 3a 59 1d 8d b2-5c 21 be 02 52 28 45 9d "..:Y...\!..R(E.
    0060 - 72 e3 84 23 b6 f0 e2 7c-8a a3 e8 00 2b fd 42 1d r..#...|....+.B.
    0070 - 23 35 6d f7 7d 85 39 1c-ad cd 49 f1 fd dd 15 de #5m.}.9...I.....
    0080 - f6 9c ff 5e 45 9c 7c eb-6b 85 78 b5 49 ea c4 45 ...^E.|.k.x.I..E
    0090 - 6e 02 24 1b 45 fc 41 a2-87 dd 17 4a 04 36 e6 63 n.$.E.A....J.6.c
    00a0 - 72 a4 ad
    00a4 - <SPACES/NULS> Start Time: 1476476711 Timeout : 300 (sec)
Verify return code: 0 (ok)
---
```

在此输出中要注意的第一件事是最后一行，您可以在其中看到**验证返回代码 (Verify return code)**。如果存在证书问题，返回代码将为非零值，并且会有错误说明。

**展开此证书错误代码列表，查看常见错误及其补救方法**

0 X509_V_OK 操作成功。

2 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT 无法找到不受信任证书的颁发者证书。

3 X509_V_ERR_UNABLE_TO_GET_CRL 无法找到证书的 CRL。

4 X509_V_ERR_UNABLE_TO_DECRYPT_CERT_SIGNATURE 无法解密证书签名。这意味着无法确定实际签名值，而不是与预期值不匹配。这仅对 RSA 密钥有意义。

5 X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE 无法解密 CRL 签名。这意味着无法确定实际签名值，而不是与预期值不匹配。未使用。

6 X509_V_ERR_UNABLE_TO_DECODE_ISSUER_PUBLIC_KEY 无法读取证书 SubjectPublicKeyInfo 中的公钥。

7 X509_V_ERR_CERT_SIGNATURE_FAILURE 证书签名无效。

8 X509_V_ERR_CRL_SIGNATURE_FAILURE 证书签名无效。

9 X509_V_ERR_CERT_NOT_YET_VALID 证书无效：notBefore 日期晚于当前时间。有关详细信息，请参阅下面的验证返回代码：9（证书尚未生效）。

10 X509_V_ERR_CERT_HAS_EXPIRED The certificate has expired;也就是说，notAfter 日期早于当前时间。有关详细信息，请参阅下面的验证返回代码：10（证书已过期）。

11 X509_V_ERR_CRL_NOT_YET_VALID CRL 尚未生效。

12 X509_V_ERR_CRL_HAS_EXPIRED CRL 已过期。

13 X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD 证书 notBefore 字段包含无效时间。

14 X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD 证书 notAfter 字段包含无效时间。

15 X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD CRL lastUpdate 字段包含无效时间。

16 X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD CRL nextUpdate 字段包含无效时间。

17 X509_V_ERR_OUT_OF_MEM 尝试分配内存时发生错误。这绝不应该发生。

18 X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT 通过的证书是自签名证书，在受信任证书列表中找不到相同的证书。

19 X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN 可以使用不受信任的证书建立证书链，但无法在本地找到根证书。

20 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY 无法找到本地查找的证书的颁发者证书。这通常意味着受信任证书列表不完整。

21 X509_V_ERR_UNABLE_TO_VERIFY_LEAF_SIGNATURE 无法验证签名，因为该链仅包含一个证书，并且它不是自签名证书。有关详细信息，请参阅下面的“验证返回代码：21（无法验证第一个证书）”。验证返回代码：21（无法验证下面的第一个证书）以了解详细信息。

22 X509_V_ERR_CERT_CHAIN_TOO_LONG 证书链长度大于提供的最大深度。未使用。

23 X509_V_ERR_CERT_REVOKED 证书已被撤销。

24 X509_V_ERR_INVALID_CA CA 证书无效。它不是 CA 或其扩展名与提供的用途不一致。

25 X509_V_ERR_PATH_LENGTH_EXCEEDED BasicConstraints 路径长度参数已被超过。

26 X509_V_ERR_INVALID_PURPOSE 提供的证书不能用于指定的目的。

27 X509_V_ERR_CERT_UNTRUSTED 根 CA 未标记为用于指定用途的受信任。

28 X509_V_ERR_CERT_REJECTED 根 CA 被标记为拒绝指定用途。

29 X509_V_ERR_SUBJECT_ISSUER_MISMATCH 当前候选颁发者证书被拒绝，因为其使用者名称与当前证书的颁发者名称不匹配。仅在设置了 -issuer_checks 选项时显示。

30 X509_V_ERR_AKID_SKID_MISMATCH 当前候选颁发者证书被拒绝，因为其使用者密钥标识符存在且与当前证书的颁发机构密钥标识符不匹配。仅在设置了 -issuer_checks 选项时显示。

31 X509_V_ERR_AKID_ISSUER_SERIAL_MISMATCH 当前候选颁发者证书被拒绝，因为其颁发者名称和序列号存在，并且与当前证书的颁发机构密钥标识符不匹配。仅在设置了 -issuer_checks 选项时显示。

32 X509_V_ERR_KEYUSAGE_NO_CERTSIGN 当前候选颁发者证书被拒绝，因为其 keyUsage 扩展不允许证书签名。

50 X509_V_ERR_APPLICATION_VERIFICATION 应用特定错误。未使用。

### 检测到新证书

如果升级具有自签名证书的设备，并且在升级过程后生成了新证书，则CDO可能会生成“检测到新证书”(New Certificate Detected) 消息作为**配置状态 (Configuration Status)** 和**连接 (Connectivity)** 状

态。您必须手动确认并解决此问题，然后才能继续从CDO对其进行管理。证书同步且设备处于正常状态后，即可管理设备。

**Note** 当您同时将多个托管设备批量重新连接到 CDO 时，CDO 会自动审核并接受设备上的新证书，并继续与其重新连接。

使用以下程序解析新证书：

1. 导航到**设备和服务 (Device & Services)** 页面。
2. 使用过滤器显示**检测到新证书 (New Certificate Detected)** 连接或配置状态的设备，然后选择所需的设备。
3. 在右侧窗格中，点击**查看证书 (Review Certificate)**。CDO 允许您下载证书以供审核并接受新证书。
4. 在设备同步窗口中，点击**接受 (Accept)**，或在重新连接到设备窗口中，点击**继续 (Continue)**。

   CDO 会自动将设备与新的自签名证书同步。您可能需要手动刷新**设备和服务 (Devices & Services)** 页面，才能在设备同步后查看设备。

### 证书错误代码

#### 验证返回代码：0（正常），但 CDO 返回证书错误

CDO 获得证书后，它会尝试通过对“https://”进行 GET 调用来连接到设备的 URL。<device_ip>：<port> "。如果这不起作用，CDO 将显示证书错误。如果您发现证书有效（openssl 返回 0 ok），则问题可能是其他服务正在侦听您尝试连接的端口。只能使用命令：

```
curl -k -u <username>:<password> https://<device_id>:<device_port>/admin/exec/show%20version
```

确定您是否确实在与 ASA 通信，并检查 HTTPS 服务器是否在 ASA 上的正确端口上运行：

```
 # show asp table socket
Protocol         Socket         State         Local Address              Foreign Address
SSL              00019b98        LISTEN        192.168.1.5:443             0.0.0.0:*
SSL              00029e18        LISTEN        192.168.2.5:443             0.0.0.0:*
TCP              00032208        LISTEN        192.168.1.5:22              0.0.0.0:*
```

#### 验证返回代码：9（证书尚未生效）

此错误意味着所提供证书的颁发日期是未来，因此客户端不会将其视为有效。这可能是由于证书构建不良导致的，或者在自签名证书的情况下，可能是由于设备生成证书时时间错误。

您应该会在错误中看到一行，包括证书的 notBefore 日期：

```
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=9:certificate is not yet valid
notBefore=Oct 21 19:43:15 2016 GMT
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
notBefore=Oct 21 19:43:15 2016 GMT
```

通过此错误，您可以确定证书何时生效。

**补救**

证书的 notBefore 日期需要是过去的日期。您可以使用更早的 notBefore 日期重新颁发证书。当客户端或颁发设备上的时间设置不正确时，也会出现此问题。

**验证返回代码：10（证书已过期）**

此错误意味着所提供的至少一个证书已过期。您应该会在错误中看到一行，包括证书的notBefore日期：

```
 error 10 at 0 depth lookup:certificate has expired
```

到期日期位于证书正文中。

**补救**

如果证书确实已过期，则唯一的补救方法是获取另一个证书。如果证书仍将到期，但openssl声称它已过期，请检查计算机上的时间和日期。例如，如果某个证书设置为在2020年到期，但您的计算机上的日期是 2021 年，则您的计算机会将该证书视为已过期。

**验证返回代码：21（无法验证第一个证书）**

此错误表示证书链存在问题，并且openssl无法验证设备提供的证书是否应受信任。我们来看看上面示例中的证书链，了解证书链的工作原理：

```
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
i:/C=US/O=Google Inc/CN=Google Internet Authority G2

-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA

-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority

-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
....lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE----- ---
```

证书链是服务器提供的证书列表，从服务器自己的证书开始，然后包括将服务器的证书与证书颁发机构的顶级证书链接的更高级别的中间证书。每个证书都会列出其使用者（以“s:”开头的行及其颁发者）（以“i”开头的行）。

使用者是证书所标识的实体。它包括组织名称，有时还包括为其颁发证书的实体的通用名称。

颁发者是颁发证书的实体。它还包括一个组织字段，有时还包括一个通用名称。

如果服务器具有由受信任证书颁发机构直接颁发的证书，则无需在其证书链中包含任何其他证书。它将显示一个如下所示的证书：

```
--- Certificate chain 0 s:/C=US/ST=California/L=Anytown/O=ExampleCo/CN=*.example.com
i:/C=US/O=Trusted Authority/CN=Trusted Authority
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
....lots of base64...
tzw9TylimhJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE----- ---
```

鉴于此证书，openssl 将验证 ***.example.com** 的 ExampleCo 证书是否由受信任的颁发机构证书正确签名，该证书存在于 openssl 的内置信任存储区中。验证后，openssl 将成功连接到设备。

但是，大多数服务器没有直接由受信任 CA 签名的证书。相反，与第一个示例一样，服务器的证书由一个或多个中间设备签名，而最高级别的中间设备具有由受信任 CA 签名的证书。默认情况下，OpenSSL 不信任这些中间 CA，并且只有在获得以受信任 CA 结尾的完整证书链时才能对其进行验证。

由中间机构签署证书的服务器必须提供将其链接到受信任 CA 的所有证书，包括所有中间证书。如果它们不提供整个链，则 openssl 的输出将如下所示：

```
depth=0 OU = Example Unit, CN = example.com
verify error:num=20:unable to get local issuer certificate
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=27:certificate not trusted
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=21:unable to verify the first certificate
verify return:1

CONNECTED(00000003)

---
Certificate chain
0 s:/OU=Example Unit/CN=example.com
i:/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
-----BEGIN CERTIFICATE-----
...lots of b64...
-----END CERTIFICATE-----
---
Server certificate
subject=/OU=Example Unit/CN=example.com
issuer=/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
---
No client certificate CA names sent
---
SSL handshake has read 1509 bytes and written 573 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
```

```
Expansion: NONE
SSL-Session:
Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: 24B45B2D5492A6C5D2D5AC470E42896F9D2DDDD54EF6E3363B7FDA28AB32414B
Session-ID-ctx:
Master-Key:
21BAF9D2E1525A5B935BF107DA3CAF691C1E499286CBEA987F64AE5F603AAF8E65999BD21B06B116FE9968FB7C62EF7C

Key-Arg : None
Krb5 Principal: None
PSK identity: None
PSK identity hint: None
Start Time: 1476711760
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

此输出显示服务器仅提供一个证书，并且提供的证书是由中间机构而不是受信任的根签名的。输出还显示特征验证错误。

**补救**

此问题是由设备提供的证书配置错误引起的。解决此问题的唯一方法是将正确的证书链加载到设备上，以便 CDO 或任何其他程序可以安全地连接到设备，以便为连接的客户端提供完整的证书链。

要将中间 CA 添加到信任点，请访问以下链接之一（具体取决于您的情况 - 是否在 ASA 上生成了 CSR）：

- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc13
- https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc15

## 检测到新证书

如果升级具有自签名证书的设备，并且在升级过程后生成了新证书，则CDO可能会生成“检测到新证书”(New Certificate Detected) 消息作为**配置状态 (Configuration Status)** 和**连接 (Connectivity)** 状态。您必须手动确认并解决此问题，然后才能继续从CDO对其进行管理。证书同步且设备处于正常状态后，即可管理设备。

**注释** 当您选择批量重新连接设备至 CDO (Bulk Reconnect Devices to CDO) 同时将多个托管设备连接到CDO时，CDO 会自动审核并接受设备上的新证书，并继续与其重新连接。

使用以下程序解析新证书：

**步骤 1** 在导航栏中，点击 **设备和服务**。

**步骤 2** 点击**设备**选项卡。

**步骤 3** 点击适当的设备类型选项卡。

**步骤 4** 使用过滤器显示**检测到新证书 (New Certificate Detected)** 连接或配置状态的设备，然后选择所需的设备。

**步骤 5** 在右侧窗格中，点击**查看证书 (Review Certificate)**。CDO 允许您下载证书以供审核并接受新证书。

**步骤 6** 在设备同步窗口中，点击**接受 (Accept)**，或在重新连接到设备窗口中，点击**继续 (Continue)**。

CDO 会自动将设备与新的自签名证书同步。您可能需要手动刷新**设备和服务 (Devices & Services)** 页面，才能在设备同步后查看设备。

# 对载入错误进行故障排除

出现设备载入错误的原因有很多。

可以采取以下操作：

**步骤 1** 在**清单 (Inventory)** 页面中，点击**设备 (Devices)** 选项卡。

**步骤 2** 点击相应的设备类型选项卡，然后选择遇到此错误的设备。在某些情况下，您会在右侧看到错误说明。执行说明中提到的必要操作。

或

**步骤 3** 从 CDO 中删除设备实例，然后尝试重新载入设备。

# 解决“检测到冲突”状态

CDO 允许您在每个实时设备上启用或禁用冲突检测。如果 冲突检测 已启用，并且在未使用 CDO 的情况下对设备的配置进行了更改，则设备的配置状态将显示为**检测到冲突 (Conflict Detected)**。

要解决“检测到冲突”(Conflict Detected) 状态，请执行以下程序：

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**Note** 对于 本地防火墙管理中心，请导航至**工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)** 并选择处于**检测到冲突 (Conflict Detected)** 状态的 FMC，然后从步骤 4 继续操作。

**步骤 2** 点击**设备 (Devices)** 选项卡以找到设备。

**步骤 3** 点击设备类型选项卡。

**步骤 4** 选择报告冲突的设备，然后点击右侧详细信息窗格中的**查看冲突 (Review Conflict)**。

**步骤 5** 在**设备同步 (Device Sync)** 页面中，通过查看突出显示的差异来比较两种配置。

- 标记为“最后一次设备配置”(Last Known Device Configuration) 的面板是存储在 CDO 上的设备配置。
- 标记为“在设备上找到”(Found on Device) 的面板是存储在运行 ASA 配置中的配置。

**步骤 6** 通过选择以下选项之一来解决冲突：

- **接受设备更改 (Accept Device changes)**：这将使用设备的运行配置覆盖 CDO **上存储的配置** 和任何待处理的更改。

  **Note** 由于 CDO 不支持在命令行界面之外部署对Cisco IOS 设备的更改，因此在解决冲突时，您对Cisco IOS 设备的唯一选择是选择**接受而不查看 (Accept Without Review)**。

- **拒绝设备更改 (Reject Device Changes)**：这将使用存储在 CDO 上的配置覆盖设备上存储的配置。

**Note** 所有配置更改（拒绝或接受）都记录在更改日志中。

# 解决“未同步”状态

使用以下程序解决配置状态为“未同步”的设备：

**步骤 1** 在导航栏中，点击**清单 (Inventory)**。

**Note** 对于 本地防火墙管理中心，请导航至**工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)** 并选择处于**未同步 (Not Synced)** 状态的 FMC，然后从步骤 5 继续操作。

**步骤 2** 点击 **设备** 选项卡以查找设备，或点击 **模板** 选项卡以查找型号设备。

**步骤 3** 点击设备类型选项卡。

**步骤 4** 选择报告为“未同步”的设备。

**步骤 5** 在右侧的未同步面板中，选择以下任一选项：

- **预览并部署...** - 如果要将配置更改从 CDO 推送到设备，请预览并部署您现在所做的更改，或者等待并一次部署多个更改。预览和部署所有设备的配置更改
- 放弃更改 - 如果您不想将配置更改从 CDO 推送到设备，或者您想要“撤消”您开始在 CDO 上进行的配置更改。此选项使用设备上存储的运行配置覆盖 CDO 中存储的配置。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。