

AMP仮想プライベートクラウドとThreat Gridアプライアンスの統合

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[統合のアーキテクチャ](#)

[統合に関する基本情報](#)

[手順](#)

[SSL証明書の再生成](#)

[SSL証明書のアップロード](#)

[Threat Gridアプライアンスのクリーンインターフェイスの証明書は自己署名です](#)

[Threat Gridアプライアンスのクリーンインターフェイス内の証明書は、企業の認証局\(CA\)によって署名されます](#)

[例](#)

[確認](#)

[AMPプライベートクラウドデータベースのサンプル廃棄更新の確認](#)

[例](#)

[トラブルシューティング](#)

[AMPプライベートクラウドデバイスで、ホストが無効、証明書がテストされていない、APIキーがテストされていないという警告が表示される](#)

[無効なThreat Grid APIキーに関するAMPプライベートクラウドデバイスの警告](#)

[サンプルスコア>=95はAMPプライベートクラウドデバイスで受信されますが、サンプルの配置に変化は見られません](#)

[AMPプライベートクラウドデバイスで、無効なThreat Grid SSL証明書に関する警告](#)

[証明書に関連するThreat Gridアプライアンスの警告](#)

[警告メッセージ – 秘密キーから派生した公開キーが一致しません](#)

[警告メッセージ：秘密キーに非PEMコンテンツが含まれています](#)

[警告メッセージ – 秘密キーから公開キーを生成できません](#)

[警告メッセージ – 解析エラー：PEMデータをデコードできませんでした](#)

[警告メッセージ：クライアント/サーバCA証明書ではありません](#)

[関連情報](#)

このドキュメントでは、Advanced Malware Protection(AMP)仮想プライベートクラウドとThreat Gridアプライアンスの統合を完了する手順について説明します。このドキュメントでは、統合プロセスに関連する問題のトラブルシューティング手順について説明します。

著者：Cisco TACエンジニア、Armando Garcia

次の項目に関する知識があることが推奨されます。

- AMP仮想プライベートクラウドの運用
- Threat Gridアプライアンスの運用と運用

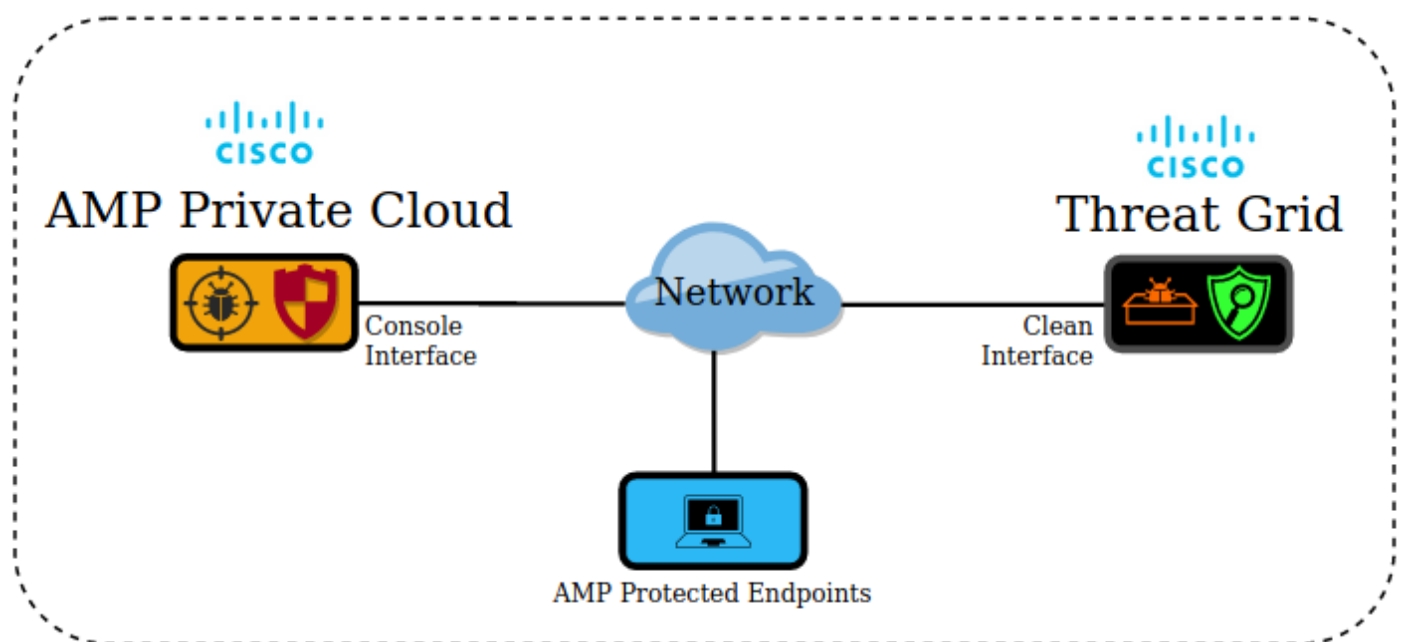
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- AMPプライベートクラウド3.2.0
- Threat Gridアプライアンス2.12.0.1

注：このドキュメントは、アプライアンスまたは仮想バージョンのThreat GridアプライアンスおよびAMPプライベートクラウドデバイスに対して有効です。

背景説明

統合のアーキテクチャ



統合に関する基本情報

- Threat Gridアプライアンスは、AMPプライベートクラウドデバイスから送信されたサンプルを分析します。
- サンプルは、手動または自動でThreat Gridアプライアンスに送信できます。
- AMPプライベートクラウドデバイスでは、自動分析はデフォルトでは有効になっていません。
- Threat Gridアプライアンスは、サンプルの分析からレポートとスコアをAMPプライベートクラウドデバイスに提供します。

- Threat Gridアプライアンスは、スコアが95以上のサンプルについてAMPプライベートクラウドデバイスに通知 (ポーク) します。
- 分析のスコアが95以上の場合、AMPデータベース内のサンプルには悪意のある処理がマークされます。
- レトロスペクティブ検出は、AMPプライベートクラウドによって、スコアが95以上のサンプルに適用されます。

手順

ステップ1:Threat Gridアプライアンスをセットアップして設定します (まだ統合されていません)。必要に応じて、アップデートを確認してインストールします。

ステップ2 : エンドポイントのプライベートクラウド用AMPをセットアップして設定します (まだ統合されていません)。

ステップ3:Threat Grid管理UIで、[Configuration]タブを選択し、[SSL]を選択します。

ステップ4 : クリーンインターフェイス(PANDEM)の新しいSSL証明書を生成またはアップロードします。

SSL証明書の再生成

新しい自己署名証明書は、クリーンインターフェイスのホスト名が、そのクリーンインターフェイスのアプライアンスに現在インストールされている証明書のサブジェクト代替名(SAN)と一致しない場合に生成できません。アプライアンスがインターフェイスの新しい証明書を生成し、自己署名証明書のSANフィールドに現在のインターフェイスのホスト名を設定します。

ステップ4.1:[アクション(Actions)]列で(...)を選択し、ポップアップメニューから[新しい証明書の生成(Generate New Certificate)]を選択します。

ステップ4.2:Threat Grid UIでOperationsを選択し、次の画面でActivateを選択してReconfigureを選択します。

注 : この生成された証明書は自己署名です。

SSL証明書のアップロード

Threat Gridアプライアンスのクリーンインターフェイス用に証明書がすでに作成されている場合、この証明書をアプライアンスにアップロードできます。

ステップ4.1:[アクション(Actions)]列で(...)を選択し、ポップアップメニューから[新規証明書のアップロード(Upload New Certificate)]を選択します。

ステップ4.2 : 画面に表示されるテキストボックスに証明書と対応する秘密キーをPEM形式でコピーし、[Add Certificate]を選択します。

ステップ4.3:Threat Grid UIでOperationsを選択し、次の画面でActivateを選択してReconfigureを

選択します。

ステップ5:AMPプライベートクラウドデバイスの管理UIで、[統合]を選択し、[脅威グリッド]を選択します。

ステップ6:[Threat Grid Configuration Details]で、[Edit]を選択します。

ステップ7:[Threat Grid Hostname]に、Threat GridアプライアンスのクリーンインターフェイスのFQDNを入力します。

ステップ8:Threat Grid SSL証明書で、Threat Gridアプライアンスのクリーンインターフェイスの証明書を追加します。(以下の注を参照)

Threat Gridアプライアンスのクリーンインターフェイスの証明書は自己署名です

ステップ8.1:Threat Grid管理UIで、[Configuration]を選択し、[SSL]を選択します。

ステップ8.2:[アクション(Actions)]列で(...)を選択し、ポップアップメニューで[証明書のダウンロード(Download Certificate)]を選択します。

ステップ8.3:ダウンロードしたファイルをThreat Grid統合ページのAMP仮想プライベートデバイスに追加します。

Threat Gridアプライアンスのクリーンインターフェイス内の証明書は、企業の認証局(CA)によって署名されます

ステップ8.1:テキストファイルに、Threat Gridアプライアンスのクリーンインターフェイスと完全なCA証明書チェーンの証明書をコピーします。

注:テキストファイルの証明書はPEM形式である必要があります。

完全な証明書チェーンがROOT_CA certificate > Threat_Grid_Clean_Interface certificate;次に、図に示すように、テキストファイルを作成する必要があります。



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

完全な証明書チェーンがROOT_CA certificate > Sub_CA Certificate > Threat_Grid_Clean_Interface certificate;次に、図に示すように、テキストファイルを作成する必要があります。

```
-----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 Grid API]Threat 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：Threat Gridユーザーのアカウント設定で、[Disable API Key]パラメータが[True]に設定されていないことを確認します。

ステップ10：すべての変更が完了したら、[Save]を選択します。

ステップ11:AMP仮想クラウドデバイスに再設定を適用します。

ステップ12:AMPプライベートクラウドデバイスの管理UIから、[統合]を選択し、[脅威グリッド]を選択します。

ステップ13:「詳細」から、廃棄更新サービスURL、廃棄更新サービスのユーザーおよび廃棄更新サービスのパスワードの値をコピーします。この情報は、ステップ17で使用します。

ステップ14:Threat Grid管理UIで、[Configuration]を選択し、[CA Certificates]を選択します。

ステップ15:[Add Certificate]を選択し、AMP Private Cloud Disposition Update Service証明書に署名したCA証明書をPEM形式でコピーします。

注：AMPプライベートクラウド廃棄更新証明書に署名したCA証明書がサブCAである場合は、チェーン内のすべてのCAがCA証明書にアップロードされるまで、このプロセスを繰り返します。

ステップ16:Threat Gridポータルで、[Administration]を選択し、[Manage AMP Private Cloud Integration]を選択します。

ステップ17:[Disposition Update Syndication Service]ページで、ステップ13で収集した情報を入力します。

- サービスURL:AMPプライベートクラウドデバイスの廃棄更新サービスのFQDN。
- ユーザ：AMPプライベートクラウドデバイスのDisposition Update Serviceのユーザ。
- パスワード：AMPプライベートクラウドデバイスの廃棄更新サービスのパスワード。

この時点ですべての手順が正しく適用されていれば、統合は正常に動作している必要があります。

確認

Threat Grid

注：手順1、2、3、4のみを実稼働環境に適用して統合を検証するのに適しています。ステップ5は、統合に関する詳細を知るための情報として提供され、実稼働環境に適用することは推奨されません。

1:[AMP Private Cloud Device Admin UI] > [Integrations] > [Threat Grid][Test Connection]Threat Grid Connection test successful!

Threat Grid Configuration Details		Edit
Hostname	<input type="text" value=""/> .cisco.com	
API Key	<input type="text" value=""/> <input type="button" value=""/>	
Threat Grid SSL Certificate		<input type="button" value="Test Connection"/>
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

✔ Threat Grid Connection test successful!

2:AMPWeb



AMP for Endpoints



armando garcia ▾

File Analysis

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



Submit File



There are no File Analyses to view

ステップ3:AMPプライベートクラウドコンソールの[Analysis] > [File Analysis]から手動で送信されたファイルがThreat Gridアプライアンスで認識され、スコアのレポートがThreat Gridアプライアンスによって返されることを確認します。



AMP for Endpoints



armando garcia ▾

✔ 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



AMP for Endpoints



armando garcia ▾

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

ステップ4:AMPプライベートクラウドデバイスの廃棄更新サービス証明書に署名したCAが、認証

局のThreat Gridアプライアンスにインストールされていることを確認します。

ステップ5：スコアが95より大きいThreat Gridアプライアンスでマークされたサンプルが、レポートの後に悪意のある状態でAMPプライベートクラウドデータベースに記録され、サンプルスコアがThreat Gridアプライアンスによって提供されることを確認します。

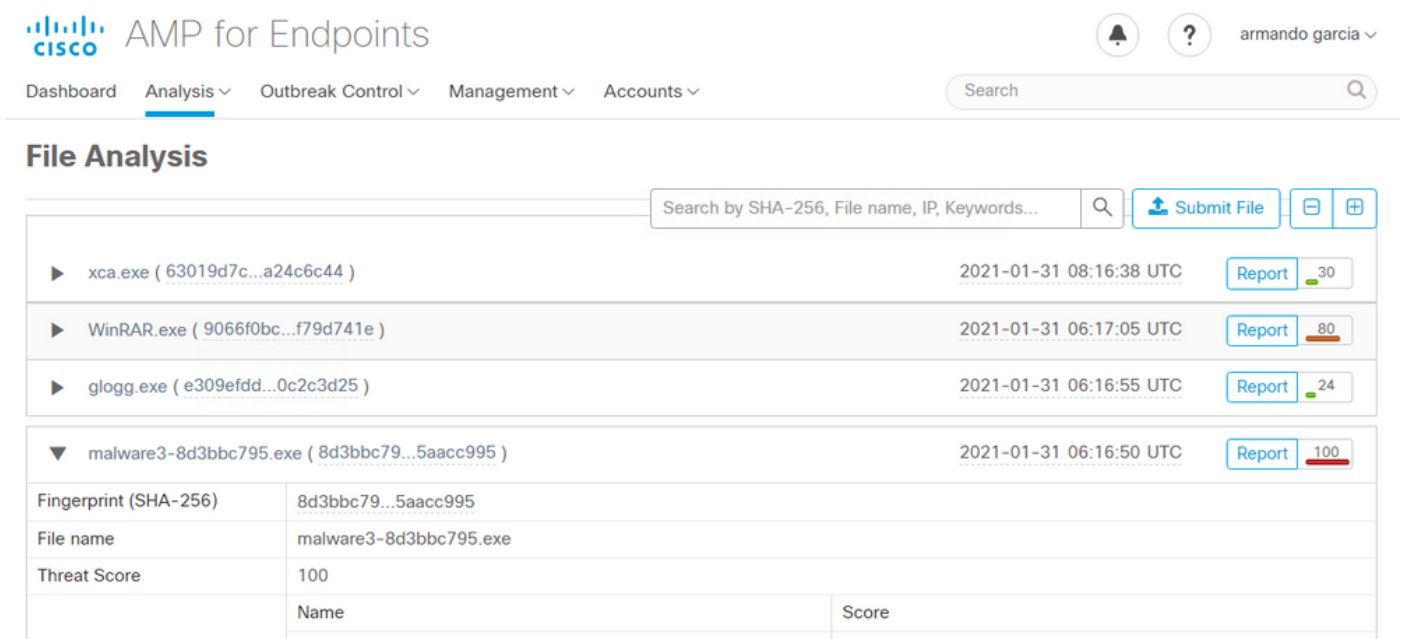
注：AMPプライベートクラウドコンソールの[ファイルの分析]タブでサンプルレポートと ≥ 95 サンプルスコアを正常に受信した場合は、必ずしもファイルの性質がAMPデータベースで変更されたことを意味するものではありません。AMPプライベートクラウドデバイスの廃棄更新サービス証明書に署名したCAがThreat Gridアプライアンスの認証局にインストールされていない場合、レポートとスコアはAMPプライベートクラウドデバイスで受信されますが、Threat Gridアプライアンスからは受信されません。

警告：次のテストは、Threat Gridアプライアンスが ≥ 95 スコアのファイルをマークした後で、AMPデータベースのサンプルのディスポジション変更をトリガーするために完了しました。このテストの目的は、Threat Gridアプライアンスが ≥ 95 のサンプルスコアを提供する際のAMPプライベートクラウドデバイスの内部動作に関する情報を提供することでした。廃棄の変更プロセスをトリガーするために、Cisco internal makemalware.exeアプリケーションでマルウェア模倣テストファイルをしました。例：malware3-419d23483.exeSHA256:8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995

注意：実稼働環境でマルウェア模倣テストファイルをデトネーションすることは推奨されません。

AMPプライベートクラウドデータベースのサンプル廃棄更新の確認

AMP Threat Grid Threat Grid AMP 100 ≥ 95 AMP Threat Grid ≥ 95 AMP



File Analysis

File Name	Threat Score	Time
xca.exe (63019d7c...a24c6c44)	30	2021-01-31 08:16:38 UTC
WinRAR.exe (9066f0bc...f79d741e)	80	2021-01-31 06:17:05 UTC
glogg.exe (e309efdd...0c2c3d25)	24	2021-01-31 06:16:55 UTC
malware3-8d3bbc795.exe (8d3bbc79...5aacc995)	100	2021-01-31 06:16:50 UTC

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

条件

- 統合は正常に完了しました。

- サンプルレポートとスコアは、ファイルを手動で送信した後にファイル分析で認識されます。

次に実行するコマンド

- Threat Gridアプライアンスでスコア \geq 95とマークされた各サンプルに対して、AMPプライベートクラウドデバイスのファイル/data/poked/poked.logにエントリが追加されます。
- /data/poked/poked.logは、最初の \geq 95サンプルスコアがThreat Gridアプライアンスによって提供された後、AMPプライベートクラウドデバイスで作成されます。
- AMPプライベートクラウドのdb_protectデータベースには、サンプルの現在の性質が保持されます。この情報を使用して、Threat Gridアプライアンスがスコアを提示した後で、サンプルの処分が3であるかどうかを確認できます。

サンプルレポートと \geq 95スコアがAMPプライベートクラウドコンソールのファイル分析で認識される場合は、次の手順を適用します。

ステップ1:SSH経由でAMPプライベートクラウドデバイスにログインします。

ステップ2 : サンプルのエントリが/data/poked/poked.logにあることを確認します。

Threat Gridアプライアンスから \geq 95のサンプルスコアを受信したことがないAMPプライベートクラウドデバイスの/data/poked/ディレクトリを表示すると、poked.logファイルがシステムで作成されていないことを示します。

AMPプライベートクラウドデバイスがThreat GridアプライアンスからPOKEを受け取っていない場合、図に示すように、/data/poked/poked.logファイルがディレクトリに見つかりません。

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

最初の \geq 95サンプルスコアを受信した後の/data/poked/ディレクトリのリストは、ファイルが作成されたことを示しています。

最初のサンプルを受け取った後に \geq 95スコア。

```
[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":"W32.80389C7958-100.SBX.T6","ok":1,"time":1612031118,"hash":"8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951c1f7c5aacc995","engine":"sha256",
"user":"-", "mode":"tg", "score":100}
[root@fireamp ~]#
```

Threat Gridアプライアンスによって提供されるPOKEからのサンプル情報は、poked.logファイル内で認識できます。

ステップ3 : サンプルSHA256を使用してこのコマンドを実行し、AMPプライベートクラウドデバイスのデータベースから現在の状態を取得します。

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

例

サンプルがThreat Gridアプライアンスにアップロードされる前にサンプルの処分を取得するため

のデータベースクエリは、図に示すように結果を提供しません。

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

Threat Gridアプライアンスからレポートとスコアを受信した後でサンプルのディスポジションを取得するデータベースクエリは、悪意があると見なされるディスポジション3のサンプルを示しません。

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

トラブルシューティング

統合プロセスでは、考えられる問題が認識される可能性があります。このドキュメントのこの部分では、最も一般的な問題のいくつかを取り上げています。

AMPプライベートクラウドデバイスで、ホストが無効、証明書がテストされていない、APIキーがテストされていないという警告が表示される

症状

警告メッセージ：Threat Gridホストが無効です。Threat Grid SSL Certificate could not be tested, Threat Grid API key could not be tested, is received in the AMP Private Cloud device after is selected in **Integrations > Threat Grid**.

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.

統合のネットワークレベルに問題があります。

推奨手順：

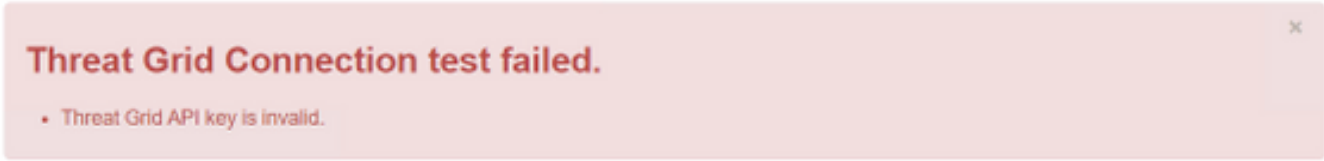
- AMPプライベートクラウドデバイスコンソールインターフェイスがThreat Gridアプライアンスのクリーンインターフェイスに到達できることを確認します。
- AMPプライベートクラウドデバイスがThreat GridアプライアンスのクリーンインターフェイスのFQDNを解決できることを確認します。
- AMPプライベートクラウドデバイスとThreat Gridアプライアンスのネットワークパスにフィルタリングデバイスがないことを確認します。

Threat Grid APIAMP

症状

警告メッセージ：Threat Grid Connectionテストが失敗しました。Threat Grid APIが無効です。
[統合] > [脅威グリッド]で[接続のテスト]ボタンを選択した後にAMPプライベートクラウドデバイスで受信されます。

Connect Threat Grid Appliance to AMP for Endpoints Appliance



AMPThreat GridAPI

推奨手順：

- Threat Gridアプライアンスユーザのアカウント設定で、[Disable API Key]パラメータが [True]に設定されていないことを確認します。
 - Disable API Keyパラメータは次のように設定する必要があります。FalseまたはUnset。

API

API Key *****

Disable API Key True False Unset

Can Download Sample Content Via API True False Unset

- AMPプライベートクラウド管理ポータルで設定されたThreat Grid APIキーが、Threat Gridアプライアンスのユーザ設定で同じAPIキーであることを確認します。
- 正しいThreat Grid APIキーがAMPプライベートクラウドデバイスデータベースに保存されているかどうかを確認します。

AMPプライベートクラウドデバイスのコマンドラインから、AMPデバイスで設定されている現在のThreat Grid APIキーを確認できます。SSH経由でAMPプライベートクラウドデバイスにログインし、次のコマンドを実行して現在のThreat GridユーザAPIキーを取得します。

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

これは、Threat GridアプライアンスAPIキー用のAMPプライベートクラウドデバイスのデータベース内の正しいエントリです。

```
[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 |
+-----+-----+-----+
```

統合のどのステップでもThreat Gridユーザ名がAMPプライベートクラウドデバイスで直接設定されていなかったとしても、Threat Grid APIキーが正しく適用されていれば、Threat Gridユーザ名

はAMPデータベースのtg_loginパラメータで認識されます。

これは、Threat Grid APIキーのAMPデータベースの誤ったエントリです。

```
[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_loginNULLThreat GridAMPThreat Grid

サンプルスコア>=95はAMPプライベートクラウドデバイスで受信されますが、サンプルの配置に変化は見られません

症状

レポートおよび>=95のサンプルスコアは、サンプルの送信後にThreat Gridアプライアンスから正常に受信されますが、AMPプライベートクラウドデバイスではサンプルの配置に変更は認識されません。

推奨手順：

- サンプルSHA256が/data/poked/poked.logの内容である場合は、AMPプライベートクラウドデバイスで確認します。

SHA256が/data/poked/poked.logにある場合は、次のコマンドを実行して、AMPデータベース内の現在のサンプル配置を確認します。

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

- [管理] > [AMPプライベートクラウド統合の管理]で、正しいAMPプライベートクラウド統合パスワードがThreat Gridアプライアンス管理ポータルに追加されたことを確認します。

AMPプライベートクラウド管理ポータル。

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"/> Change Password

Threat Gridアプライアンスコンソールポータル。



Disposition Update Syndication Service

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" value=""/>	disposition_update_user	Edit Remove

- AMPプライベートクラウドデバイスのDisposition Update Service証明書に署名したCAが、CA証明書のThreat Gridアプライアンス管理ポータルにインストールされたことを確認します。

次の例では、AMPプライベートクラウドデバイスのDisposition Update Service証明書の証明書チェーンはRoot_CA > Sub_CA > Disposition_Update_Service証明書です。したがって、RootCAとSub_CAは、Threat GridアプライアンスのCA証明書にインストールする必要があります。

AMPプライベートクラウド管理ポータルの証明機関。



✖ **Sanity Check Failing**

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	-	
Certificate (click to collapse)			
Issuer	rootca_vpc		Download Delete
Subject	subca-dus		
Validity	2020-12-05 12:01:00 UTC	-	

Configuration

Authentication

CA Certificates

Change Password

Clustering

Date and Time

Email

Integrations

License

Network

Network Exit

NFS

Notifications

SSH

SSL

Syslog

CA Certificates

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 Fin	-03-0 for ab
Sub Issu Fin	-03-2 for ab
Sub Issu Fin	-07-2 for ov
Sub Issu Fin	-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

- AMPFQDNThreat Grid[(Administration)] > [AMP(Manage AMP Private Cloud Integration)]AMPIPFQDN

disposition_update_user

disposition_update_user

AMPプライベートクラウドデバイスで、無効なThreat Grid SSL証明書に関する警告

症状

警告メッセージ：「Threat Grid SSL certificate is invalid」がAMPプライベートクラウドデバイスで受信され、[Integrations] > [Threat Grid]で[Test Connection]ボタンを選択した後に受信されます。

Threat Grid Connection test failed.

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

推奨手順：

- Threat Gridアプライアンスのクリーンインターフェイスにインストールされた証明書が企業CAによって署名されているかどうかを確認します。

CAによって署名されている場合は、完全な証明書チェーンをファイル内でAMPプライベートクラウドデバイス管理ポータルIntegrations > Threat Grid SSL Certificateに追加する必要があります。

Threat Grid Configuration Details Edit

Hostname	<input type="text" value="cisco.com"/>
API Key	<input type="text" 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


AMPプライベートクラウドデバイスにインストールされている現在のThreat Gridアプライアンス証明書は、次の場所にあります。/opt/fire/etc/ssl/threat_grid.crt にアクセスしてください。

証明書に関連するThreat Gridアプライアンスの警告

警告メッセージ – 秘密キーから派生した公開キーが一致しません

症状

警告メッセージ：秘密キーから派生した公開キーが一致せず、証明書をインターフェイスに追加しようとした後に、Threat Gridアプライアンスで受信されます。


Threat Grid Appliance

[Home](#)
[Configuration](#)
[Status](#)
[Operations](#)
[Support](#)

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)

```
-----BEGIN CERTIFICATE-----
hvcNAQELBQADggEBAKXz8oIDWacWY5V0XSHWrQIMULAMNAE8OZIXNkuByG6vvhj
P
JkgjjU9xKrke5LCr+trWnr+qjZlc4ecVCm8FXBWUtr8BjHcimbHUbZIVLYp6WDxO

HMS37fv44R9Cir4pjUz0bc61HS4wo5PAfUyjPtO1Dy0dHia4zE3pH4X3D9rzQYYd
Cl6KJpevCJzFyoQW3ahTZoxr4F11I5wO3XcH41Q=
-----END CERTIFICATE-----
```

Private Key (PEM)

```
-----BEGIN RSA PRIVATE KEY-----
wZfa8sZJp30zivJrtvBioPnwmPpNZzhqIW3cC90ASaRSXeU+4c+HmUknahEHJNn8
IjBkA4UJQgWgeD4QKOj8cQKBgQCIZmRmL7H7d1avaPzbEIA0kYnlqIXsBKDCHjYo
g+H0Nxldl8zU5HYFab9LO361thYO+OBwd3EGhbQ2u7CeinFp8Y7mQuqQNFTbHIZO

/8E/D+jdT8zhA3aWNXADf8b9xjIRE324TFAfJf/3a59q27y/d96tCa1PFaMOiXGc
nY2D9lwNsn5uk1IHL2SojLtvx8BYqw98w0uuBOMqZZVNprSparsyw==
-----END RSA PRIVATE KEY-----
```

public key derived from private key does not match

Add Certificate
Cancel

秘密キーからエクスポートされた公開キーが、証明書に設定されている公開キーと一致しません

。

推奨手順：

- 秘密キーが証明書内の公開キーと一致するかどうかを確認します。

秘密キーが証明書内の公開キーと一致する場合、モジュラスと公開指数は同じである必要があります。この分析では、モジュラスの秘密キーと証明書の公開キーが同じ値であるかどうかを確認するだけで十分です。

ステップ1:OpenSSLツールを使用して、秘密キーのモジュラスと証明書に設定されている公開キーを比較します。

```
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
```

警告メッセージ：秘密キーに非PEMコンテンツが含まれています

症状

警告メッセージ：秘密キーには非PEMコンテンツが含まれており、証明書をインターフェイスに追加しようとする、Threat Gridアプライアンスで受信されます。

The screenshot shows the Cisco Threat Grid Appliance web interface. The navigation menu includes Home, Configuration, Status, Operations, and Support. The left sidebar shows the Configuration menu with options like Authentication, CA Certificates, Change Password, Clustering, Date and Time, Email, Integrations, License, Network, Network Exit, NFS, Notifications, SSH, SSL, and Syslog. The main content area is titled "Upload SSL certificate for PANDEM". It contains two text input fields: "Certificate (PEM)" and "Private Key (PEM)". The Certificate field contains a PEM-formatted certificate, and the Private Key field contains a PEM-formatted private key. Below the Private Key field, a red warning message states "private key contains non-PEM content". At the bottom of the form, there are two buttons: "Add Certificate" and "Cancel".

秘密キーファイル内のPEMデータが破損しています。

推奨手順：

-

ステップ1:OpenSSLツールを使用して、秘密キーの整合性を確認します。

```
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
```

OpenSSLコマンドの出力が**RSA Key ok**でない場合は、キー内のPEMデータに問題が見つかったことを意味します。

OpenSSLコマンドで問題が見つかった場合は、次のようになります。

- 秘密キー内のPEMデータが欠落しているかどうかを確認します。

秘密キーファイル内のPEMデータは、64文字の行で表示されます。ファイル内のPEMデータを一目で確認すると、データが欠落しているかどうかを確認できます。データが欠落している行は、ファイル内の他の行と整列していません。

```

$ cat wrong-private-key.key
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCbKYwggSiAgEAAoIBAQCvfIytwkf9UIc5
DluK9PTbKvDrShgn8/Cen9wXEUDIBNahlFiZvwZb/5FL+I1ry/P0WKJMiXRhLQ52
Y0oogQsuDTw79Moa6xXYLKq1P5QRIV6tQQDNIHUoHFNSLkoo0H0ubkDtGo/PW4fE
/JNGbMIU/d1DDuzxfGze0viztT90rpCbZyQP2r+sGxa0KM0c3AEgK/pYA7aCv/G
P6rGkHc/ViM1NTuWVIWdIcLgTUX0DeHLjTicI2q/vH/i0WeIgAv10aGuBCOeg      <-----
NwOgPyY3XI8g7l
WXZW1XhNAgMBA
Uh4/Vrdg1TYXfi
fINIJto/x0azh
mdhzCQSTBfYbM
JqSwA5BEgqeH3
WtVHzbVDqJ+rb
SU+TvjNWQGcUs:
4HA6/VsM10NHKT4EhvSks
tU9huSCL7t4BF7VpSeKXM
s7k0sCwmhKUaMacTYAnrg
47ttvLvX3zweLCEXsDXK6
r4M7HiocsbkLjijScTFYQ
rgd4kJ6ddAaSjQS7sJxaf
3gQDePpxacxGRZLXfja3s
a8y8ZQd0lqPZrV0Z6Mym2
i5S+/LS4jHB5hcCfnZpL4M0zHYvX+HPuGHm2xOCy51K5KsfDPa/SrbhDkxZty0SG
lCgVLEycQ5t1xtI6qiBLKNmtrQKBgQDKI+BTMrHFYD50gPcBZyGXVhmSyHcZOP9k
OosXngeKtpdqL8Ck/H2QftFpOAFoHQxD/tiJA6E1eK9HFVnsq9+xbCU1fRlPxeCS
Cbcf1DYBwaMn8Ywp9PfZKpgu/gI3XIUWT6T0LcBGtdspYDEbApvYA091PoS0vcBn
g7LG+bcJIQKBgHFn/ZziDtrkSzJSM6fVGPJHCuTI+yZRuBkkz/8ohv1Rf+En+VY
9QG0GBq/MEBZy3TV+SUYfPX1SQ9eQDDYNQToKsfpUh0QvuQ0JeIGSm+E6jFApNeg
QauT9x0TkVDP1bP5LFkTMG27Brzr9oG95F45hrZ0gW0D+w7YdTY1GD7ZAoGASHku
b4XoeNS1771hUg5w27qR9q+LC+8EmiHnRrNxDsnCZd7zGfQw7MKbQDdfQdfQUvyn
FBDKFsrLRT1rJVDGJe2ZNaE/QmE20AVNs7PG3UBYx/RxhYV/60smGGsXz10Mn+A0
SxuwKWoARshnMsDvsTYwofm1SMwT1MmCKpbTiiECgYBi8ZjgsdFv2NtYlmb1pAYS
DHiErbldtVumF42Tax+fucqUrdB3LZo6FjagvPy+LBjA3VjtRYkDjQmstvxD5jfd
V3Pq4IwaocGU8RQUJY5L6rmw+y1s6Z+iNkIcPeZtWidSgP+NZa1xvhfj8XeL5600
a+IQn0Y41zLJ22ScgyFzEQ==
-----END PRIVATE KEY-----

```

- 秘密キーの最初の行が5つのハイフンで始まり、単語BEGIN PRIVATE KEY、末尾が5つのハイフンで終わっていることを確認します。

例：

—BEGIN PRIVATE KEY—

- 秘密キーの最後の行が5つのハイフンで始まり、単語END PRIVATE KEY、末尾が5つのハイフンで終わることを確認します。

例：

—秘密キーの終了—

例：PEM形式と秘密キー内のデータを正しく入力します。

```
$ cat correct-private-key.key
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCbKjYwgGSIAGEAaoIBAQCvfIytwKf9UIc5
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+SUYfPX1S09eQDDYNQToKsfpUh0QvuQ0JeIGSm+E6jFApNeg
QauT9x0TkVDP1bP5LFkTMG27Brzr9oG95F45hrZ0gW0D+w7YdTYlGD7ZAoGASHku
b4XoeNS1771hUg5w27qR9q+LC+8EmiHnRrNxDsnCZd7zGfQw7MKbQDdFQdfQUvyn
FBDKFsrlRT1rJVDGJe2ZNaE/QmE20AVNs7PG3UBYx/RxhYV/60smGGsXz10Mn+A0
SxuwKWoARshnMsDvsTYwofmlSMwTlMmCKpbTiiECgYBi8ZjgsdFv2NtYlmb1pAYS
DHiErbldtVumF42Tax+fucqUrdB3LZo6FjagvPy+LbjA3VjtRYkDjQmstvxD5jfd
V3Pq4IwaocGU8RQUJY5L6rmw+y1s6Z+iNkIcPeZtWidSgP+NZa1xvhfj8XeL560o
a+IQn0Y41zLJ22ScgyFzEQ==
-----END PRIVATE KEY-----
```

警告メッセージ – 秘密キーから公開キーを生成できません

症状

警告メッセージ：秘密キーから公開キーを生成できません。証明書をインターフェイスに追加しようとした後、脅威グリッドアプライアンスで受信されます。

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/OiUQ/8uLk1sG7rVE5ROe/Ev9OvjL5nF
[Redacted]
wbTboJukREZOyiBoQDPcSWHqe8j3FEtJlf9yfv2bthOFQQ+Lf3BU4ZPiXPVEtuUL
7FIP0kjC/33s5ZWpC8OzCmdPvFgx//JbpWr1gIIYVs1uYg==
-----END CERTIFICATE-----
```

Private Key (PEM)

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAACAQEAucb3AU15P91Ym/PvHva/xKBCbLeY7+jQJGO7wm7eruX3KTZY
EE9N6qn1+2YecCmOAA01sTqTQaHVVHJdCsczgz1mGalFI6Xinl8JI9i+n2NDIcNr
XBVPvCUs5fnH2cZwKGTen/NDJhnyC5DIb17RLy7Y+wxhMiyRCHH3aZ3I0Mpl1k4X
[Redacted]
cjSc9W8Fy/CDXbX27KncS4qWe91phsKXq0jo7wIDAQABAolBAFrH8EHRsvNTXY5v
yCSwXQtfalYpjXGGqdduaPzdlrICrCGWbbgimKeYQByGTU9v7vXAx2EAh57Izvb2
```

cannot generate public key from private key

秘密キーファイル内の現在のPEMデータから公開キーを生成することはできません。

推奨手順：

-

1:OpenSSL

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

OpenSSLコマンドの出力が**RSA Key okでない場合は**、キー内のPEMデータに問題が見つかったことを意味します。

ステップ2:OpenSSLツールを使用して、秘密キーから公開キーをエクスポートできるかどうかを確認します。

```
openssl rsa -in
```

例：公開キーのエクスポートに失敗し、公開キーのエクスポートに成功しました。

```
$ 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/TKGusV2CygqtT+UESFerUEAzYh1KBxTUi5KKNB9Lm5A7RqPz1uHxPyTRmzC
FP3dQw7s8X4Bs3tL4s7U/Tq6Qm2ckD9q/rBswjijNHNwBICv6WA02gr/xj+qxPB3
P1YjNTU71lSFnSHC4E1Fzg3hy40yHCNqv7x/4jlniIAL9dGhrGQjnoFQ1DcDoD8m
N1yPIOx3C0lweVForZmx+Dg61+J4uIjytkVceBw0v1bDNdDRyk+BiB0pLF12VtV4
TQIDAQAB
-----END PUBLIC KEY-----
```

警告メッセージ – 解析エラー：PEMデータをデコードできませんでした

症状

警告メッセージ：解析エラー：PEMデータをデコードできませんでした。証明書をインターフェイスに追加しようとした後、Threat Gridアプライアンスで受信されます。

The screenshot shows the 'Upload SSL certificate for PANDEM' page in the Threat Grid Appliance configuration interface. The left sidebar lists various configuration categories, with 'SSL' selected. The main content area has two text input fields: 'Certificate (PEM)' and 'Private Key (PEM)'. Both fields contain PEM-formatted data. A red error message, 'parse error: PEM data could not be decoded', is displayed below the certificate field. At the bottom of the form are 'Add Certificate' and 'Cancel' buttons.

証明書ファイル内の現在のPEMデータから証明書をデコードできません。証明書ファイル内のPEMデータが破損しています。

- 証明書ファイル内のPEMデータから証明書情報を取得できるかどうかを確認します。

ステップ1:OpenSSLツールを使用して、PEMデータファイルの証明書情報を表示します。

```
openssl x509 -in
```

PEMデータが破損している場合、OpenSSLツールが証明書情報をロードしようとするエラーが発生します。

例：証明書ファイルのPEMデータが破損しているため、証明書情報を読み込めませんでした。

```
$ 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:
```

警告メッセージ：クライアント/サーバCA証明書ではありません

症状

警告メッセージ：解析エラー：クライアント/サーバのCA証明書ではなく、[Configuration] > [CA Certificates]にCA証明書を追加しようとする、Threat Gridアプライアンスで受信されます。

The screenshot shows the Threat Grid Appliance web interface. The left sidebar contains a navigation menu with items like Configuration, Authentication, CA Certificates, Change Password, Clustering, Date and Time, Email, Integrations, License, Network, Network Exit, NFS, Notifications, SSH, SSL, and Syslog. The main content area is titled 'CA Certificates' and shows a 'Certificate (PEM)' field. The field contains a corrupted PEM certificate. Below the field, there is a red error message: 'not a client/server CA cert'. At the bottom, there are two buttons: 'Add Certificate' and 'Cancel'.

CA証明書のBasic Constraints拡張値がCAとして定義されていません。True に設定します。

Basic Constraints拡張機能の値がCAに設定されている場合は、OpenSSLツールで確認します。CA証明書でTrueを指定します。

ステップ1:OpenSSLツールを使用して、PEMデータファイルの証明書情報を表示します。

```
openssl x509 -in
```

ステップ2：証明書の情報で、基本制約拡張の現在の値を検索します。

例：Threat Gridアプライアンスによって受け入れられるCAの基本制約値。

```
Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Basic Constraints:
    CA:TRUE
  X509v3 Key Usage:
    Digital Signature, Key Agreement, Certificate
```

関連情報

- [Threat Gridアプライアンス – コンフィギュレーションガイド](#)
- [Cisco AMP仮想プライベートクラウドアプライアンス – 設定例とテクニカルノート](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)