

AMP虚拟私有云和Threat Grid设备的集成

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[集成架构](#)

[有关集成的基本信息](#)

[步骤](#)

[重新生成SSL证书](#)

[上传SSL证书](#)

[Threat Grid设备安全接口中的证书是自签名的](#)

[Threat Grid设备干净界面中的证书由企业证书颁发机构\(CA\)签名](#)

[示例](#)

[确认](#)

[确认AMP私有云数据库中的样本处置情况更新](#)

[示例](#)

[故障排除](#)

[AMP私有云设备中有关主机无效、证书未测试、API密钥未测试的警告](#)

[AMP私有云设备中有关无效Threat Grid API密钥的警告](#)

[AMP私有云设备接收的分数 \$\geq 95\$ 的样本，但样本性质中未发现任何变化](#)

[AMP私有云设备中有关无效Threat Grid SSL证书的警告](#)

[Threat Grid设备中与证书相关的警告](#)

[警告消息 — 从私钥派生的公钥不匹配](#)

[警告消息 — 私钥包含非PEM内容](#)

[警告消息 — 无法从私钥生成公钥](#)

[警告消息 — 解析错误：无法解码PEM数据](#)

[警告消息 — 不是客户端/服务器CA证书](#)

[相关信息](#)

本文档介绍完成高级恶意软件防护(AMP)虚拟私有云与Threat Grid设备集成的过程。本文档提供与集成过程相关的问题的故障排除步骤。

作者：Armando Garcia，思科TAC工程师。

Cisco 建议您了解以下主题：

- 工作和运行AMP虚拟私有云
- 工作和运行Threat Grid设备

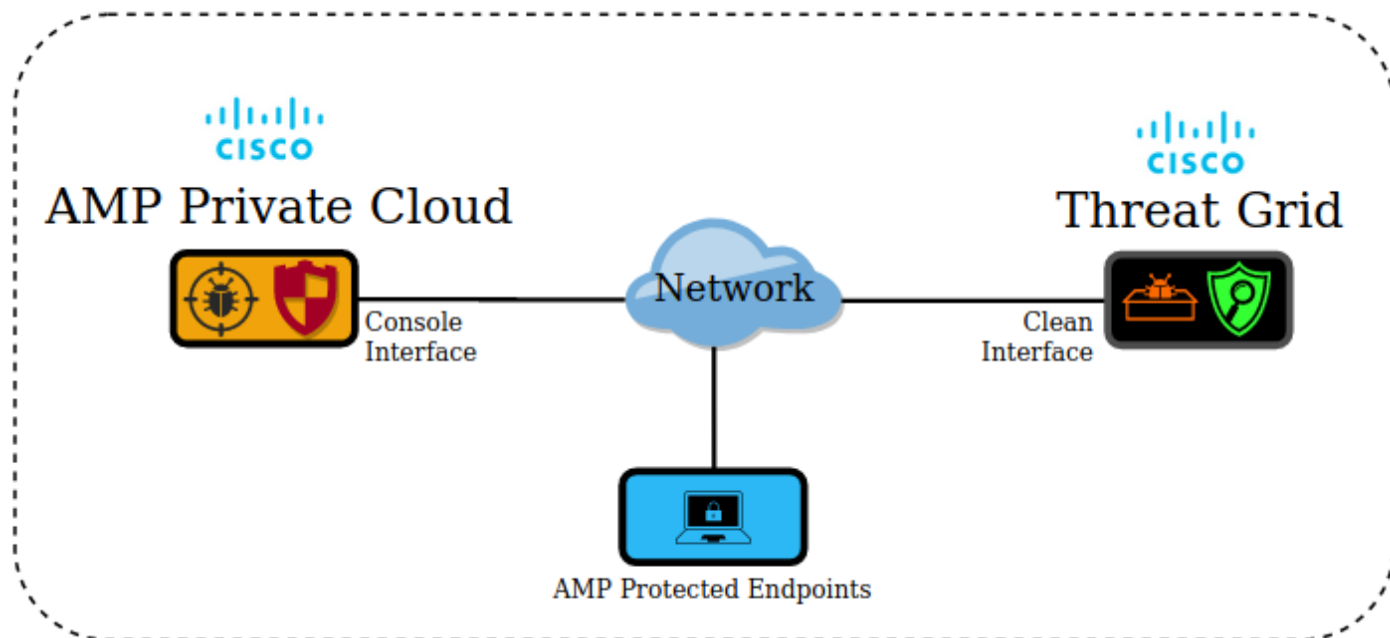
本文档中的信息基于以下软件和硬件版本：

- AMP私有云3.2.0
- Threat Grid设备2.12.0.1

注意：本文档对设备或虚拟版本中的Threat Grid设备和AMP私有云设备有效。

背景信息

集成架构



有关集成的基本信息

- Threat Grid设备分析AMP私有云设备提交的示例。
- 示例可以手动或自动提交到Threat Grid设备。
- 默认情况下，AMP私有云设备中未启用自动分析。
- Threat Grid设备向AMP私有云设备提供报告和样本分析得分。
- Threat Grid设备会通知（戳）AMP私有云设备任何分数大于或等于95分的样本。
- 如果分析得分大于或等于95，则AMP数据库中的样本将标记为恶意性质。
- AMP私有云应用追溯性检测，对得分大于或等于95的样本进行采样。

步骤

步骤1.设置和配置Threat Grid设备（尚未集成）。检查更新并安装（如果需要）。

步骤2.设置和配置面向终端的AMP私有云（尚未集成）。

步骤3.在Threat Grid管理员UI中，选择Configuration选项卡并选择SSL。

步骤4.为Clean接口(PANDEM)生成或上传新的SSL证书。

重新生成SSL证书

如果干净接口的主机名与设备中当前为干净接口安装的证书中的使用者备用名称(SAN)不匹配，则可以生成新的自签名证书。设备为接口生成新证书，在自签名证书的SAN字段中配置当前接口主机名。

第4.1步。从“操作”列中选择(...)，然后从弹出菜单中选择“生成新证书”。

第4.2步。在Threat Grid UI中，选择操作，在下一个屏幕中选择激活，然后选择**重新配置**。

注意：此生成的证书是自签名的。

上传SSL证书

如果已为Threat Grid设备干净接口创建了证书，则此证书可以上传到设备。

第4.1步。从“操作”列中选择(...)，然后从弹出菜单中选择“上传新证书”。

步骤4.2.将证书和PEM格式的相应私钥复制到屏幕上显示的文本框中，并选择Add Certificate。

第4.3步。在Threat Grid UI中，选择操作，在下一个屏幕中选择激活，然后选择**重新配置**。

步骤5.在AMP私有云设备管理员UI中，选择“集成”并选择“Threat Grid”。

步骤6.在Threat Grid Configuration Details (Threat Grid配置详细信息)中，选择Edit(编辑)。

步骤7.在Threat Grid主机名中，输入Threat Grid设备的干净接口的FQDN。

步骤8.在Threat Grid SSL证书中，添加Threat Grid设备的干净接口的证书。(请参阅以下注释)

Threat Grid设备安全接口中的证书是自签名的

第8.1步。在Threat Grid管理员UI中，选择Configuration并选择SSL。

步骤8.2.从“操作”列中选择(...),然后从弹出菜单中选择“下载证书”。

步骤8.3.继续将下载的文件添加到Threat Grid集成页面的AMP虚拟专用设备。

Threat Grid设备干净界面中的证书由企业证书颁发机构(CA)签名

步骤8.1.在文本文件中复制Threat Grid设备的安全接口证书和完整的CA证书链。

注意：文本文件中的证书必须为PEM格式。

如果完整的证书链是：ROOT_CA证书> Threat_Grid_Clean_Interface证书；然后需要创建文本文件，如图所示。



```
-----BEGIN CERTIFICATE-----  
Threat_Grid_Clean_Interface certificate PEM data  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
ROOT_CA certificate PEM data  
-----END CERTIFICATE-----
```

如果完整的证书链是：ROOT_CA证书> Sub_CA证书> Threat_Grid_Clean_Interface证书；然后需要创建文本文件，如图所示。

```
-----BEGIN CERTIFICATE-----  
Threat_Grid_Clean_Interface certificate PEM data  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
Sub_CA certificate PEM data  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
ROOT_CA certificate PEM data  
-----END CERTIFICATE-----
```

9.Threat Grid API KeyThreat GridAPI

API

| | | | |
|---|----------------------------|---|-----------------------------|
| API Key | ***** |   | |
| Disable API Key  | <input type="radio"/> True | <input checked="" type="radio"/> False | <input type="radio"/> Unset |
| Can Download Sample Content Via API  | <input type="radio"/> True | <input checked="" type="radio"/> False | <input type="radio"/> Unset |

注意：在Threat Grid用户的帐户设置中，确认**Disable API Key**参数未设置为True。

步骤10.完成所有更改后，选择“保存”。

步骤11.对AMP虚拟云设备应用重新配置。

步骤12.从AMP私有云设备管理员UI中，选择“集成”并选择“Threat Grid”。

步骤13.从详细信息中复制“处置更新服务URL”、“处置更新服务”用户和“处置更新服务”密码的值。此信息用于步骤17。

步骤14.在Threat Grid管理员UI中，选择**Configuration**并选择**CA Certificates**。

步骤15.选择**Add Certificate**并以PEM格式复制签署AMP私有云处置更新服务证书的CA证书。

注意：如果签署AMP私有云处置更新证书的CA证书是子CA，请重复此过程，直到链中的所有CA都上传到CA证书。

步骤16.在Threat Grid门户中，选择Administration，然后选择Manage AMP Private Cloud Integration。

步骤17.在Disposition Update Syndication Service页面中，输入在步骤13中收集的信息。

- 服务URL:AMP私有云设备的处置更新服务的FQDN。
- 用户：来自AMP私有云设备的处置更新服务的用户。
- 密码：AMP私有云设备的处置更新服务的密码。

此时，如果所有步骤都应用正确，则集成必须成功运行。

确认

注意：仅步骤1、2、3和4适合在生产环境中应用以验证集成。步骤5作为信息提供，以了解有关集成的详细信息，不建议在生产环境中应用。

1.AMPUI >> Threat GridThreat Grid

Threat Grid Configuration Details Edit

| | |
|------------------------------------|---|
| Hostname | <input type="text" value="cisco.com"/> |
| API Key | <input type="password" value="....."/> |
| Threat Grid SSL Certificate | |
| Issuer | subca_tga_clean |
| Subject | <input type="text" value="cisco.com"/> |
| Validity | 2020-11-24 00:00:00 UTC - 2021-11-23 23:59:59 UTC |

Test Connection

tus ▾ Integrations ▾ Support ▾

✔ Threat Grid Connection test successful!

2.AMP

cisco AMP for Endpoints 🔔 ? armando garcia ▾

Dashboard Analysis ▾ Outbreak Control ▾ Management ▾ Accounts ▾

File Analysis

There are no File Analyses to view

步骤3.确认Threat Grid设备中感知到从AMP私有云控制台**Analysis > File Analysis**手动提交的文件，并且Threat Grid设备返回具有分数的报告。

File has been uploaded for analysis

File Analysis

Search by SHA-256, File name, IP, Keywords... Submit File

There are no File Analyses to view

File Analysis

Search by SHA-256, File name, IP, Keywords... Submit File

| | | |
|-----------------------------------|-------------------------|-----------|
| glogg.exe (e309efdd...0c2c3d25) | 2021-01-31 06:16:55 UTC | Report 24 |
|-----------------------------------|-------------------------|-----------|

步骤4. 确认在证书颁发机构的Threat Grid设备中安装了签署AMP私有云设备的处置更新服务证书的CA。

步骤5. 确认在报告和样本分数由Threat Grid设备提供后，Threat Grid设备标记的分数 ≥ 95 的任何样本都记录在具有恶意性质的AMP私有云数据库中。

注意：在AMP私有云控制台的“文件分析”(File Analysis)选项卡中成功接收样本报告和大于 ≥ 95 的样本分数并不意味着文件性质在AMP数据库中发生了更改。如果签署AMP私有云设备的处置更新服务证书的CA未安装在证书颁发机构的Threat Grid设备中，则AMP私有云设备会收到报告和分数，但不会从Threat Grid设备接收任何poke。

警告：在Threat Grid设备标记了分数 ≥ 95 的文件后，完成下一次测试，以触发AMP数据库中的样本性质更改。此测试的目的是在Threat Grid设备提供的样本分数 ≥ 95 时提供有关AMP私有云设备内部操作的信息。为了触发处置更改过程，使用Cisco内部Makemalware.exe应用创建了模拟恶意软件的测试文件。示例：malware3-419d23483.exeSHA256:8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995。

警告：不建议在生产环境中引爆任何模拟恶意软件的测试文件。

确认AMP私有云数据库中的样本处置情况更新

AMPThreat GridThreat GridAMP100 ≥ 95 AMPThreat Grid ≥ 95 AMP

File Analysis

Search by SHA-256, File name, IP, Keywords...

| | | |
|--|-------------------------|---|
| ▶ xca.exe (63019d7c...a24c6c44) | 2021-01-31 08:16:38 UTC | <input type="button" value="Report"/> 30 |
| ▶ WinRAR.exe (9066f0bc...f79d741e) | 2021-01-31 06:17:05 UTC | <input type="button" value="Report"/> 80 |
| ▶ glogg.exe (e309efdd...0c2c3d25) | 2021-01-31 06:16:55 UTC | <input type="button" value="Report"/> 24 |
| ▼ malware3-8d3bbc795.exe (8d3bbc79...5aacc995) | 2021-01-31 06:16:50 UTC | <input type="button" value="Report"/> 100 |

| | | |
|-----------------------|------------------------|-------|
| Fingerprint (SHA-256) | 8d3bbc79...5aacc995 | |
| File name | malware3-8d3bbc795.exe | |
| Threat Score | 100 | |
| | Name | Score |

如果：

- 集成已成功完成。
- 手动提交文件后，在文件分析中会看到示例报告和分数。

然后：

- 对于Threat Grid设备以分数 ≥ 95 标记的每个示例，AMP私有云设备中的 /data/poked/poked.log文件中都会添加一个条目。
- 在Threat Grid设备提供第一个 ≥ 95 的样本得分后，在AMP私有云设备中创建 /data/poked/poked.log。
- AMP私有云中的db_protect数据库保存样本的当前性质。此信息可用于在Threat Grid设备提供分数后确认样本的性质是否为3。

如果在AMP私有云控制台的文件分析中看到示例报告和 ≥ 95 分，请应用以下步骤：

步骤1.通过SSH登录AMP私有云设备。

步骤2.确认/data/poked/poked.log中有示例条目。

列出从未从Threat Grid设备收到 ≥ 95 样本分数的AMP私有云设备中的/data/poked/目录后，系统中未创建poked.log文件。

如图所示，如果AMP私有云设备从未收到来自Threat Grid设备的戳，则目录中找不到 /data/poked/poked.log文件。

```
[root@fireamp ~]# ls /data/poked/
poked_error.log
[root@fireamp ~]#
```

在收到第一个 ≥ 95 的样本得分后列出/data/poked/目录，显示文件已创建。

收到分数 ≥ 95 的第一个样本后。


```
[root@fireamp ~]# ls /data/poked/
poked_error.log  poked.log
[root@fireamp ~]#
[root@fireamp ~]# cat /data/poked/poked.log
Jan 30 18:25:18 fireamp poked[9557]: [9557] info @0.004940 127.0.0.1 --
{"disposition": "malicious", "force": 0, "state": "local", "name": "W32.80388C7958-100.S8X.TG", "ok": 1, "time": 1612031118, "hash": "8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995", "engine": "sha256", "user": "-", "mode": "tg", "score": 100}
[root@fireamp ~]#
```

Threat Grid设备提供的戳的示例信息可以在poked.log文件中感知。

步骤3.使用示例SHA256运行此命令，以从AMP私有云设备的数据库检索当前处置情况。

```
mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x
```

示例

在将样本上传到Threat Grid设备之前获取样本性质的数据库查询不提供任何结果，如图所示。

```
[root@fireamp ~]# mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995;"
[root@fireamp ~]#
```

在从Threat Grid设备收到报告和分数后获取样本性质的数据库查询显示性质为3且被视为恶意的样本。

```
[root@fireamp ~]# mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995;"
+-----+-----+
| hex(fingerprint) | disposition_id |
+-----+-----+
| 8D3BBC795BB47447984BF2842D3A0119BAC0D79A15A59686951E1F7C5AACC995 | 3 |
+-----+-----+
[root@fireamp ~]#
```

故障排除

在集成过程中，可以发现可能的问题。在本文档的这一部分，我们讨论了一些最常见问题。

AMP私有云设备中有关主机无效、证书未测试、API密钥未测试的警告

症状

警告消息：Threat Grid主机无效，无法测试Threat Grid SSL证书，无法测试Threat Grid API密钥，在选中Integrations > Threat Grid中的Test Connection按钮后，将在AMP私有云设备中收到该密钥。

Connect Threat Grid Appliance to AMP for Endpoints Appliance

Threat Grid Connection test failed.

- Threat Grid host is invalid.
- Threat Grid SSL Certificate could not be tested.
- Threat Grid API key could not be tested.

在集成中，网络级存在问题。

推荐步骤：

- 确认AMP私有云设备控制台接口可以到达Threat Grid设备的干净接口。
- 确认AMP私有云设备可以解析Threat Grid设备干净接口的FQDN。

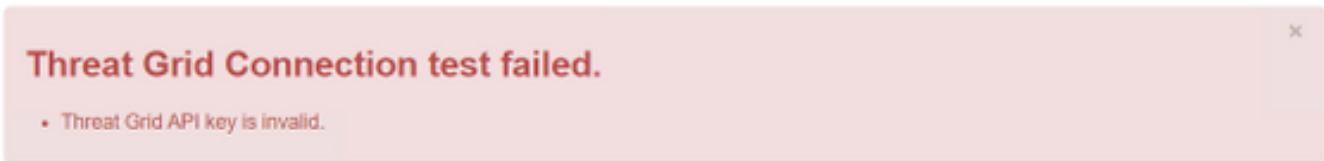
- 确认AMP私有云设备和Threat Grid设备的网络路径中没有过滤设备。

AMP Threat Grid API

症状

警告消息：Threat Grid连接测试失败，Threat Grid API无效，在选择“集成”>“Threat Grid”中的“测试连接”按钮后，将在AMP私有云设备中收到该AP。

Connect Threat Grid Appliance to AMP for Endpoints Appliance



AMP Threat Grid API

推荐步骤：

- 在Threat Grid设备用户的帐户设置中确认，Disable API Key参数未设置为True。
— 禁用API密钥参数必须设置为：False或Unset。

API



- 确认在AMP私有云管理员门户 **Integrations > Threat Grid** 中配置的Threat Grid API密钥与Threat Grid设备中的用户设置中的API密钥相同。
- 确认是否将正确的Threat Grid API密钥保存在AMP私有云设备数据库中。

从AMP私有云设备命令行，可以确认AMP设备中配置的当前Threat Grid API密钥。通过SSH登录AMP私有云设备并运行以下命令以检索当前Threat Grid用户API密钥：

```
mysql -e "select tg_api_key, tg_login, api_client_id from db_smbe.businesses;"
```

这是AMP私有云设备数据库中用于Threat Grid设备API密钥的正确条目。

```
[root@fireamp ~]# mysql -e "select tg_api_key, tg_login, api_client_id from db_smbe.businesses;"
+-----+-----+-----+
| tg_api_key          | tg_login          | api_client_id      |
+-----+-----+-----+
| mirtlif: [REDACTED] | argarci2_samples-user | de4c23c64d3e36034bb7 |
+-----+-----+-----+
[root@fireamp ~]#
```

即使在集成的任何步骤中，AMP私有云设备中未直接配置Threat Grid用户名，如果正确应用了

Threat Grid API密钥，则AMP数据库的tg_login参数中也会显示Threat Grid用户名。

这是AMP数据库中用于Threat Grid API密钥的错误条目。

```
[root@fireamp ~]# mysql -e "select tg_api_key, tg_login, api_client_id from db_smbe.businesses;"
+-----+-----+-----+
| tg_api_key          | tg_login | api_client_id      |
+-----+-----+-----+
| thisisanwrongapikey | NULL    | de4c23c64d3e36034bb7 |
+-----+-----+-----+
[root@fireamp ~]#
```

tg_loginNULLAMPThreat GridThreat Grid

AMP私有云设备接收的分数 ≥ 95 的样本，但样本性质中未发现任何变化

症状

提交样本后，从Threat Grid设备成功接收报告和 ≥ 95 个样本分数，但AMP私有云设备中未发现样本性质发生任何变化。

推荐步骤：

- 如果示例SHA256位于/data/poked/poked.log的内容中，请在AMP私有云设备中确认。如果在/data/poked/poked.log中找到SHA256，则运行此命令以确认AMP数据库中的当前样本性质。

```
mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x"
```

- 确认已将正确的AMP私有云集成密码添加到Threat Grid设备管理门户的“管理”(Administration)>“管理AMP私有云集成”(Manage AMP Private Cloud Integration)中。AMP私有云管理门户。

Step 2: Threat Grid Portal Setup

1. Go to the Threat Grid Appliance Portal.
2. Navigate to the `Manage AMP for Endpoints Integration` page on the Threat Grid appliance.
3. Add the Service URL, User, and Password from the section below.

| Details | |
|-------------|---|
| Service URL | https://dupdateamp3.argarci2-lab.com/ |
| User | disposition_update_user |
| Password | <input type="password" value="ew236 [REDACTED] xJYfPK"/> <input type="button" value="Change Password"/> |

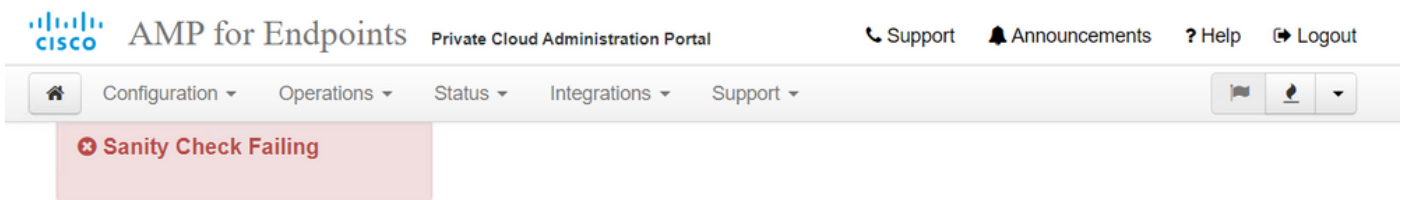
Threat Grid设备控制台门户。

| Service URL | User | Password | Action(s) |
|---|--|--|---|
| | disposition_update_user | | Edit Remove |
| | disposition_update_user | | Edit Remove |
| | disposition_update_user | | Edit Remove |
| | disposition_update_user | | Edit Remove |
| | disposition_update_user | | Edit Remove |
| | disposition_update_user | | Edit Remove |
| <input type="text" value="https://dupdateamp3.argarci2-lat"/> | <input type="text" value="disposition_update_user"/> | <input type="text" value="ew236[redacted]xJYfPK"/> | Save Cancel |
| <input type="text"/> | disposition_update_user | | Edit Remove |

- 确认已签署AMP私有云设备处置更新服务证书的CA已安装在CA证书的Threat Grid设备管理门户中。

在以下示例中，AMP私有云设备处置更新服务证书的证书链是Root_CA > Sub_CA > Disposition_Update_Service证书;因此，RootCA和Sub_CA必须安装在Threat Grid设备的CA证书中。

AMP私有云管理门户中的证书颁发机构。



Certificate Authorities are used by your Private Cloud device to verify SSL certificates and connections.

[Add Certificate Authority](#)

| Certificate | | | | (click to collapse) |
|-------------|-------------------------|---|--|-------------------------|
| Issuer | rootca_vpc | | Download Delete | |
| Subject | rootca_vpc | | | |
| Validity | 2020-11-15 00:00:00 UTC | - | | 2025-11-14 23:59:59 UTC |
| Certificate | | | | (click to collapse) |
| Issuer | rootca_vpc | | Download Delete | |
| Subject | subca-dus | | | |
| Validity | 2020-12-05 12:01:00 UTC | - | | 2023-12-05 12:01:00 UTC |

| Details | Validity |
|--|----------------------------|
| Subject: CN=rootca_vpc Issuer: CN=rootca_vpc Fingerprint: 66:BF:EB:63:36:9F:AC:E9:39:AD:76:A4:0E:5A:57:B1:45:B9:FD:A4:FD:63:7E:5A:11:FF:47:AA:CC:1E:FF:F2 | 2020-11-1 Valid for alr |
| Sub Issu Fing | -03-0 for ab |
| Sub Issu Fing | -03-2 for ab |
| Sub Issu Fing | -07-2 for ov |
| Sub Issu Fing | -03-0 for ab |
| Subject: CN=subca-dus Issuer: CN=rootca_vpc Fingerprint: 51:D5:74:9A:6C:44:4B:1A:E9:45:93:CB:B6:7C:3A:EB:7B:8B:BD:04:51:4D:79:8E:D4:23:35:92:C0:17:9D:5C | 2020-12-0 Valid for alr |

[Add Certificate](#) [Lookup Certificate](#)

- AMPFQDNThreat Grid“(Administration)>“AMP”(Manage AMP Private Cloud Integration)AMPIPFQDN

https://dupdateamp3.argarci2-lab

disposition_update_user

ew236 [redacted] xJYfPK

AMP私有云设备中有关无效Threat Grid SSL证书警告

症状

警告消息：“Threat Grid SSL证书无效”，在选择“集成”>“Threat Grid”中的“测试连接”按钮后，将在AMP私有云设备中收到。

Threat Grid Connection test failed.

- Threat Grid SSL Certificate is invalid.
- Threat Grid API key could not be tested.

推荐步骤：

- 确认Threat Grid设备安全界面中安装的证书是否由公司CA签名。

如果由CA签名，则必须将完整的证书链添加到文件中，添加到Threat Grid SSL证书中的AMP私有云设备管理门户Integrations > Threat Grid。

Threat Grid Configuration Details Edit

Hostname

API Key

Threat Grid SSL Certificate

| | | |
|----------|--|-------------------------|
| Issuer | subca_tga_clean | |
| Subject | <input type="text" value="cisco.com"/> | |
| Validity | 2020-11-24 00:00:00 UTC | 2021-11-23 23:59:59 UTC |

Test Connection

在AMP私有云设备中，当前安装的Threat Grid设备证书位于：`/opt/fire/etc/ssl/threat_grid.crt`。

Threat Grid设备中与证书相关的警告

警告消息 — 从私钥派生的公钥不匹配

症状

警告消息：从私钥派生的公钥不匹配，在尝试向接口添加证书后，会在Threat Grid设备中接收。

The screenshot shows the 'Upload SSL certificate for PANDEM' page in the Threat Grid Appliance interface. The left sidebar contains a navigation menu with 'SSL' selected. The main content area has two text input fields for 'Certificate (PEM)' and 'Private Key (PEM)'. Both fields contain long alphanumeric strings and are partially obscured by black redaction boxes. Below the fields, a red error message reads: 'public key derived from private key does not match'. At the bottom, there are 'Add Certificate' and 'Cancel' buttons.

从私钥导出的公钥与证书中配置的公钥不匹配。

推荐步骤：

- 确认私钥是否与证书中的公钥匹配。

如果私钥与证书中的公钥匹配，则模数和公共指数必须相同。对于此分析，只需确认私钥中的模数值与证书中的公钥值是否相同即可。

步骤1.使用OpenSSL工具比较私钥中的系数和证书中配置的公钥。

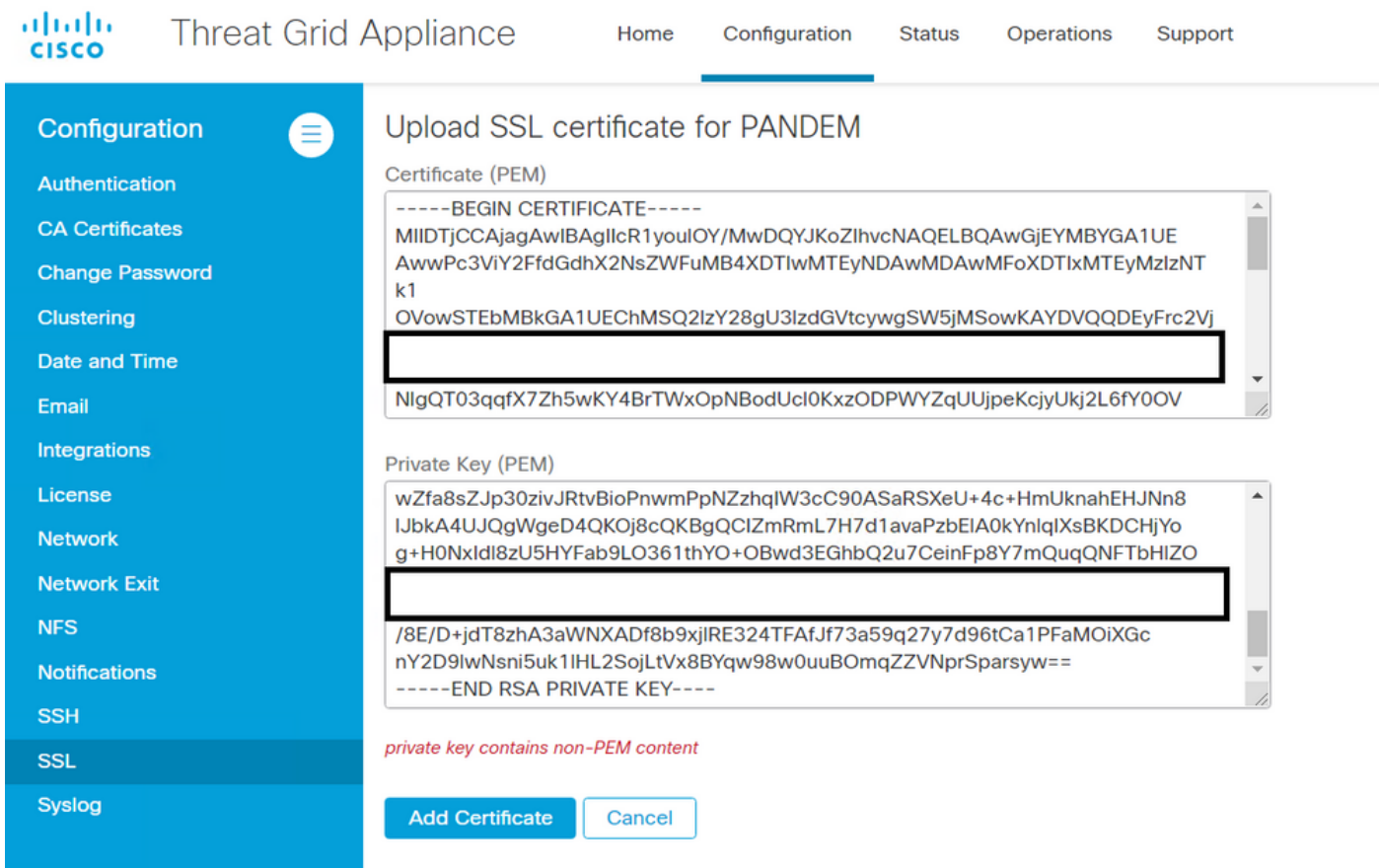
```
openssl x509 -noout -modulus -in
```

```
$ openssl x509 -noout -in certificate.cert | openssl md5
(stdin)= d41d8cd98f00b204e9800998ecf8427e
$
$
$ openssl rsa -noout -in private-key.key | openssl md5
(stdin)= d41d8cd98f00b204e9800998ecf8427e
```

警告消息 — 私钥包含非PEM内容

症状

警告消息：私钥包含非PEM内容，在尝试向接口添加证书后，会在Threat Grid设备中接收该内容。



私钥文件中的PEM数据已损坏。

推荐步骤：

-

步骤1.使用OpenSSL工具验证私钥的完整性。

```
openssl rsa -check -noout -in  
PEMPEM
```

```
$ openssl rsa -check -noout -in wrong-private-key.key  
unable to load Private Key  
140333463315776:error:09091064:PEM routines:PEM_read_bio_ex:bad base64 decode:../crypto/pem/pem_lib.c:929:
```

```
$ openssl rsa -check -noout -in correct-private-key.key  
RSA key ok
```

如果OpenSSL命令输出不是**RSA Key ok**，则意味着在密钥内的PEM数据中发现了问题。

如果OpenSSL命令发现问题，则：

- 确认私钥中是否缺少PEM数据。

私钥文件中的PEM数据以64个字符的行显示。快速查看文件内的PEM数据可显示数据是否丢失。缺少数据的行与文件中的其他行不对齐。

```
$ cat wrong-private-key.key  
-----BEGIN PRIVATE KEY-----  
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCbKYwggSiAgEAAoIBAQCvfIytwkf9UIc5  
DlUk9PTbKvDrShgn8/Cen9wXEUDIBNahlfizvwZb/5FL+I1ry/P0WKJMiXRhLQ52  
Y0oogQsuDTw79Moa6xXYLKq1P5QRIV6tQQDNiHUoHFNSLkoo0H0ubkDtGo/PW4fE  
/JNGbMIU/d1DDuzxfGze0viztT90rpCbZyQP2r+sGxaOKM0c3AEgK/pYA7aCv/G  
P6rGkHc/ViM1NTuWVIWdIcLgTUX0DeHLjTIcI2q/vH/i0WeIgAv10aGuBCOeg <-----  
NwOgPyY3XI8g7l 4HA6/VsM10NHKT4EhvSks  
WXZW1XhNAGMBA tU9huSCL7t4BF7VpSeKXM  
Uh4/Vrdg1TYXfi s7k0sCwmhKUaMacTYAnrg  
fINIJto/x0azh 47ttvLvX3zweLCEXsDXK6  
mdhzCQSTBfYbM. 4M7HiocsbkLjijScTFYQ  
JqSwA5BEgqeH3. 4gd4kJ6ddAaSjQS7sJxaf  
WtVHzbVDqJ+rb' 43gQDePpxacxGRZLXfja3s  
SU+TvjNWQGcUs. 48y8ZQd0lqPZrV0Z6Mym2  
i5S+/LS4jHB5hcCfnZpL4M0zHYvX+HPuGHm2xOCy51K5KsfDPa/SrbhDkxZty0SG  
lCgVLEycQ5t1xtI6qiBLKNmtrQKBgQDKI+BTMrHFYD50gPcBZyGXVhmSyHcZOP9k  
OosXngeKtpdqL8Ck/H2QftFpOAFoHQxD/tiJA6E1eK9HfVnsq9+xbCU1fRlPxeCS  
CbcflDYBwaMn8Ywp9PfZKPgu/gI3XIUWT6T0LcBGtdspYDEbApvYA091PoS0vcBn  
g7LG+bcJIQKBgHFn/ZziDtrkSzJSN6fVGPhJHCutI+yZRuBkkz/8ohv1Rf+En+VY  
9QG0GBq/MEBZy3TV+SUYfPX1SQ9eQDDYNQToKsfpUHQvuQ0JeIGSm+E6jFApNeg  
QauT9x0TkVDP1bP5LFkTMG27Brzr9oG95F45hrZ0gW0D+w7YdTYlGD7ZAoGASHku  
b4XoeNS1771hUg5w27qR9q+LC+8EmiHnRrNxDsnCzd7zGfQw7MKbQDdFQdfQUvyn  
FBDKFsrlRT1rJVDGJe2ZNaE/QmE20AVNs7PG3UBYx/RxhYV/60smGGsXz10Mn+A0  
SxuwKWoARshnMsDvsTYwofm1SMwTlMmCKpbTiiECgYBi8ZjgsdFv2NtYlmb1pAYS  
DHierblDtVumF42Tax+fucqUrdB3LZo6FjagvPy+LBjA3VjtRYkDjQmstvxD5jfd  
V3Pq4IwaocGU8RQUJY5L6rmw+y1s6Z+iNkIcPeZtWidSgP+NZa1xvhfj8XeL560o  
a+IQn0Y41zLJ22ScgyFzEQ==  
-----END PRIVATE KEY-----
```


• 确认私钥中的第一行以5个连字符开头，单词BEGIN PRIVATE KEY，以5个连字符结束。
示例。

— 开始私钥 —

• 确认私钥中最后一行以5个连字符开头，单词END PRIVATE KEY，以5个连字符结尾。
示例。

— 最终私钥 —

示例。正确的PEM格式和私钥内的数据。

```
$ cat correct-private-key.key
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCbKYYggSiAgEAAoIBAQCvfIytwkf9UIc5
DluK9PTbKvDrShgn8/Cen9wXEUDIBNahlFiZvwZb/5FL+I1ry/P0WKJMiXRhLQ52
Y0oogQsuDTw79Moa6xXYLKq1P5QRIV6tQQDNiHUoHFNSLkoo0H0ubkDtGo/Pw4fE
/JNGbMIU/d1DDuzxfGze0viztT90rpCbZyQP2r+sGxa0KM0c3AEgK/pYA7aCv/G
P6rGkHc/ViM1NTuWVIWdIcLgTUX0DeHLjTicI2q/vH/i0WeIgAv10aGuBC0egVDU
NwOgPyY3XI8g7H [REDACTED] 4HA6/VsM10NHKT4EhvSks
WXZW1XhNAGMBA [REDACTED] tU9huSCL7t4BF7VpSeKXM
Uh4/Vrdg1TYXfB [REDACTED] s7k0sCwmhKUaMAcTYAnrg
fINIJto/x0azhe [REDACTED] 47ttvLvX3zweLCEXsDXK6
mdhzCQSTBfYbM4 [REDACTED] R4M7HiocsbkLjiJScTFYQ
JqSwA5BEgqeH3a [REDACTED] hgd4kJ6ddAaSjQS7sJxaf
WtVHzbVDqJ+rb9 [REDACTED] BgQDePpxacxGRZLXfja3s
SU+TvjNWQGCUsX [REDACTED] a8y8ZQd0lqPZrV0Z6Mym2
i5S+/LS4jHB5hcCfnZpL4M0zHYvX+HPuGHm2x0Cy51K5KsfdPa/SrbhDkxZty0SG
lCgVLEycQ5t1xtI6qiBLKNmtrQKBgQDKI+BTMrHFYD50gPcBZyGXVhmSyHcZOP9k
OosXngeKtpdqL8Ck/H2QftFp0AFoHQxD/tiJA6E1eK9HfVnsq9+xbCU1fRLPxeCS
Cbcf1DYBwaMn8Ywp9PfZKPgu/gI3XIUWT6T0LcBGtdspYDEbApvYA091PoS0vcBn
g7LG+bcJIQKBGHFn/ZziDtrkSzJSN6fVGPhJHCutI+yZRuBkkz/8ohv1Rf+En+VY
9QG0GBq/MEBZy3TV+SUYfPX1SQ9eQDDYNQToKsfpUh0QvuQ0JeIGSm+E6jFApNeg
QauT9x0TkVDP1bP5LFkTMG27Brzr9oG95F45hrZ0gwOD+w7YdTY1GD7ZAoGASHku
b4XoeNS1771hUg5w27qR9q+LC+8EmiHnRrNxDsncZd7zGfQw7MKbQDdFQdfQUvyn
FBDKFsrLRT1rJVDGJe2ZNaE/QmE20AVNs7PG3UBYx/RxhYV/60smGGsXz10Mn+A0
SxuwKWoARshnMsDvsTYwofm1SMwT1MmCKpbTiiECgYBi8ZjgsdFv2NtYlmb1pAYS
DHiErbldtVumF42Tax+fucqUrdB3LZo6FjagvPy+LBjA3VjtRYkDjQmstvxD5jfd
V3Pq4IwaocGU8RQUJY5L6rmw+y1s6Z+iNkIcPeZtwidSgP+NZa1xvhfj8XeL560o
a+IQn0Y41zLJ22ScgyFzEQ==
-----END PRIVATE KEY-----
```

警告消息 — 无法从私钥生成公钥

症状

警告消息：无法从私钥生成公钥，在尝试向接口添加证书后，会在Threat Grid设备中接收公钥。

Configuration

- Authentication
- CA Certificates
- Change Password
- Clustering
- Date and Time
- Email
- Integrations
- License
- Network
- Network Exit
- NFS
- Notifications
- SSH
- SSL**
- Syslog

Upload SSL certificate for PANDEM

Certificate (PEM)

```
AN
BgkqhkiG9w0BAQsFAAOCAQEAsCQ1iOkPkLj6A1R94eueZ64zCYGuf8wg0z2S9Kle
epjqQobaJadl3WTh7LMHuxHZP02YZJIO/OjUQ/8uLk1sG7rVE5ROe/Ev9OvjL5nF
[Redacted]
wbTboJukREZOyiBoQDPcSWHqe8j3FEtJlf9yfv2bthOFQQ+Lf3BU4ZPiXPVEtuUL
7FIP0kjC/33s5ZWpC8OzCmdPvFgx//JbpWr1gllYVs1uYg==
-----END CERTIFICATE-----
```

Private Key (PEM)

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAACAQEAucb3AU15P91Ym/PvHva/xKBCbLeY7+jQJGO7wm7eruX3KTZY
EE9N6qn1+2YecCmOAA01sTqTQaHVHJdCsczgz1mGalFI6Xinl8lJl9i+n2NDlcNr
XBVPvCUs5fnH2cZwKGTen/NDJhnyC5Dlb17RLy7Y+wxhMiyRCHH3aZ3l0Mpl1k4X
[Redacted]
cjSc9W8Fy/CDXbX27KncS4qWe91phsKXq0jo7wIDAQABAolBAFrH8EHRsvNTXY5v
yCSwXQtfALYpjXGGqdduaPzdlrICrCGWbbgimKeYQByGTU9v7vXAx2EAh57lzb2
```

cannot generate public key from private key

无法从私钥文件内的当前PEM数据生成公钥。

推荐步骤：

- 1.OpenSSL

```
openssl rsa -check -noout -in
```

如果OpenSSL命令输出不是RSA Key ok，则意味着在密钥内的PEM数据中发现了问题。

步骤2.使用OpenSSL工具验证公钥是否可以从私钥导出。

openssl rsa -in
 示例。公钥导出失败，公钥导出成功。

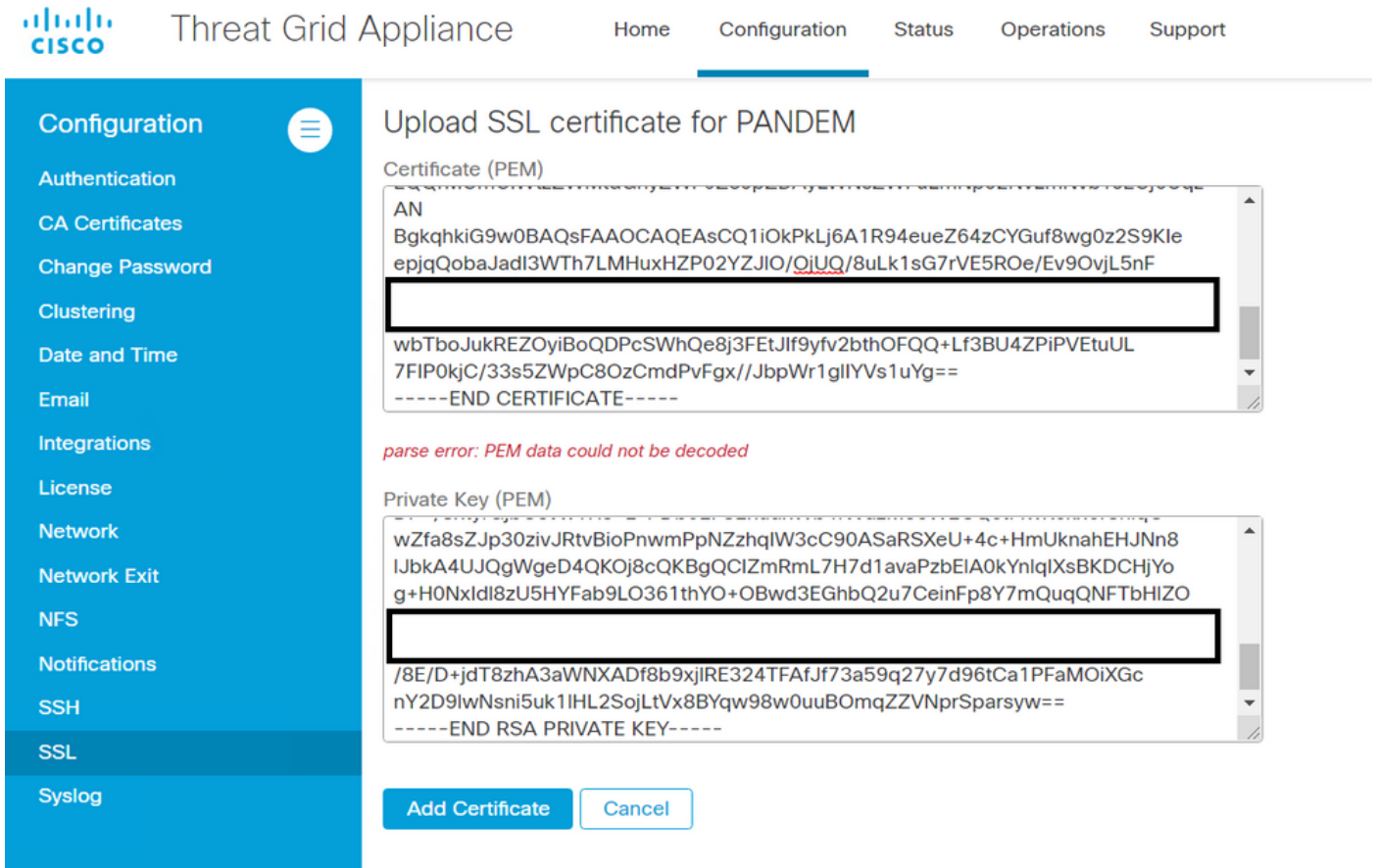
```
$ openssl rsa -in wrong-private-key.key -pubout
unable to load Private Key
140195161523520:error:09091064:PEM routines:PEM_read_bio_ex:bad base64 decode:../crypto/pem/pem_lib.c:929:

$ openssl rsa -in correct-private-key.key -pubout
writing RSA key
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAr3yMrcJH/VCH0Q5bivT0
2yrw60oYJ/Pwnp/cFxFayATWoZRYmb8GW/+RS/iNa8vz9FiiTII0YS0dmNKKIEL
Lg080/TKGusV2CyyqtT+UESFerUEAzYh1KBxTUi5KKNB9Lm5A7RqPz1uHxPyTRmzC
FP3dQw7s8X4Bs3tL4s7U/Tq6Qm2ckD9q/rBswjijNHNwBICv6WA02gr/xj+qxpB3
P1YjNTU7l1SFnSHC4E1Fzg3hy40yHCNqv7x/4jlniIAL9dGhrgQjnofQ1DcDoD8m
N1yPI0x3C0lweVForZmx+Dg6l+J4uIjytkVceBw0v1bDNdDRyk+BIB0pLF12VtV4
TQIDAQAB
-----END PUBLIC KEY-----
```

警告消息 — 解析错误：无法解码PEM数据

症状

警告消息：parse error:PEM数据无法解码，在尝试向接口添加证书后，会在Threat Grid设备中接收。



无法从证书文件内的当前PEM数据解码证书。证书文件中的PEM数据已损坏。

- 确认是否可以从证书文件内的PEM数据检索证书信息。

步骤1.使用OpenSSL工具显示PEM数据文件中的证书信息。

```
openssl x509 -in
```

如果PEM数据损坏，当OpenSSL工具尝试加载证书信息时，会发现错误。

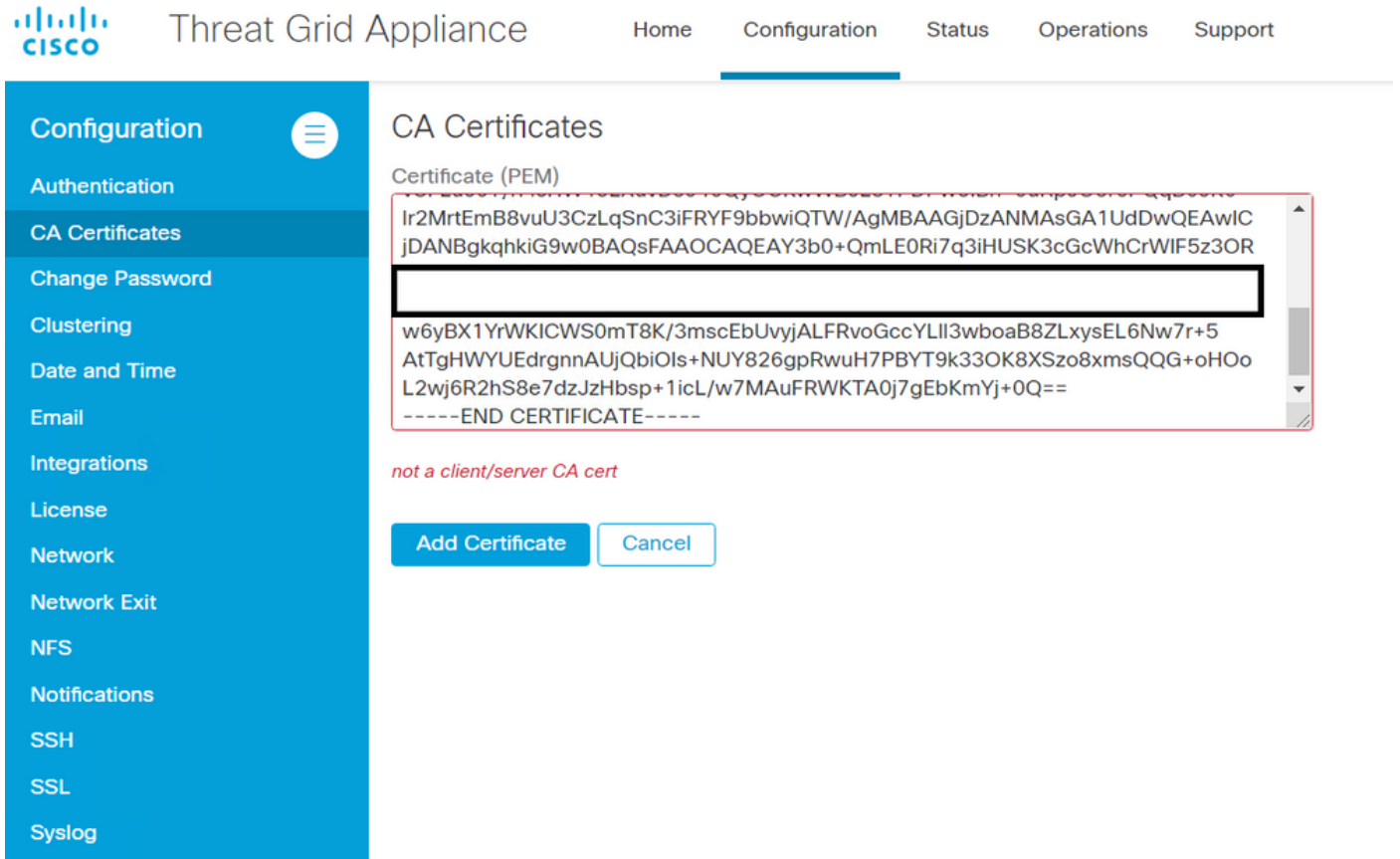
示例。由于证书文件中的PEM数据损坏，尝试加载证书信息失败。

```
$ openssl x509 -in wrong-certificate.cert -text -noout
unable to load certificate
140159319831872:error:09091064:PEM routines:PEM_read_bio_ex:bad base64 decode:../crypto/pem/pem_lib.c:929:
```

警告消息 — 不是客户端/服务器CA证书

症状

警告消息：parse error:尝试将CA证书添加到Configuration > CA Certificates后，在Threat Grid设备中将收到客户端/服务器CA证书，而不是证书。



CA证书中的基本约束扩展值未定义为CA:没错。

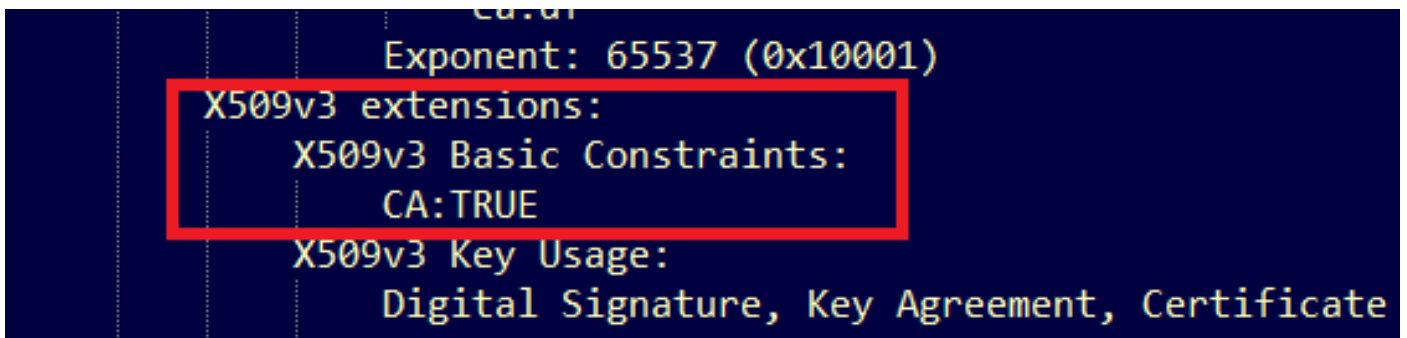
使用OpenSSL工具确认Basic Constraints扩展值是否设置为CA:在CA证书中为True。

步骤1.使用OpenSSL工具显示PEM数据文件中的证书信息。

```
openssl x509 -in
```

步骤2.在证书信息中搜索基本约束扩展的当前值。

示例。Threat Grid设备接受的CA的基本约束值。



相关信息

- [Threat Grid设备 — 配置指南](#)
- [思科AMP虚拟私有云设备 — 配置示例和技术说明](#)
- [技术支持和文档 - Cisco Systems](#)