

# Integratie met AMP Virtual Private Cloud en Threat Grid-applicatie

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Architectuur van de integratie](#)

[Basisinformatie over de integratie](#)

[Procedure](#)

[SSL-certificaten opnieuw genereren](#)

[SSL-certificaten uploaden](#)

[Certificaat in de schone interface van Threat Grid-apparaat is zelf ondertekend](#)

[Certificaat in de interface Threat Grid-apparaat wordt gecertificeerd door een certificeringsinstantie \(CA\).](#)

[Voorbeeld](#)

[Verificatie](#)

[Bevestiging van de bijwerking van de monsterverwerking in de AMP Private Cloud Database](#)

[Voorbeeld](#)

[Probleemoplossing](#)

[Waarschuwing in Advanced Malware Protection Private Cloud Appliance ongeldig, certificaat niet getest, API-toets niet getest](#)

[Waarschuwing in AMP Private Cloud-apparaat met betrekking tot ongeldige Threat Grid API-toets](#)

[Monsterscores  \$\geq 95\$  worden ontvangen door het Advanced Malware Protection Private Cloud Appliance, maar er wordt geen verandering waargenomen in de steekproefdispositie](#)

[Waarschuwing in AMP Private Cloud-apparaat met betrekking tot ongeldig Threat Grid SSL-certificaat](#)

[Waarschuwingen in Threat Grid-apparaat in verband met certificaten](#)

[Waarschuwingsbericht - Publieke toets afgeleid van particuliere sleutel komt niet overeen](#)

[Waarschuwingsbericht - Private key bevat niet-PEM-inhoud](#)

[Waarschuwingsbericht - Kan geen openbare toets uit de privétoets genereren](#)

[Waarschuwingsbericht - parse fout: PEM-gegevens kunnen niet worden gedecodeerd](#)

[Waarschuwingsbericht - geen client/server CA-cert](#)

[Gerelateerde informatie](#)

## Inleiding

Dit document beschrijft de procedure om de integratie van de Advanced Malware Protection (AMP) Virtual Private Cloud en de Threat Grid-applicatie te voltooien. Het document bevat ook stappen voor het opsporen en verhelpen van problemen die verband houden met het integratieproces.

Bijgedragen door Armando Garcia, Cisco TAC Engineer.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Werk en gebruik de Advanced Malware Protection Virtual Private Cloud
- Werk en gebruik Threat Grid-applicatie

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

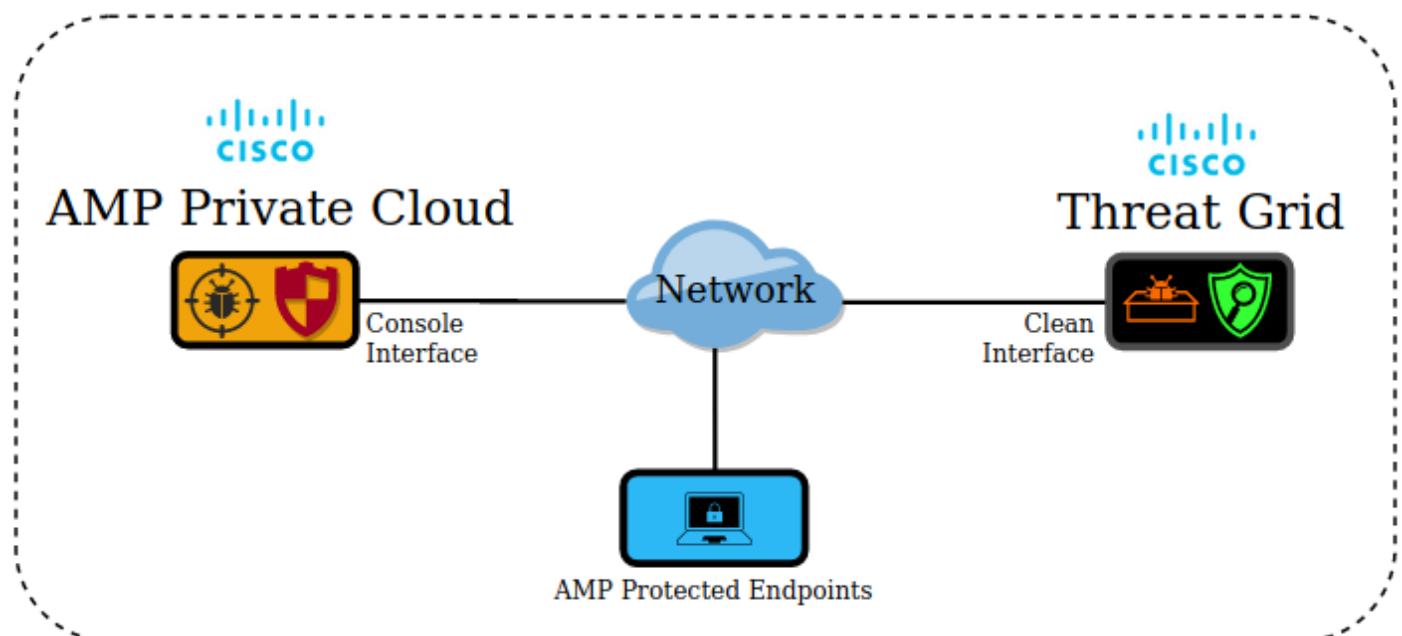
- Advanced Malware Protection Private Cloud 3.2.0
- Threat Grid-applicatie 2.12.0.1

**Opmerking:** De documentatie is geldig voor Threat Grid-apparaten en voor AMP Private Cloud-apparaten in het apparaat of de virtuele versie.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

## Achtergrondinformatie

### Architectuur van de integratie



### Basisinformatie over de integratie

- Het Threat Grid-apparaat analyseert monsters die door het Advanced Malware Protection Private Cloud Appliance zijn ingediend.
- Monsters kunnen handmatig of automatisch aan het Threat Grid-apparaat worden geleverd.
- Automatische analyse is standaard niet ingeschakeld in het Advanced Malware Protection

Private Cloud Appliance.

- Het Threat Grid-apparaat geeft aan het Advanced Malware Protection Private Cloud-apparaat een rapport en score uit de analyse van de steekproef.
- Het Threat Grid-apparaat informeert (poke) het Advanced Malware Protection Private Cloud-apparaat over een monster met een score van minimaal 95.
- Als de score van de analyse groter is dan of gelijk aan 95, wordt de steekproef in de AMP database gemarkeerd met een dispositie van kwaadaardig.
- Retrospectieve detecties worden door de AMP Private Cloud toegepast op monsters met een score groter dan of gelijk aan 95.

## Procedure

Stap 1. Stel de Threat Grid-applicatie in en configureren (nog geen integratie). Controleer op updates en installeer, indien nodig.

Stap 2. Stel de Advanced Malware Protection voor Endpoints Private Cloud in (nog geen integratie).

Stap 3. Selecteer in de beheerder van het Threat Grid UI het tabblad **Configuration** en kies **SSL**.

Stap 4. genereren of uploaden van een nieuw SSL-certificaat voor de Clean interface (PANDEM).

### SSL-certificaten opnieuw genereren

Er kan een nieuw zichzelf ondertekend certificaat worden gegenereerd als de hostnaam van de schone interface niet overeenkomt met de Onderwerp Alternatieve Naam (SAN) in het certificaat dat momenteel in het apparaat is geïnstalleerd voor de schone interface. Het apparaat genereert een nieuw certificaat voor de interface en configureren de huidige interface-hostname in het SAN-veld van het zelfgetekende certificaat.

Stap 4.1. Selecteer in de kolom Acties (..) en selecteer in het pop-upmenu **Generate New Certificate**.

Stap 4.2. Selecteer in Threat Grid UI de optie **Operations** in het volgende scherm en selecteer **Activeren** en kies **Herstellen**.

**Opmerking:** dit gegenereerd certificaat is zelf ondertekend.

### SSL-certificaten uploaden

Als er al een certificaat is gemaakt voor de reinigingsinterface van Threat Grid-apparaat, kan dit certificaat naar het apparaat worden geüpload.

Stap 4.1. Selecteer in de kolom Handelingen (..) en selecteer in het popupmenu de optie **Nieuw certificaat uploaden**.

Stap 4.2. Kopieer het certificaat en de bijbehorende privé-toets in PEM-indeling in de tekstvakjes

die op het scherm verschijnen en selecteer **Certificaat toevoegen**.

Stap 4.3. Selecteer in Threat Grid UI de optie **Operations** in het volgende scherm en selecteer **Activeren** en kies **Herstellen**.

Stap 5. Selecteer in de ADM UI-applicatie voor Private Cloud **Integraties** en kies **Threat Grid**.

Stap 6. Selecteer de optie **Bewerken** in de informatie over de configuratie van het Threat Grid.

Stap 7. Voer in de Threat Grid Hostname de FQDN in van de schone interface van het Threat Grid-apparaat.

Stap 8. Voeg in het Threat Grid SSL-certificaat het certificaat toe van de schone interface van het Threat Grid-apparaat. (Zie opmerkingen hieronder)

### **Certificaat in de schone interface van Threat Grid-apparaat is zelf ondertekend**

Stap 8.1. Selecteer de **Configuration** in de Threat Grid-beheerder UI en kies **SSL**.

Stap 8.2. Selecteer in de kolom Handelingen (..) en selecteer in het popupmenu de optie **Downloadcertificaat**.

Stap 8.3. Voeg het gedownload bestand toe aan het AMP Virtual Private device op de Threat Grid-integratiepagina.

### **Certificaat in de interface Threat Grid-apparaat wordt gecertificeerd door een certificeringsinstantie (CA).**

Stap 8.1. Kopieer in een tekstbestand het certificaat van de schone interface van Threat Grid-apparaat en de volledige CA-certificeringsketen.

**Opmerking:** De certificaten in het tekstbestand moeten in PEM-indeling zijn.

#### **Voorbeeld**

Als de gehele certificeringsketen: ROOT\_CA certificaat > Threat\_Grid\_Clean\_Interface certificaat;  
Het tekstbestand moet vervolgens worden gemaakt, zoals in de afbeelding wordt weergegeven.

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

Als de gehele certificeringsketen: ROOT\_CA certificaat > Sub\_CA certificaat > Threat\_Grid\_Clean\_Interface certificaat; Het tekstbestand moet vervolgens worden gemaakt, zoals in de afbeelding wordt weergegeven.

```
-----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-----
```

Stap 9. In Threat Grid API-toets voert u de API-toets in van de Threat Grid-gebruiker die is gekoppeld aan de geüploade monsters.

# API

API Key \*\*\*\*\*  

Disable API Key 

Can Download Sample Content Via API 

**Opmerking:** In de accountinstellingen van de Threat Grid-gebruiker bevestig dat de **sleutel API uitschakelen** niet op True is ingesteld.

Stap 10. Nadat alle wijzigingen zijn voltooid, selecteert u **Opslaan**.

Stap 1. Pas een aanpassing op het Advanced Malware Protection Virtual Cloud Appliance toe.

Stap 12. Selecteer vanuit de ADM UI-applicatie voor Private Cloud, **Integraties** en kies **Threat Grid**.

Stap 13. Kopieer uit **details** de waarden van de URL van de upgrade-service van de dispersie, de gebruiker van de update Service en het wachtwoord voor de upgrade van de dispersie. Deze informatie wordt in Stap 17 gebruikt.

Stap 14. Selecteer in Threat Grid-beheerder UI de optie **Configuration** en kies **CA-certificaten**.

Stap 15. Selecteer **Certificaat** en exemplaar in PEM-indeling **toevoegen** aan het CA-certificaat dat het certificaat voor upgrade van de AMP Private Cloud Disposition Service heeft ondertekend.

**Opmerking:** Als het CA-certificaat dat het AMP Private Cloud Disposition Update-certificaat heeft ondertekend een sub-CA is, herhaal dan het proces totdat alle CA's in de keten zijn geüpload naar **CA-certificaten**.

Stap 16. Selecteer in het Threat Grid-portaal het optie Beheer en selecteer Advanced Malware Protection Private Cloud Integration.

Stap 17. Typ de informatie in Stap 13 van de pagina Automation Service.

- Service-URL: FQDN van de Disposition Update Service van het Advanced Malware Protection Private Cloud-apparaat.
- Gebruiker: Gebruiker van de Update Service van de Dispositie van het Advanced Malware Protection Private Cloud-apparaat.
- Wachtwoord: Wachtwoord voor bijwerken van de beschikbaarheid van het Advanced Malware Protection Private Cloud-apparaat.

Op dit moment, als alle stappen correct werden uitgevoerd, moet de integratie met succes werken.

## Verificatie

Dit zijn de stappen om te bevestigen dat het Threat Grid-apparaat met succes is geïntegreerd.

**Opmerking:** Alleen de stappen 1, 2, 3 en 4 zijn geschikt om in een productieomgeving te worden toegepast om de integratie te controleren. Stap 5 wordt verstrekt als informatie om meer te weten te komen over de integratie en wordt niet geadviseerd om in een productieomgeving te worden toegepast.

Stap 1. Selecteer Test Connection in AMP Private Cloud Apparaat Admin UI > Integraties > Threat Grid en bevestig de bericht Threat Grid Connection-test met succes! ontvangen.

Threat Grid Configuration Details Edit

Hostname

API Key

**Threat Grid SSL Certificate** 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

tus ▾ Integrations ▾ Support ▾

**✔ Threat Grid Connection test successful!**

Stap 2. Bevestig de webpagina Bestandsanalyse in de Advanced Malware Protection Private Cloud Console wordt geladen zonder fouten.

**CISCO** AMP for Endpoints 🔔 ? armando garcia ▾

Dashboard Analysis ▾ Outbreak Control ▾ Management ▾ Accounts ▾

**File Analysis**

There are no File Analyses to view

Stap 3. Controleer dat bestanden die handmatig worden ingediend via de **analyse** van de **Advanced Malware Protection Private Cloud Analysis > File Analysis** in het Threat Grid-apparaat worden aangetroffen en dat een rapport met een score wordt teruggegeven door het Threat Grid-apparaat.

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
-----------------------------------	-------------------------	-----------

Stap 4. Bevestig de CA's die het certificaat voor bijwerken service van de locatie van het Advanced Malware Protection van het Advanced Malware Protection Private Cloud-apparaat hebben ondertekend, in het Threat Grid-apparaat in de **certificaatautoriteiten** geïnstalleerd.

Stap 5. Bevestig dat een monster dat gemarkeerd is door het Threat Grid-apparaat met een score  $\geq 95$ , wordt opgenomen in de Advanced Malware Protection Private Cloud-database met de verwerking van kwaadaardig materiaal na het rapport en de voorbeeldscore worden geleverd door het Threat Grid-applicatie.

**Opmerking:** Een geslaagde ontvangst van een steekproefrapport en een score van  $\geq 95$  in de AMP Private Cloud console van het tabblad **File Analysis** betekent niet noodzakelijk dat de bestandsindeling in de AMP-database werd gewijzigd. Als de CA's die het certificaat voor update van de locatie van het AMP Private Cloud-apparaat hebben getekend, niet in het Threat Grid-apparaat zijn geïnstalleerd **bij de certificaatautoriteiten**, worden rapporten en scores ontvangen door het Advanced Malware Protection Private Cloud-apparaat, maar er worden geen fouten ontvangen van het Threat Grid-apparaat.

**Waarschuwing:** De volgende test is uitgevoerd om een steekproefwijziging in de AMP-database op te starten nadat het Threat Grid-apparaat een bestand met een score van  $\geq 95$  heeft gemarkeerd. Het doel van deze test was informatie te verstrekken over de interne operaties in het Advanced Malware Protection Private Cloud device wanneer het Threat Grid-applicatie een voorbeeldscore van  $\geq 95$  biedt. Om het proces van de verandering van de beschikbaarheid te activeren, is er een testbestand gemaakt met de interne makemalware.exe-toepassing. Steekproef: malware3-419d23483.exeSHA256: 8d3bbc795bb4747984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995.

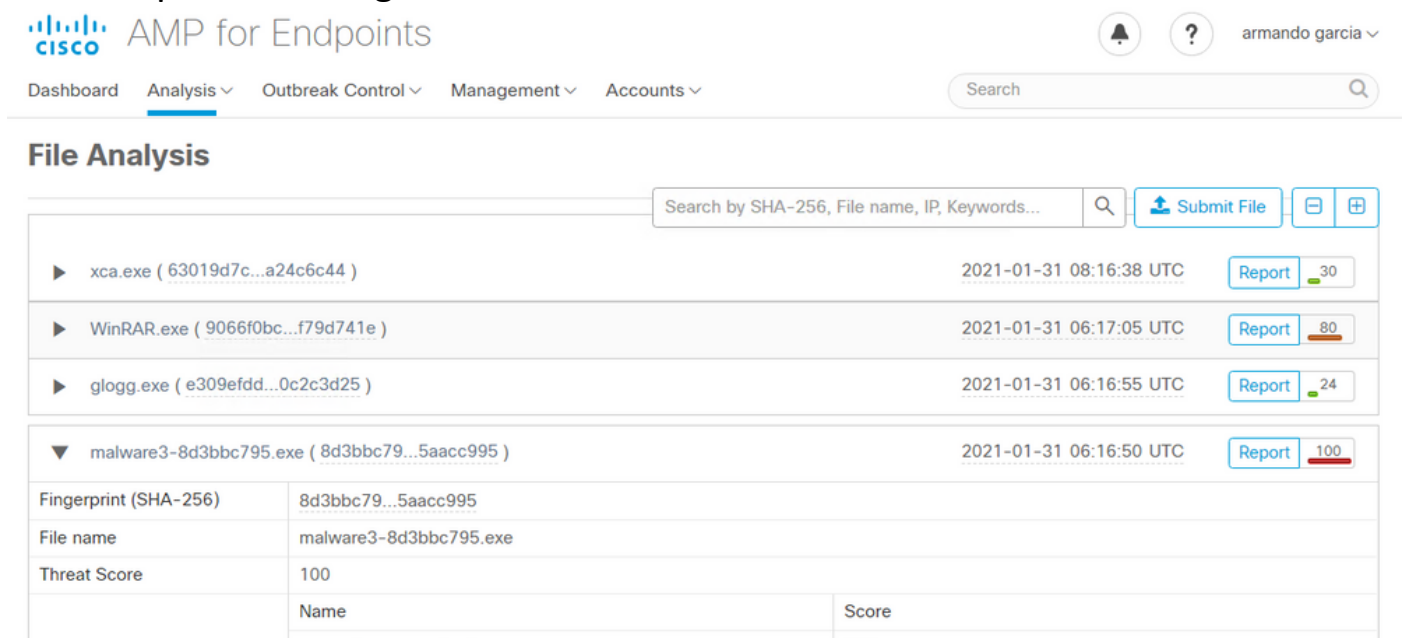
**Voorzichtig:** Het wordt niet aangeraden om een testbestand tegen malware imitatie in een



productieomgeving te laten ontploffen.

## Bevestiging van de bijwerking van de monsterverwerking in de AMP Private Cloud Database

Het testmalware-bestand is handmatig vanuit **Bestandsanalyse** in de Advanced Malware Protection Private Cloud-console aan het Threat Grid-apparaat voorgelegd. Na de analyse van de steekproef werd door het Threat Grid-apparaat een steekproefrapport en een steekproefscore van 100 aan het AMP Private Cloud-apparaat verstrekt. Een voorbeeldscore  $\geq 95$  leidt tot een dispositie verandering voor de steekproef in de databank van het apparaat van de AMP Private Cloud. Deze verandering van de steekproefdispositie in de AMP-database op basis van een door Threat Grid verstrekte steekproefscore  $\geq 95$  is wat een pekel wordt genoemd.



The screenshot shows the 'File Analysis' section of the Cisco AMP for Endpoints console. It features a search bar and a 'Submit File' button. A list of files is displayed with columns for file name, timestamp, and a 'Report' button with a score indicator. The file 'malware3-8d3bbc795.exe' has a score of 100. Below the list, a table provides details for this file.

Name	Score
malware3-8d3bbc795.exe	100

Als:

- De integratie is met succes voltooid.
- Na het handmatig indienen van bestanden worden voorbeeldrapporten en scores in **Bestandsanalyse** waargenomen.

Dan:

- Voor elke steekproef die het Threat Grid-apparaat markeert met een score  $\geq 95$ , wordt een ingang aan het bestand /data/poked/poked.log in het AMP Private Cloud-apparaat toegevoegd.
- /data/poked/poked.log wordt gecreëerd in het Advanced Malware Protection Private Cloud device nadat de eerste  $\geq 95$  voorbeeldscore door het Threat Grid-apparaat is geleverd.
- De db\_protection database in de AMP Private Cloud houdt de huidige dispositie voor de steekproef vast. Deze informatie kan worden gebruikt om te bevestigen of de steekproef een afstand van 3 heeft na het Threat Grid-apparaat, mits de score wordt bepaald.

Als het voorbeeldrapport en de score  $\geq 95$  in **File Analysis** in de AMP Private Cloud console worden gezien, pas deze stappen toe:

Stap 1. Meld u aan via SSH bij het Advanced Malware Protection Private Cloud Appliance.

Stap 2. Controleer of er een vermelding in `/data/poked/poked.log` is voor de steekproef.

Uit een lijst van de `/data/poked/` folder in een AMP Private Cloud-apparaat dat nog nooit een  $\geq 95$  voorbeeldscore van een Threat Grid-apparaat heeft ontvangen, blijkt dat het `gekokeerde.log`-bestand niet in het systeem is aangemaakt.

Als het Advanced Malware Protection Private Cloud-apparaat nooit een poke van een Threat Grid-apparaat heeft ontvangen, wordt het `/data/poked/poked.log`-bestand niet in de map gevonden, zoals in de afbeelding.

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

Als de eerste  $\geq 95$  voorbeeldscore is ontvangen, toont dit aan dat het bestand is aangemaakt.

Na ontvangst van de eerste steekproef met een score van  $\geq 95$ .

```
[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": "W32.80388C795B-100.SBX.TG", "ok": 1, "time": 1612031118, "hash": "8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aac995", "engine": "sha256", "user": "-", "mode": "tg", "score": 100}
[root@fireamp ~]#
```

Informatie over voorbeelden uit de slang die door het Threat Grid-apparaat is geleverd, kan in het `gekokeerde.log`-bestand worden aangetroffen.

Stap 3. **Start** deze opdracht met de steekproef SHA256 om de huidige dispositie uit de database van het Advanced Malware Protection Private Cloud device op te halen.

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

### Voorbeeld

Een database query om de steekproefdispositie te krijgen voordat de steekproef wordt geüpload naar het Threat Grid-applicatie levert geen resultaten op, zoals in de afbeelding worden getoond.

```
[root@fireamp ~]# mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aac995;"
[root@fireamp ~]#
```

Een gegevensbank query om de steekproefdispositie te krijgen nadat het rapport en de score werden ontvangen van het Threat Grid-apparaat, toont de steekproef met een dispositie van drie die als kwaadaardig wordt beschouwd.

```
[root@fireamp ~]# mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aac995;"
+-----+-----+
| hex(fingerprint) | disposition_id |
+-----+-----+
| 80388C795BB47447984BF2842D3A0119BAC0D79A15A59686951E1F7C5AAC995 | 3 |
+-----+-----+
[root@fireamp ~]#
```

# Probleemoplossing

In het integratieproces kunnen mogelijke problemen worden onderkend. In dit deel van het document worden enkele van de meest voorkomende kwesties behandeld.

## Waarschuwing in Advanced Malware Protection Private Cloud Appliance ongeldig, certificaat niet getest, API-toets niet getest

### Symptoom

Het waarschuwingsbericht: Threat Grid-host is ongeldig, Threat Grid SSL-certificaat kon niet worden getest, Threat Grid API-toets kon niet worden getest, wordt ontvangen in het AMP Private Cloud-apparaat nadat de **Test Connection**-knop in **integraties > Threat Grid** is geselecteerd.

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.

Er is een probleem op netwerkniveau in de integratie.

### Aanbevolen stappen:

- Bevestig de interface Advanced Malware Protection Private Cloud device dat de Threat Grid-wasmachine kan bereiken.
- Bevestig dat het apparaat van de Advanced Malware Protection Private Cloud de FQDN-oplossing van de interface van Threat Grid-apparaat kan oplossen.
- Bevestig dat er geen filterapparaat is in het netwerkpad van het Advanced Malware Protection Private Cloud Appliance en het Threat Grid-apparaat.

## Waarschuwing in AMP Private Cloud-apparaat met betrekking tot ongeldige Threat Grid API-toets

### Symptoom

Het waarschuwingsbericht: Threat Grid-verbindingstest mislukt, is Threat Grid API ongeldig, wordt ontvangen in het Advanced Malware Protection Private Cloud device nadat de knop **Test Connection** in **Integraties > Threat Grid** is geselecteerd.

Connect Threat Grid Appliance to AMP for Endpoints Appliance

#### Threat Grid Connection test failed.

- Threat Grid API key is invalid.

De Threat Grid API-toets is ingesteld in de AMP Private Cloud.

Aanbevolen stappen:

- Bevestig in de rekeninginstellingen van de gebruiker Threat Grid, wordt de belangrijke parameter Off API niet op True ingesteld.
  - De API-toets moet worden ingesteld op: Onjuist of ongedaan maken

## API

API Key \*\*\*\*\*  

Disable API Key   True  False  Unset

Can Download Sample Content Via API   True  False  Unset

- Bevestig de Threat Grid API-toets die is geconfigureerd in de AMP Private Cloud Admin portal **Integraties > Threat Grid**, is dezelfde API-toets in de gebruikersinstellingen in het Threat Grid-apparaat.
- Controleer of de juiste Threat Grid API-toets is opgeslagen in de database van het AMP Private Cloud-apparaat.

Van de opdrachtregel van AMP Private Cloud device kan deze worden bevestigd door de huidige Threat Grid API-toets die in het AMP-apparaat is geconfigureerd. Meld u aan bij het Advanced Malware Protection Private Cloud Appliance via SSH en voer deze opdracht uit om de huidige Threat Grid-gebruiker API-toets op te halen:

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

Dit is een juist item in de database van het AMP Private Cloud-apparaat voor de Threat Grid API-toets.

```
[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 ~]#
```

Zelfs al was de Threat Grid-gebruikersnaam niet direct ingesteld in het AMP Private Cloud Devices in een willekeurige stap van de integratie, de Threat Grid-gebruikersnaam wordt in de tg\_login parameter in de AMP-database gezien als de Threat Grid API-toets correct is toegepast.

Dit is een onjuiste vermelding in de AMP-database voor de Threat Grid API-toets.

```
[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 ~]#
```

De tg\_login parameter is NULL. De Threat Grid-gebruikersnaam is niet uit het Threat Grid-apparaat gehaald door het Advanced Malware Protection Private Cloud-apparaat na de aanpassing.

## Monsterscores >=95 worden ontvangen door het Advanced Malware Protection Private Cloud Appliance, maar er wordt geen verandering waargenomen in de steekproefdispositie

### Symptoom

Rapporten en >=95 voorbeeldscores worden na indiening van een monster met succes van het Threat Grid-apparaat ontvangen, maar in het AMP Private Cloud-apparaat wordt geen verandering in de monsterverwerking waargenomen.

### Aanbevolen stappen:

- Bevestig het apparaat van de Private Cloud van de AMP als de steekproef SHA256 in de inhoud van /data/poked/poked.log staat.

Als SHA256 in /data/poked/poked.log wordt gevonden, dan voert u deze opdracht uit om de huidige steekproefpositie in de AMP database te bevestigen.

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

- Bevestig het juiste AMP Private Cloud Integration-wachtwoord dat aan het Threat Grid-beheerportaal voor apparaat in **Beheer > Advanced Malware Protection Private Cloud Integration is toegevoegd**.

DOM Private Cloud-beheerportal.

#### 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"/> <span>Change Password</span>

Threat Grid-portaal voor wasconsole.



### Disposition Update Syndication Service

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

- Bevestig de CA's die het certificaat voor update van de service van de AMP Private Cloud device hadden getekend, dat is geïnstalleerd in het beheerportal voor Threat Grid in **CA-certificaten**.

In het onderstaande voorbeeld is de certificeringsketen voor de AMP Private Cloud device Disposition Update Service certificaat **Root\_CA > Sub\_CA > Dispositie\_Update\_Service certificaat**; Daarom moeten RootCA en Sub\_CA in **CA Certificaten** worden geïnstalleerd in de Threat Grid-applicatie.

Certificaatautoriteiten in het beheerportal voor Advanced Malware Protection Private Cloud.



✖ **Sanity Check Failing**

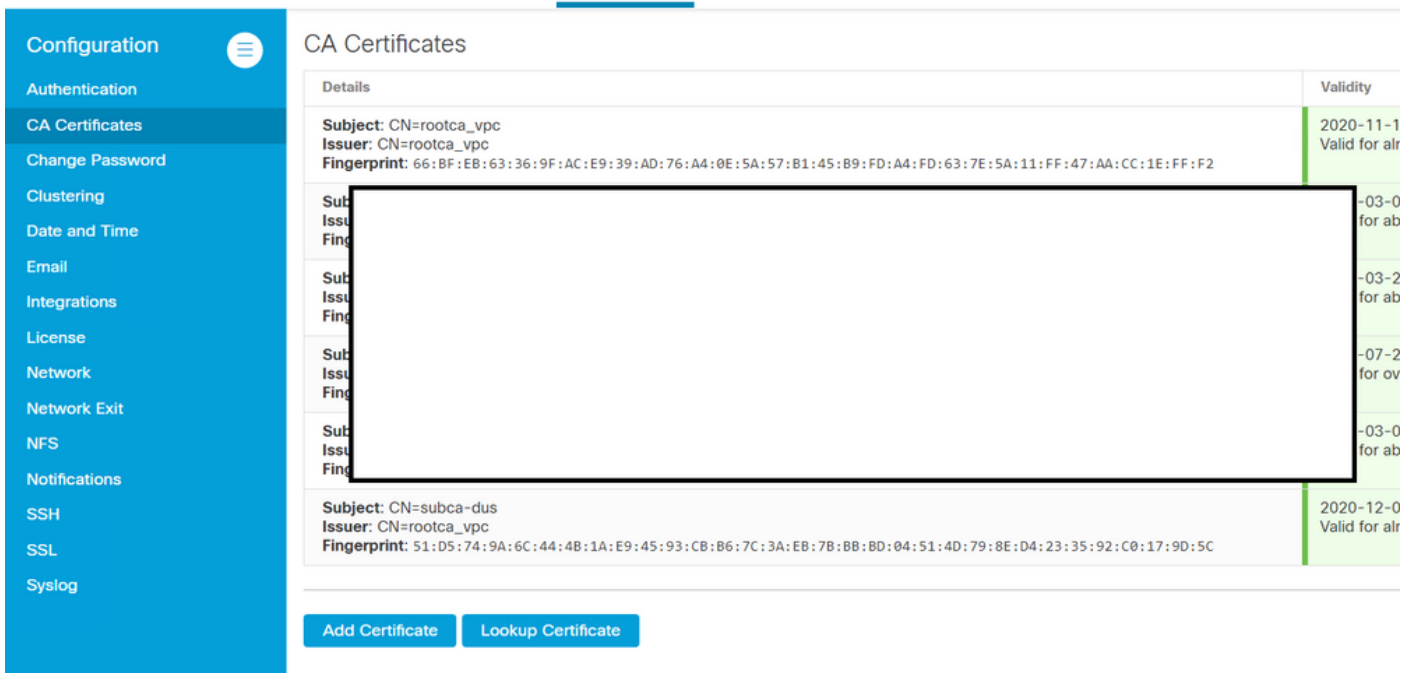
Certificate Authorities are used by your Private Cloud device to verify SSL certificates and connections.

Add Certificate Authority

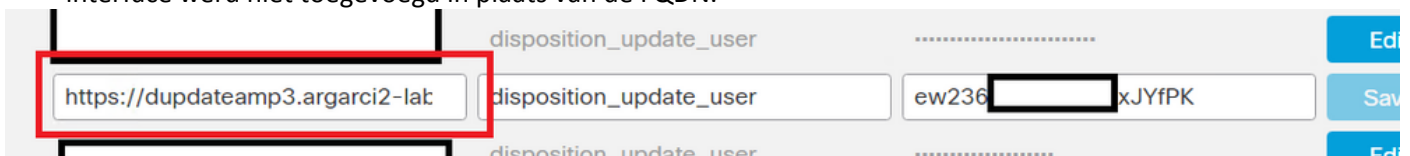
Certificate <span style="float: right;">(click to collapse)</span>			
Issuer	rootca_vpc		<span>Download</span> <span style="background-color: red; color: white; padding: 5px;">Delete</span>
Subject	rootca_vpc		
Validity	2020-11-15 00:00:00 UTC	-	

Certificate <span style="float: right;">(click to collapse)</span>			
Issuer	rootca_vpc		<span>Download</span> <span style="background-color: red; color: white; padding: 5px;">Delete</span>
Subject	subca-dus		
Validity	2020-12-05 12:01:00 UTC	-	





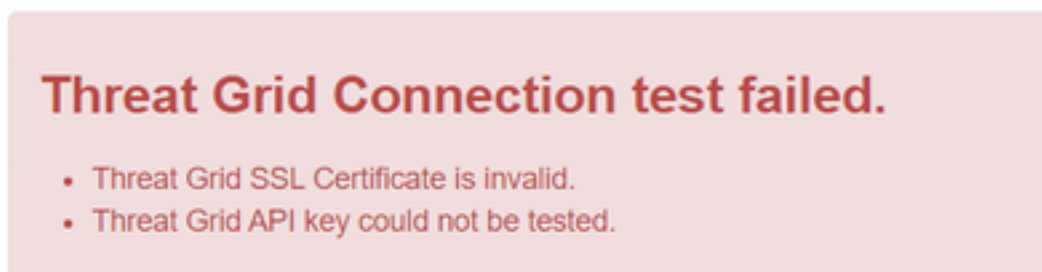
- Bevestig dat de FQDN-service voor bijwerken van de AMP Private Cloud device op de juiste manier is toegevoegd aan het Threat Grid-beheerportaal voor apparaat in **Beheer > Advanced Malware Protection Private Cloud Integration beheren**. Bevestig ook het IP-adres van de AMP Private Cloud device console-interface werd niet toegevoegd in plaats van de FQDN.



## Waarschuwing in AMP Private Cloud-apparaat met betrekking tot ongeldig Threat Grid SSL-certificaat

### Symptoom

Het waarschuwingsbericht: "Threat Grid SSL-certificaat is ongeldig", wordt in het Advanced Malware Protection Private Cloud-apparaat ontvangen nadat de knop **Test Connection** in **Integraties > Threat Grid** is geselecteerd.



### Aanbevolen stappen:

- Controleer of het certificaat dat in de interface Threat Grid-apparaat is geïnstalleerd, is ondertekend door een CA-bedrijf.

Als deze door een CA is ondertekend, moet de volledige certificatenketen in een bestand worden toegevoegd aan de **integraties** van de **beheerportal** voor de AMP Private Cloud device > **Threat**

## Grid in Threat Grid SSL-certificaat.

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

In het Advanced Malware Protection Private Cloud Appliance kunt u de geïnstalleerde Threat Grid-certificaten vinden in: /opt/fire/etc/ssl/threat\_grid.crt.

## Waarschuwingen in Threat Grid-apparaat in verband met certificaten

### Waarschuwingsbericht - Publieke toets afgeleid van particuliere sleutel komt niet overeen

#### Symptoom

Het waarschuwingsbericht: De openbare sleutel die is afgeleid van de privé-toets komt niet overeen, wordt ontvangen in het Threat Grid-apparaat nadat is geprobeerd een certificaat aan een interface toe te voegen.

The screenshot shows the Threat Grid Appliance web interface. The top navigation bar includes 'Home', 'Configuration', 'Status', 'Operations', and 'Support'. The left sidebar lists various configuration options, with 'SSL' highlighted. The main content area is titled 'Upload SSL certificate for PANDEM'. It contains two text input fields: 'Certificate (PEM)' and 'Private Key (PEM)'. Both fields contain PEM-formatted text. Below the 'Private Key (PEM)' field, a red error message reads: 'public key derived from private key does not match'. At the bottom of the form are two buttons: 'Add Certificate' and 'Cancel'.



De openbare toets die uit de particuliere toets wordt geëxporteerd, komt niet overeen met de openbare toets die in het certificaat is ingesteld.

Aanbevolen stappen:

- Bevestig of de privé-toets overeenkomt met de openbare sleutel in het certificaat.

Als de particuliere toets overeenkomt met de openbare toets in het certificaat, dan moeten de modulus en de publieke exponent hetzelfde zijn. Voor deze analyse is het voldoende om te bevestigen of de modulus dezelfde waarde heeft in de particuliere sleutel en de openbare sleutel in het certificaat.

Stap 1. Gebruik het OpenSSL-gereedschap om de modulus in de particuliere sleutel en de openbare sleutel in het certificaat te vergelijken.

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

Voorbeeld. Succesvolle match van een privésleutel en een openbare sleutel, ingesteld in een certificaat.

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

## Waarschuwingsbericht - Private key bevat niet-PEM-inhoud

### Symptoom

Het waarschuwingsbericht: Particuliere sleutel bevat niet-PEM-inhoud en wordt in het Threat Grid-apparaat ontvangen nadat is geprobeerd een certificaat aan een interface toe te voegen.

- 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-----
MIIDTjCCAjagAwIBAgIlcR1youIOY/MwDQYJKoZIhvcNAQELBQAwGjEYMBYGA1UE
AwwPc3ViY2FfdGdhX2NsZWZuMB4XDTEwMTEyNDAwMDAwMFOxMTEyMTEyMzNT
k1
OVowSTEBMBkGA1UEChMSMQ2lZy28gU3lzdGVtcywgSW5jMSowKAYDVQQDEyFrc2Vj

```

Private Key (PEM)

```
wZfa8sZJp30zivJRtvBioPnwmPpNZzhqIW3cC90ASaRSXeU+4c+HmUknahEHJNn8
lJbkA4UJQgWgeD4QKOj8cQKBgQCIZmRmL7H7d1avaPzbEIA0kYnlqIXsBKDCHjYo
g+H0NxlIdl8zU5HYFab9LO361thYO+OBwd3EGhbQ2u7CeinFp8Y7mQuqQNFTbHIZO

```

*private key contains non-PEM content*

De PEM-gegevens in het privé-sleutelbestand zijn beschadigd.

Aanbevolen stappen:

- Bevestig de integriteit van de gegevens in de privétoets.

Stap 1. Gebruik het OpenSSL-gereedschap om de integriteit van de particuliere sleutel te controleren.

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

Voorbeeld. Uitkomsten uit een privé-toets met fouten in de PEM-gegevens in het bestand en uit een andere privé-toets zonder fouten in de PEM-inhoud.

```
$ 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
```

Als de OpenSSL-opdrachtoutput niet **RSA-Key** is, betekent dit dat er problemen zijn gevonden met de PEM-gegevens in de toets.

Als er problemen zijn gevonden met de OpenSSL-opdracht, dan:

- Bevestig of PEM-gegevens in de privétoets ontbreken.

PEM-gegevens in het privé-sleutelbestand worden weergegeven in lijnen met 64 tekens. Een snelle controle van de PEM-gegevens in het bestand kan aantonen of er gegevens ontbreken. De regel met ontbrekende gegevens wordt niet uitgelijnd met andere regels in het bestand.

```

$ cat wrong-private-key.key
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCbKYwggSiAgEAAoIBAQCvfiYtwkf9UIc5
DluK9PTbKvDrShgn8/Cen9wXEUDIBNahlFiZvwZb/5FL+I1ry/P0WKJMiXRhLQ52
Y0oogQsuDTw79Moa6xXYLKq1P5QRIV6tQQDNIHUoHFNSLkoo0H0ubkDtGo/PW4fE
/JNGbMIU/d1DDuzxfgGze0viztT90rpCbZyQP2r+sGxaOKM0c3AEgK/pYA7aCv/G
P6rGkHc/ViM1NTuWVIWdIcLgTUX0DeHLjTIcI2q/vH/i0WeIgAv10aGuBCOeg <-----
NwOgPyY3XI8g7l 4HA6/VsM10NHKT4EhvSks
WXZW1XhNAgMBA. tU9huSCL7t4BF7VpSeKXM
Uh4/Vrdg1TYXfi s7k0sCwmhKUaMacTYAnrg
fINIJto/x0azh. 47ttvLvX3zweLCEXsDXK6
mdhzCQSTBFybM. 24M7HiocsbkLjijScTFYQ
JqSwA5BEgqeH3. 1gd4kJ6ddAaSjQS7sJxaf
WtVHzbVDqJ+rb! 3gQDePpxacxGRZLXfja3s
SU+TvjNWQGcUs: a8y8ZQd0lqPZrV0Z6Mym2
i5S+/LS4jHB5hcCfnZpL4M0zHYvX+HPuGHm2xOCy51K5KsfDPa/SrbhDkxZty0SG
lCgVLEycQ5t1xtI6qiBLKNmtrQKBgQDKI+BTMrHFYD50gPcBZyGXVhmSyHcZOP9k
OosXngeKtpdqL8Ck/H2QftFpOAFoHQxD/tiJA6E1eK9HFVnsq9+xbCU1fRlPxeCS
CbcfIDYBwaMn8Ywp9PfZKPgu/gI3XIUWT6T0LcBGtdspYDEbApvYA091PoS0vcBn
g7LG+bcJIQKBGhFn/ZziDtrkSzJ5N6fVGPJHCuTI+yZRuBkkz/8ohv1Rf+En+VY
9QG0GBq/MEBzy3TV+SUYfPX1SQ9eQDDYNQToKsfpUh0QvuQ0JeIGSm+E6jFApNeg
QauT9x0TkVDP1bP5LFkTMG27Brzr9oG95F45hrZ0gW0D+w7YdTYlGD7ZAoGASHku
b4XoeNS1771hUg5w27qR9q+LC+8EmiHnRrNxDsnCzd7zGfQw7MKbQDdfQdfQUvyn
FBDKFsrLRT1rJVDGJe2ZNaE/QmE20AVNs7PG3UByx/RxhYV/60smGGsXz10Mn+A0
SxuwKWoARshnMsDvsTYwofmlSMwTlMmCKpbTiiECgYBi8ZjgsdFv2NtYlmb1pAYS
DHiErbldtVumF42Tax+fucqUrdB3LZo6FjagvPy+LBjA3VjtRYkDjQmstvxD5jfd
V3Pq4IwaocGU8RQUJY5L6rmw+y1s6Z+iNkIcPeZtWidSgP+NZa1xvhfj8XeL5600
a+IQn0Y41zLJ22ScgyFzEQ==
-----END PRIVATE KEY-----

```

- Bevestig de eerste regel in de privé sleutel met 5 koppeltkens, de woorden **BEGIN PRIVATE KEY**, en eindigt met 5 koppeltkens.

Voorbeeld.

—BEGIN PARTICULIERE SLEUTEL—

- Bevestig de laatste regel in de privé sleutel met 5 koppeltkens, de woorden **EINDPRIVATE KEY**, en eindigt met 5 koppeltkens.

Voorbeeld.

—EINDPRIVÉ-SLEUTEL—

Voorbeeld. Correcte PEM-indeling en gegevens in een privétoets.

```
$ cat correct-private-key.key
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCvfIytwfk9UIc5
DluK9PTbKvDrShgn8/Cen9wXEUDIBNahlFiZvwZb/5FL+I1ry/P0WKJMiXRhLQ52
Y0oogQsuDTw79Moa6xXYLKq1P5QRIV6tQQDNiHUoHFNSLkoo0H0ubkDtGo/PW4fE
/JNGbMIU/d1DDuzxfGze0viztT90rpCbZyQP2r+sGxa0KM0c3AEgK/pYA7aCv/G
P6rGkHc/ViM1NTuWVIWdIcLgTUX0DeHLjTicI2q/vH/i0WeIgAv10aGuBC0egVDU
NwOgPyY3XI8g7H [REDACTED] 4HA6/VsM10NHKT4EhvSks
WXZW1XhNAgMBAA [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
CbcflDYBwaMn8Ywp9PfZKpGu/gI3XIUWT6T0LcBGtdspYDEbApvYA091PoS0vcBn
g7LG+bcJIQKBGHFn/ZziDtrkSzJSN6fVgPhJHCutI+yZRuBkkz/8ohv1Rf+En+VY
9QG0GBq/MEBZy3TV+SUYfPX1S09eQDDYNQToKsfpUh0QvuQ0JeIGSm+E6jFApNeg
QauT9x0TkVDP1bP5LFkTMG27Brzr9oG95F45hrZ0gW0D+w7YdTYlGD7ZAoGASHku
b4XoeNS1771hUg5w27qR9q+LC+8EmiHnRrNxDsnCZd7zGfQw7MKbQDdFQdfQUvyn
FBDKFsrlRT1rJVDGJe2ZNaE/QmE20AVNs7PG3UBYx/RxhYV/60smGGsXzl0Mn+A0
SxuwKWoARshnMsDvsTYwofmlSMwTlMmCKpbTiiECgYBi8ZjgsdFv2NtYlmb1pAYS
DHierblDtVumF42Tax+fucqUrdB3LZo6FjagvPy+LbjA3VjtRYkDjQmstvxD5jfd
V3Pq4IwaocGU8RQUJY5L6rmw+y1s6Z+iNkIcPeZtWidSgP+NZa1xvhfj8XeL560o
a+IQn0Y41zLJ22ScgyFzEQ==
-----END PRIVATE KEY-----
```

## Waarschuwingsbericht - Kan geen openbare toets uit de privétoets genereren

### Symptoom

Het waarschuwingsbericht: Kan geen openbare sleutel uit de privétoets genereren, wordt in het Threat Grid-apparaat ontvangen na een poging om een certificaat aan een interface toe te voegen.

- 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
BgkqhkiG9w0BAQsFAAOCQAQEAsCQ1iOkPkLj6A1R94eueZ64zCYGuf8wg0z2S9Kle
epjqQobaJadl3WTh7LMHuxHZP02YZJIO/OjUQ/8uLk1sG7rVE5ROe/Ev9OvjL5nF
[Redacted]
wbTboJukREZOyiBoQDPcSWHqe8j3FEtJlf9yfv2bthOFQQ+Lf3BU4ZPiXPVEtuUL
7FIP0kjC/33s5ZWpC8OzCmdPvFgx//JbpWr1gIIYVs1uYg==
-----END CERTIFICATE-----
```

Private Key (PEM)

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAACAQEAucb3AU15P91Ym/PvHva/xKBCbLeY7+jQJGO7wm7eruX3KTZY
EE9N6qn1+2YecCmOAA01sTqTQaHVVHJdCscgz1mGalFI6Xinl8JI9i+n2NDIcNr
XBVPvCUs5fnH2cZwKGTen/NDJhnyC5DIb17RLy7Y+wxhMiyRCHH3aZ3I0Mpl1k4X
[Redacted]
cjSc9W8Fy/CDXbX27KncS4qWe91phsKXq0jo7wIDAQABAolBAFrH8EHRsvNTXY5v
yCSwXQtfalYpjXGGqdduaPzdIrlCrCGWbbgimKeYQByGTU9v7vXAx2EAh57Izvb2
```

*cannot generate public key from private key*

De openbare toets kan niet worden gegenereerd vanuit de huidige PEM-gegevens in het privé-sleutelbestand.

#### Aanbevolen stappen:

- Bevestig de integriteit van de gegevens in de privétoets.

Stap 1. Gebruik het OpenSSL-gereedschap om de integriteit van de particuliere sleutel te controleren.

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

Als de OpenSSL-opdrachtoutput niet **RSA-Key** is, betekent dit dat er problemen zijn gevonden met de PEM-gegevens in de toets.

Stap 2. Gebruik het OpenSSL-gereedschap om te controleren of de openbare sleutel uit de particuliere sleutel kan worden geëxporteerd.

```
openssl rsa -in
```

Voorbeeld. Opgeven van openbare sleutel en succesvolle openbare sleutel export mislukt.



```
$ 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/TKGusV2CqqtT+UESFerUEAzYh1KBxTUi5KKNB9Lm5A7RqPz1uHxPyTRmzC
FP3dQw7s8X4Bs3tL4s7U/Tq6Qm2ckD9q/rBswjijNHNwBICv6WA02gr/xj+qxpB3
P1YjNTU71lSFnSHC4E1Fzg3hy40yHCNqv7x/4jlniIAL9dGhrgQjnofQ1DcDoD8m
N1yPIOx3C0lweVForZmx+Dg6l+J4uIjytkVceBw0v1bDNdDRyk+BIb0pLF12VtV4
TQIDAQAB
-----END PUBLIC KEY-----
```

## Waarschuwingsbericht - parse fout: PEM-gegevens kunnen niet worden gedecodeerd

### Symptoom

Het waarschuwingsbericht: parse fout: PEM-gegevens kunnen niet worden gedecodeerd, worden in het Threat Grid-apparaat ontvangen nadat is geprobeerd een certificaat aan een interface toe te voegen.

The screenshot shows the Threat Grid Appliance configuration page for 'Upload SSL certificate for PANDEM'. The 'Certificate (PEM)' field contains a corrupted PEM certificate. The error message 'parse error: PEM data could not be decoded' is displayed in red. The 'Private Key (PEM)' field also contains a corrupted private key. The interface includes a navigation menu on the left with 'SSL' selected, and buttons for 'Add Certificate' and 'Cancel' at the bottom.

Het certificaat kan niet worden gedecodeerd uit de huidige PEM-gegevens in het certificaatbestand. De PEM-gegevens in het certificaatbestand zijn beschadigd.

- Controleer of de certificeringsinformatie kan worden opgehaald uit de PEM-gegevens in het certificaatbestand.

Stap 1. Gebruik het OpenSSL-gereedschap om de certificaatinformatie uit het PEM-

gegevensbestand weer te geven.

```
openssl x509 -in
```

Als de PEM-gegevens beschadigd zijn, wordt er een fout waargenomen wanneer het OpenSSL-gereedschap probeert de certificaatinformatie te laden.

Voorbeeld. Probeer de certificaatinformatie niet te laden omdat er PEM-gegevens in het certificaatbestand zijn beschadigd.

```
$ 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:
```

## Waarschuwingsbericht - geen client/server CA-cert

### Symptoom

Het waarschuwingsbericht: parse fout: geen client/server CA cert, wordt ontvangen in het Threat Grid-apparaat na een poging om een CA-certificaat aan **Configuration > CA-certificaten** toe te voegen.

The screenshot shows the Threat Grid Appliance web interface. The navigation menu on the left includes 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 long base64-encoded string, with a red box highlighting the error message: "not a client/server CA cert". Below the field are "Add Certificate" and "Cancel" buttons.

De uitbreidingswaarde van basisbeperkingen in het CA-certificaat is niet gedefinieerd als CA: Inderdaad.

Bevestig met het OpenSSL-gereedschap als de vervolgwaaarde voor de basisbeperkingen op CA is ingesteld: Waar in het CA-certificaat.

Stap 1. Gebruik het OpenSSL-gereedschap om de certificaatinformatie uit het PEM-gegevensbestand weer te geven.

```
openssl x509 -in
```

Stap 2. Zoek in de certificaatinformatie de huidige waarde van de uitbreiding **Basisbeperkingen**.

Voorbeeld. Basisbeperkingswaarde voor een CA die door het Threat Grid-apparaat wordt geaccepteerd.

```
ca.01
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:TRUE
X509v3 Key Usage:
Digital Signature, Key Agreement, Certificate
```

## Gerelateerde informatie

- [Threat Grid-applicatie - Configuratiehandleidingen](#)
- [Cisco Advanced Malware Protection Virtual Private Cloud Appliance - Configuratievoorbeelden en TechNotes](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)