

Integración de AMP Virtual Private Cloud y Threat Grid Appliance

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Arquitectura de la integración](#)

[Información básica sobre la integración](#)

[Procedimiento](#)

[Regeneración de Certificados SSL](#)

[Carga de certificados SSL](#)

[El certificado de la interfaz limpia del dispositivo Threat Grid se firma automáticamente](#)

[El certificado de la interfaz limpia del dispositivo Threat Grid está firmado por una autoridad de certificación corporativa \(CA\)](#)

[Ejemplo:](#)

[Verificación](#)

[Confirmación de la actualización de disposición de muestra en la base de datos de nube privada de AMP](#)

[Ejemplo:](#)

[Resolución de problemas](#)

[Advertencia en el dispositivo de nube privada de AMP sobre host no válido, certificado no probado, clave de API no probada](#)

[Advertencia en el dispositivo de nube privada de AMP sobre clave API Threat Grid no válida](#)

[El dispositivo de nube privada de AMP recibe puntuaciones de ejemplo \$\geq 95\$, pero no se percibe ningún cambio en la disposición de la muestra](#)

[Advertencia en el dispositivo de nube privada de AMP sobre certificado SSL de Threat Grid inválido](#)

[Advertencias en el dispositivo Threat Grid relacionadas con los certificados](#)

[Mensaje de advertencia: la clave pública derivada de la clave privada no coincide](#)

[Mensaje de advertencia: la clave privada contiene contenido no PEM](#)

[Mensaje de advertencia: no se puede generar la clave pública a partir de la clave privada](#)

[Mensaje de advertencia - error de análisis: No se pudieron descodificar los datos PEM](#)

[Mensaje de advertencia: no es un certificado de CA de cliente/servidor](#)

[Información Relacionada](#)

Introducción

Este documento describe el procedimiento para completar la integración de la nube privada virtual de protección frente a malware avanzado (AMP) y el dispositivo Threat Grid. El documento también proporciona pasos para la resolución de problemas relacionados con el proceso de integración.

Colaborado por Armando Garcia, Ingeniero del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Trabaje y opere en AMP Nube privada virtual
- Trabajar y utilizar el dispositivo Threat Grid

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

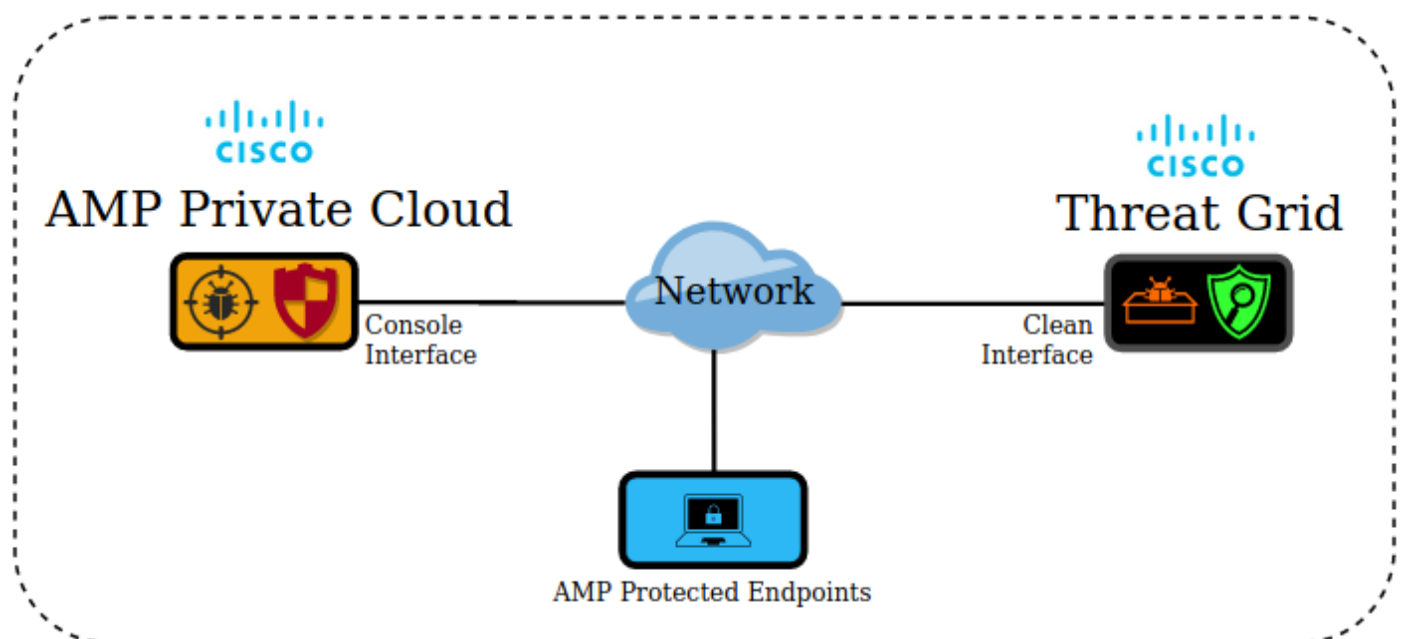
- AMP Private Cloud 3.2.0
- Threat Grid Appliance 2.12.0.1

Nota: La documentación es válida para los dispositivos Threat Grid y los dispositivos AMP Private Cloud en el dispositivo o en la versión virtual.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Arquitectura de la integración



Información básica sobre la integración

- El dispositivo Threat Grid analiza muestras enviadas por el dispositivo de nube privada de

AMP.

- Los ejemplos se pueden enviar de forma manual o automática al dispositivo Threat Grid.
- El análisis automático no está habilitado de forma predeterminada en el dispositivo AMP Private Cloud.
- El dispositivo Threat Grid proporciona al dispositivo AMP Private Cloud un informe y una puntuación a partir del análisis de la muestra.
- El dispositivo Threat Grid informa (roke) al dispositivo AMP para nube privada sobre cualquier muestra con una puntuación de 95 o más.
- Si la puntuación del análisis es mayor o igual a 95, el ejemplo de la base de datos de AMP se marca con una disposición maliciosa.
- AMP Private Cloud aplica las detecciones retrospectivas a muestras con una puntuación igual o superior a 95.

Procedimiento

Paso 1. Configure y configure el dispositivo Threat Grid (sin integración aún). Compruebe si hay actualizaciones e instálelas, si es necesario.

Paso 2. Configure y configure AMP para terminales de nube privada (sin integración aún).

Paso 3. En la interfaz de usuario del administrador de Threat Grid, seleccione la ficha **Configuration** y elija **SSL**.

Paso 4. Genere o cargue un nuevo certificado SSL para la interfaz limpia (PANDEM).

Regeneración de Certificados SSL

Se puede generar un nuevo certificado autofirmado si el nombre de host de la interfaz limpia no coincide con el nombre alternativo del sujeto (SAN) en el certificado actualmente instalado en el dispositivo para la interfaz limpia. El dispositivo genera un nuevo certificado para la interfaz, configurando el nombre de host de la interfaz actual en el campo SAN del certificado autofirmado.

Paso 4.1. En la columna Acciones seleccione (...) y en el menú emergente seleccione **Generar nuevo certificado**.

Paso 4.2. En la interfaz de usuario de Threat Grid, seleccione **Operations**, en la siguiente pantalla seleccione **Activate** y elija **Reconfigure**.

Nota: Este certificado generado se firma automáticamente.

Carga de certificados SSL

Si ya se ha creado un certificado para la interfaz limpia del dispositivo Threat Grid, este certificado se puede cargar en el dispositivo.

Paso 4.1. En la columna Acciones seleccione (...) y en el menú emergente seleccione **Cargar certificado nuevo**.

Paso 4.2. Copie el certificado y la clave privada correspondiente en formato PEM en los cuadros de texto que aparecen en la pantalla y seleccione **Agregar certificado**.

Paso 4.3. En la interfaz de usuario de Threat Grid, seleccione **Operations**, en la siguiente pantalla seleccione **Activate** y elija **Reconfigure**.

Paso 5. En la interfaz de usuario de administración del dispositivo de nube privada de AMP, seleccione **Integrations** y elija **Threat Grid**.

Paso 6. En Detalles de configuración de Threat Grid, seleccione **Editar**.

Paso 7. En el nombre de host de Threat Grid, introduzca el FQDN de la interfaz limpia del dispositivo Threat Grid.

Paso 8. En el certificado SSL de Threat Grid, agregue el certificado de la interfaz limpia del dispositivo Threat Grid. (Véanse las notas a continuación)

El certificado de la interfaz limpia del dispositivo Threat Grid se firma automáticamente

Paso 8.1. En la interfaz de usuario del administrador de Threat Grid, seleccione la **configuración** y elija **SSL**.

Paso 8.2. En la columna Acciones seleccione (...) y en el menú emergente seleccione **Descargar certificado**.

Paso 8.3. Continúe agregando el archivo descargado al dispositivo AMP Virtual Private en la página de integración de Threat Grid.

El certificado de la interfaz limpia del dispositivo Threat Grid está firmado por una autoridad de certificación corporativa (CA)

Paso 8.1. Copie en un archivo de texto el certificado de la interfaz limpia del dispositivo Threat Grid y la cadena completa de certificados de CA.

Nota: Los certificados del archivo de texto deben estar en formato PEM.

Ejemplo:

Si la cadena de certificados completa es: certificado ROOT_CA > certificado Threat_Grid_Clean_Interface; luego, el archivo de texto debe crearse, como se muestra en la imagen.

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

Si la cadena de certificados completa es: Certificado ROOT_CA > Certificado Sub_CA > Certificado Threat_Grid_Clean_Interface; luego, el archivo de texto debe crearse, como se muestra en la imagen.

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

Paso 9. En Threat Grid API Key (Clave de API de Threat Grid), introduzca la clave de API del usuario de Threat Grid que se vinculará a los ejemplos cargados.

API

API Key *****  

Disable API Key  True False Unset

Can Download Sample Content Via API  True False Unset

Nota: En la configuración de cuenta del usuario de Threat Grid, confirme que el parámetro **Disable API Key** no está establecido en True.

Paso 10. Una vez completados todos los cambios, seleccione **Guardar**.

Paso 11. Aplique una reconfiguración al dispositivo AMP Virtual Cloud.

Paso 12. En la interfaz de usuario de administración del dispositivo de nube privada de AMP, seleccione **Integrations** y elija **Threat Grid**.

Paso 13. En **Detalles**, copie los valores de la URL del Servicio de actualización de la disposición, el usuario del Servicio de actualización de la disposición y la contraseña del Servicio de actualización de la disposición. Esta información se utiliza en el Paso 17.

Paso 14. En la interfaz de usuario del administrador de Threat Grid, seleccione **Configuration** y elija **CA Certificates**.

Paso 15. Seleccione **Agregar certificado** y copie en formato PEM el certificado de CA que firmó el certificado de servicio de actualización de disposición de nube privada de AMP.

Nota: Si el certificado de CA que firmó el certificado de actualización de disposición de nube privada de AMP es una sub-CA, repita el proceso hasta que todas las CA de la cadena se carguen en **certificados de CA**.

Paso 16. En el portal Threat Grid, seleccione Administration (Administración) y seleccione Manage AMP Private Cloud Integration (Gestión de la integración de nube privada de AMP).

Paso 17. En la página Servicio de distribución de actualización de disposición, introduzca la información recopilada en el paso 13.

- URL de servicio: FQDN del servicio de actualización de disposición del dispositivo de nube privada de AMP.
- Usuario: usuario del servicio de actualización de disposición del dispositivo de nube privada de AMP.
- Contraseña: contraseña para el servicio de actualización de disposición del dispositivo de nube privada de AMP.

En este punto, si todos los pasos se aplicaron correctamente, la integración debe estar funcionando correctamente.

Verificación

Estos son los pasos para confirmar que el dispositivo Threat Grid se integró correctamente.

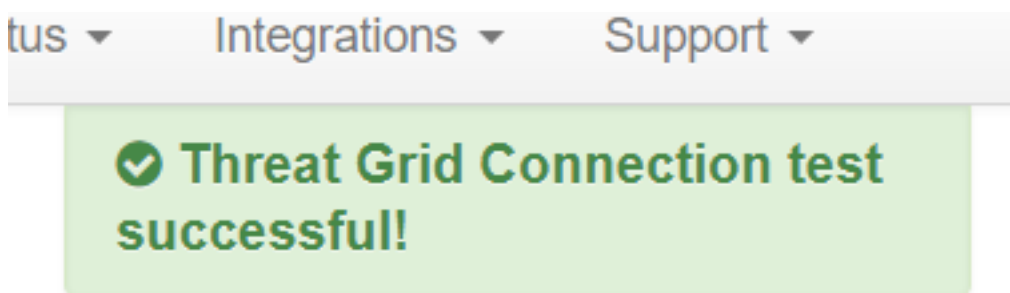
Nota: Sólo los pasos 1, 2, 3 y 4 son adecuados para ser aplicados en un entorno de producción para verificar la integración. El paso 5 se proporciona como información para obtener más información sobre la integración y no se aconseja que se aplique en un entorno de producción.

Paso 1. Seleccione Probar conexión en AMP Private Cloud Device Admin UI > Integrations > Threat Grid y confirme el mensaje Threat Grid Connection test satisfactoria. se recibe.

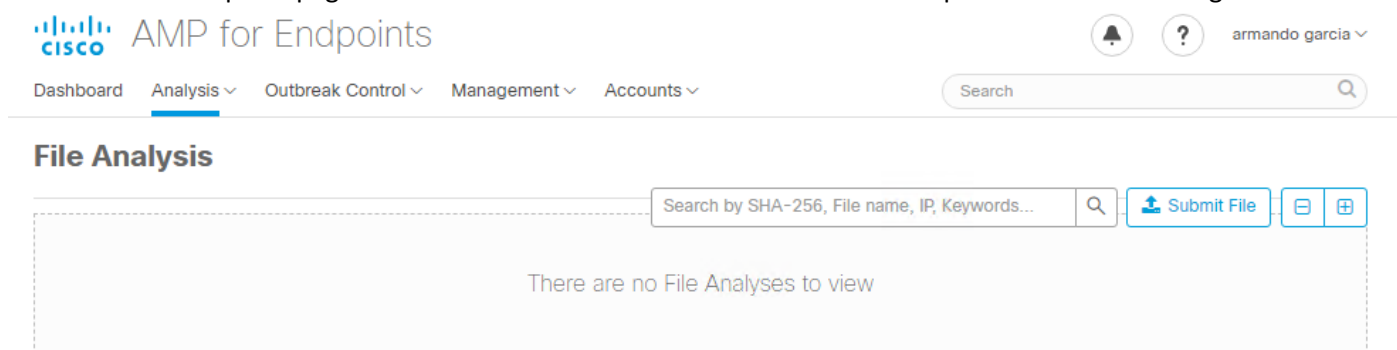
Threat Grid Configuration Details Edit

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



Paso 2. Confirme que la página web Análisis de archivos de la consola de nube privada de AMP se cargue sin errores.



Paso 3. Confirme que los archivos enviados manualmente desde la consola de nube privada de AMP **Analysis > File Analysis** se perciben en el dispositivo Threat Grid y que el dispositivo Threat Grid devuelve un informe con una puntuación.

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

Paso 4. Confirme que las CA que firmaron el certificado de Servicio de actualización de la disposición del dispositivo de nube privada de AMP estén instaladas en el dispositivo Threat Grid en **Autoridades de Certificados**.

Paso 5. Confirme que cualquier muestra marcada por el dispositivo Threat Grid con una puntuación ≥ 95 se registre en la base de datos de AMP Private Cloud con la disposición de malicioso después de que el informe y la puntuación de ejemplo sean proporcionados por el dispositivo Threat Grid.

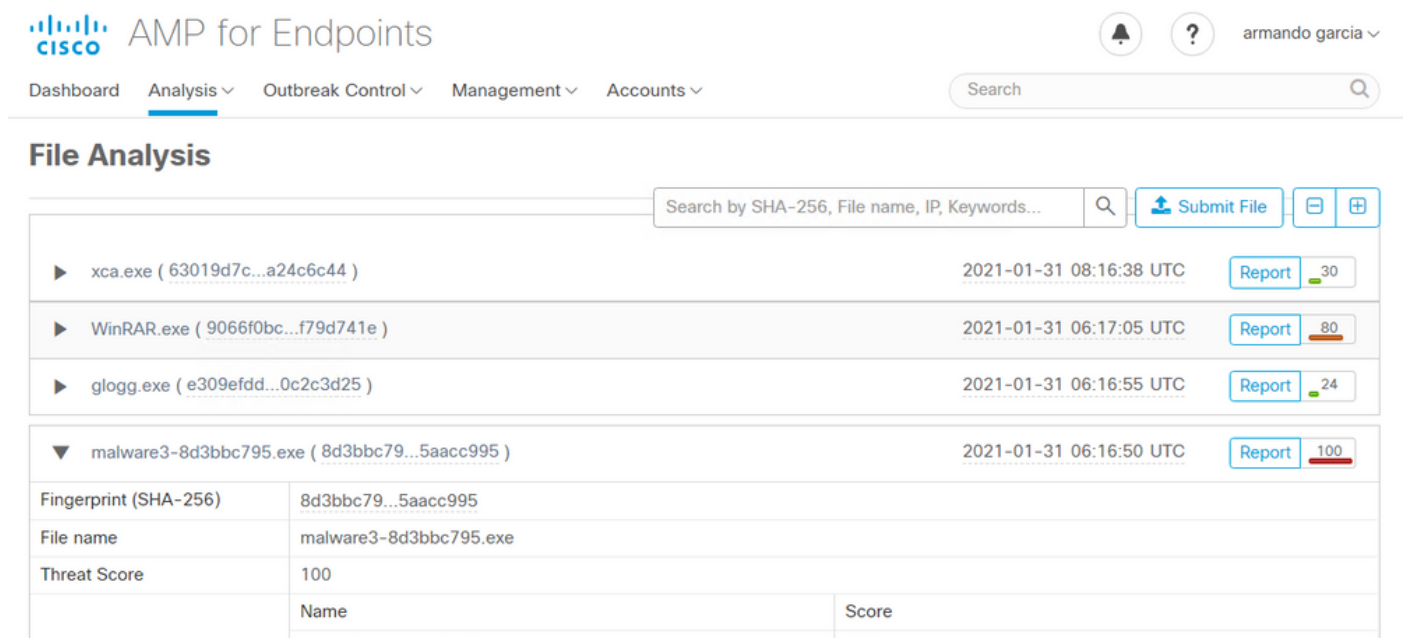
Nota: Una recepción correcta del informe de muestra y una puntuación de muestra ≥ 95 en la consola de nube privada de AMP en la pestaña **Análisis de archivos**, no significa necesariamente que la disposición del archivo se haya cambiado en la base de datos de AMP. Si las CA que firmaron el certificado de Servicio de actualización de la disposición del dispositivo de nube privada de AMP no se instalan en el dispositivo Threat Grid en **Autoridades de Certificados**, el dispositivo de nube privada de AMP recibe informes y puntuaciones, pero no se recibe ningún error en el dispositivo Threat Grid.

Advertencia: La siguiente prueba se completó para activar un cambio de disposición de muestra en la base de datos de AMP después de que el dispositivo Threat Grid haya marcado un archivo con una puntuación ≥ 95 . El objetivo de esta prueba era proporcionar información sobre las operaciones internas en el dispositivo de nube privada de AMP cuando el dispositivo Threat Grid proporciona una puntuación de muestra de ≥ 95 . Para activar el proceso de cambio de disposición, se creó un archivo de prueba de imitación de malware con la aplicación interna makemalware.exe de Cisco. Ejemplo: malware3-419d23483.exeSHA256:
8d3bbc795bb4747984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc9955.

Precaución: No se recomienda detonar ningún archivo de prueba de imitación de malware en un entorno de producción.

Confirmación de la actualización de disposición de muestra en la base de datos de nube privada de AMP

El archivo de prueba de malware se envió manualmente al dispositivo Threat Grid desde **Análisis de archivos** en la consola de AMP para nube privada. Tras el análisis de la muestra, el dispositivo Threat Grid proporcionó al dispositivo AMP para nube privada un informe de muestra y una puntuación de muestra de 100. Una puntuación de ejemplo ≥ 95 desencadena un cambio de disposición para el ejemplo en la base de datos de dispositivos de nube privada de AMP. Este cambio de la disposición de muestra en la base de datos de AMP basado en una puntuación de muestra ≥ 95 proporcionada por Threat Grid es lo que se conoce como una referencia.



The screenshot shows the AMP for Endpoints File Analysis interface. At the top, there is a navigation bar with 'Dashboard', 'Analysis', 'Outbreak Control', 'Management', and 'Accounts'. A search bar is present on the right. The main section is titled 'File Analysis' and contains a table of analyzed files. The table has columns for file name, timestamp, and a 'Report' button with a score indicator. The file 'malware3-8d3bbc795.exe' is highlighted, and its details are shown below in a table format.

Name	Score
malware3-8d3bbc795.exe	100

Si:

- La integración se completó correctamente.
- Los informes de muestra y las puntuaciones se perciben en **Análisis de archivos** después de enviar manualmente los archivos.

Luego:

- Para cada muestra que marca el dispositivo Threat Grid con una puntuación ≥ 95 , se agrega una entrada al archivo `/data/poked/poked.log` en el dispositivo AMP Private Cloud.
- `/data/poked/poked.log` se crea en el dispositivo AMP Private Cloud después de que el appliance Threat Grid proporcione la primera puntuación de ejemplo ≥ 95 .
- La base de datos `db_Protect` de AMP Private Cloud contiene la disposición actual para el ejemplo. Esta información se puede utilizar para confirmar si la muestra tiene una disposición de 3 después de que el dispositivo Threat Grid haya proporcionado la puntuación.

Si el informe de ejemplo y la puntuación ≥ 95 se perciben en **Análisis de archivos** en la consola

de nube privada de AMP, siga estos pasos:

Paso 1. Inicie sesión mediante SSH en el dispositivo AMP Private Cloud.

Paso 2. Confirme que hay una entrada en /data/poked/poked.log para el ejemplo.

Al enumerar el directorio /data/poked/ en un dispositivo AMP Private Cloud que nunca ha recibido una puntuación de ejemplo ≥ 95 de un dispositivo Threat Grid, se muestra que el archivo poked.log no se ha creado en el sistema.

Si el dispositivo de nube privada de AMP nunca ha recibido un golpe de un dispositivo de Threat Grid, el archivo /data/poked/poked.log no se encuentra en el directorio, como se muestra en la imagen.

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

Al listar el directorio /data/poked/ después de recibir la primera puntuación de ejemplo ≥ 95 , se muestra el archivo creado.

Después de recibir la primera muestra con una puntuación ≥ 95 .

```
[root@fireamp ~]# ls /data/poked/
poked_error.log  poked.log
[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": "8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995", "engine": "sha256", "user": "-", "mode": "tg", "score": 100}
[root@fireamp ~]#
```

La información de ejemplo del switch proporcionado por el dispositivo Threat Grid se puede percibir dentro del archivo poked.log.

Paso 3. **Ejecute** este comando con el ejemplo SHA256 para recuperar la disposición actual de la base de datos del dispositivo AMP Private Cloud.

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

Ejemplo:

Una consulta de base de datos para obtener la disposición de ejemplo antes de cargar el ejemplo en el dispositivo Threat Grid no proporciona resultados, como se muestra en la imagen.

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

Una consulta de base de datos para obtener la disposición de muestra después de que se recibieron el informe y la puntuación desde el dispositivo Threat Grid, muestra el ejemplo con una disposición de 3 que se considera maliciosa.

```
[root@fireamp ~]# mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995;"
+-----+-----+
| hex(fingerprint) | disposition_id |
+-----+-----+
| 80388C795BB47447984BF2842D3A0119BAC0D79A15A59686951E1F7C5AACC995 | 3 |
+-----+-----+
[root@fireamp ~]#
```

Resolución de problemas

En el proceso de integración, se pueden percibir posibles problemas. En esta parte del documento se abordan algunas de las cuestiones más comunes.

Advertencia en el dispositivo de nube privada de AMP sobre host no válido, certificado no probado, clave de API no probada

Síntoma

El mensaje de advertencia: El host de Threat Grid no es válido, el certificado SSL de Threat Grid no se pudo probar, la clave de la API de Threat Grid no se pudo probar, se recibe en el dispositivo AMP Private Cloud después de seleccionar el botón **Test Connection** en **Integraciones > 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.

Hay un problema en el nivel de red en la integración.

Pasos recomendados:

- Confirme que la interfaz de la consola del dispositivo de nube privada de AMP puede alcanzar la interfaz limpia del dispositivo Threat Grid.
- Confirme que el dispositivo de nube privada de AMP pueda resolver el FQDN de la interfaz limpia del dispositivo Threat Grid.
- Confirme que no hay ningún dispositivo de filtrado en la ruta de red del dispositivo de nube privada de AMP y del dispositivo Threat Grid.

Advertencia en el dispositivo de nube privada de AMP sobre clave API Threat Grid no válida

Síntoma

El mensaje de advertencia: Falló la prueba de Threat Grid Connection, la API de Threat Grid no es válida, se recibe en el dispositivo AMP Private Cloud después de seleccionar el botón **Probar conexión** en **Integraciones > Threat Grid**.

Connect Threat Grid Appliance to AMP for Endpoints Appliance

Threat Grid Connection test failed.

- Threat Grid API key is invalid.

La clave API del dispositivo Threat Grid configurada en la nube privada de AMP.

Pasos recomendados:

- Confirme en la configuración de cuenta del usuario del dispositivo Threat Grid, el parámetro Disable API Key (Desactivar clave de API) no se establece en True.
 - El parámetro Disable API Key (Desactivar clave de API) debe establecerse en: False o Unset.

API

API Key *****  

Disable API Key  True False Unset

Can Download Sample Content Via API  True False Unset

- Confirme que la clave de API de Threat Grid configurada en el portal de administración de AMP para nube privada **Integrations > Threat Grid**, sea la misma clave de API en la configuración del usuario en el dispositivo Threat Grid.
- Confirme si la clave de API Threat Grid correcta se guarda en la base de datos de dispositivos de AMP para nube privada.

Desde la línea de comandos del dispositivo de nube privada de AMP, se puede confirmar la clave de API de Threat Grid actual configurada en el dispositivo AMP. Inicie sesión en el dispositivo de nube privada de AMP mediante SSH y ejecute este comando para recuperar la clave de API del usuario de Threat Grid actual:

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

Se trata de una entrada correcta en la base de datos del dispositivo de nube privada de AMP para la clave API del dispositivo Threat Grid.

```
[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 ~]#
```

Aunque el nombre de usuario de Threat Grid no se configuró directamente en el dispositivo de nube privada de AMP en ningún paso de la integración, el nombre de usuario de Threat Grid se percibe en el parámetro tg_login de la base de datos de AMP si la clave API de Threat Grid se aplicó correctamente.

Se trata de una entrada errónea en la base de datos de AMP para la clave de la API Threat Grid.

```
[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 ~]#
```

El parámetro tg_login es NULL. El dispositivo de nube privada de AMP no recuperó el nombre de usuario de Threat Grid después de aplicar la reconfiguración.

El dispositivo de nube privada de AMP recibe puntuaciones de ejemplo >=95, pero no se percibe ningún cambio en la disposición de la muestra

Síntoma

Los informes y >=95 puntuaciones de ejemplo se reciben correctamente del dispositivo Threat Grid después de enviar una muestra, pero no se percibe ningún cambio en la disposición de la muestra en el dispositivo AMP Private Cloud.

Pasos recomendados:

- Confirme en el dispositivo de nube privada de AMP si el SHA256 de muestra se encuentra en el contenido de /data/poked/poked.log.

Si el SHA256 se encuentra en /data/poked/poked.log, ejecute este comando para confirmar la disposición de ejemplo actual en la base de datos de AMP.

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

- Confirme que se agregó la contraseña de integración de AMP para nube privada al portal de administración de dispositivos Threat Grid en **Administration > Manage AMP Private Cloud Integration**.

Portal de administración de nube privada de AMP.

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]kJYfPK"/> <input type="button" value="Change Password"/>

Portal de la consola del dispositivo Threat Grid.



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="password" value="ew236[]xJYfPK"/>	Save Cancel
<input type="text"/>	disposition_update_user	Edit Remove

- Confirme que las CA que firmaron el certificado del servicio de actualización de disposición del dispositivo de nube privada de AMP se instalaron en el portal de administración del dispositivo Threat Grid en **certificados CA**.

En el siguiente ejemplo, la cadena de certificado para el certificado del servicio de actualización de disposición del dispositivo de nube privada de AMP es **Root_CA > Sub_CA > Certificado de Disposition_Update_Service**; por lo tanto, RootCA y Sub_CA deben estar instalados en **certificados CA** en el dispositivo Threat Grid.

Certifica a las autoridades en el portal de administración de nube privada de AMP.



✖ 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	- 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	

Portal de administración de Threat Grid:

- Confirme que el FQDN del servicio de actualización de la disposición del dispositivo de nube privada de AMP se agregó correctamente al portal de administración del dispositivo Threat Grid en **Administration > Manage AMP Private Cloud Integration**. Confirme también que no se agregó la dirección IP de la interfaz de la consola del dispositivo de nube privada de AMP en lugar del FQDN.

Advertencia en el dispositivo de nube privada de AMP sobre certificado SSL de Threat Grid inválido

Síntoma

El mensaje de advertencia: "El certificado SSL de Threat Grid no es válido", se recibe en el dispositivo de nube privada de AMP después de seleccionar el botón **Probar conexión** en **Integraciones > Cuadrícula de amenaza**.

Pasos recomendados:

- Confirme si el certificado instalado en la interfaz limpia del dispositivo Threat Grid está firmado por una CA corporativa.

Si está firmado por una CA, la cadena de certificados completa se debe agregar dentro de un archivo a AMP Private Cloud Device Administration Portal **Integrations > Threat Grid** en **Threat**

Grid SSL Certificate.

Threat Grid Configuration Details

Hostname: [redacted] cisco.com

API Key: [redacted]

Threat Grid SSL Certificate

Issuer	subca_tga_clean	
Subject	[redacted] cisco.com	
Validity	2020-11-24 00:00:00 UTC	2021-11-23 23:59:59 UTC

Test Connection

En el dispositivo de nube privada de AMP, los certificados de dispositivo de Threat Grid instalados actualmente se encuentran en: /opt/fire/etc/ssl/threat_grid.crt.

Advertencias en el dispositivo Threat Grid relacionadas con los certificados

Mensaje de advertencia: la clave pública derivada de la clave privada no coincide

Síntoma

El mensaje de advertencia: la clave pública derivada de la clave privada no coincide, se recibe en el dispositivo Threat Grid después de intentar agregar un certificado a una interfaz.

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-----
hvcNAQELBQADggEBAKXz8olDWacWY5V0XSHWrQIMULAMNAE8OZIXNkuByG6vvhj
P
JkgjjU9xKrke5LCr+trWnr+qjZlc4ecVCm8FXBWUtr8BjHcimbHUbZIVLYp6WDxO
[redacted]
HMS37fv44R9Cir4pjUz0bc61HS4wo5PAfUyjPtO1Dy0dHia4zE3pH4X3D9rzQYYd
Cl6KJpevCJzFyoQW3ahTZoxr4F11I5wO3XcH41Q=
-----END CERTIFICATE-----
```

Private Key (PEM)

```
-----BEGIN RSA PRIVATE KEY-----
wZfa8sZJp30zivJRtvBioPnwmPpNZzhqIW3cC90ASaRSXeU+4c+HmUknahEHJNn8
IjbaA4UJQgWgeD4QKOj8cQKBgQCIZmRmL7H7d1avaPzbEIA0kYnlqIXsBKDCHjYo
g+H0Nxldl8zU5HYFab9LO361thYO+OBwd3EGhbQ2u7CeinFp8Y7mQuqQNFtBHIZO
[redacted]
/8E/D+jd18zhA3aWnXADf8b9xjIRE3241FAfJf73a59q27y7d96tCa1PFaMOiXGc
nY2D9lwNsn5uk1IHL2SojLtVx8BYqw98w0uuBOmqZZVNprSparsyw==
-----END RSA PRIVATE KEY-----
```

public key derived from private key does not match

Add Certificate Cancel

La clave pública exportada desde la clave privada no coincide con la clave pública configurada en

el certificado.

Pasos recomendados:

- Confirme si la clave privada coincide con la clave pública del certificado.

Si la clave privada coincide con la clave pública del certificado, el módulo y el exponente público deben ser los mismos. Para este análisis, basta con confirmar si el módulo tiene el mismo valor en la clave privada y la clave pública en el certificado.

Paso 1. Utilice la herramienta OpenSSL para comparar el módulo en la clave privada y la clave pública configurada en el certificado.

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

Ejemplo. Coincidencia correcta de una clave privada y una clave pública configuradas en un certificado.

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

Mensaje de advertencia: la clave privada contiene contenido no PEM

Síntoma

El mensaje de advertencia: La clave privada contiene contenido que no es de PEM y se recibe en el dispositivo Threat Grid después de intentar agregar un certificado a una interfaz.

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
AwwPc3ViY2FfdGdhX2NsZWZuMB4XDTEwMTEyMDAwMDAwMFoXDTEwMTEyMTEyMzNT
k1
OVowSTEBMBkGA1UEChMQS2l2Y28gU3lzdGVtcywgSW5jMSowKAYDVQQDEyFrc2Vj
[Redacted]
NlgQT03qqfX7Zh5wKY4BrTWxOpNBodUcl0KxzODPWYZqUUjpeKcJyUkj2L6fY0OV
```

Private Key (PEM)

```
wZfa8sZJp30zivJRtvBioPnwmPpNZzhqIW3cC90ASaRSXeU+4c+HmUknahEHJNn8
lJbkA4UJQgWgeD4QKOj8cQKBgQCIZmRmL7H7d1avaPzbEIA0kYnlqIXsBKDCHjYo
g+H0NxlIdl8zU5HYFab9LO361thYO+OBwd3EGhbQ2u7CeinFp8Y7mQuqQNFTbHIZO
[Redacted]
/8E/D+jdT8zhA3aWNXADf8b9xjIRE324TFafJf73a59q27y7d96tCa1PFaMOiXGc
nY2D9lwNsnl5uk1IHL2SojLtvx8BYqw98w0uuBOMqZZVNprSparsyw==
-----END RSA PRIVATE KEY-----
```

private key contains non-PEM content

Los datos PEM dentro del archivo de clave privada están dañados.

Pasos recomendados:

- Confirme la integridad de los datos dentro de la clave privada.

Paso 1. Utilice la herramienta OpenSSL para verificar la integridad de la clave privada.

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

Ejemplo. Salidas de una clave privada con errores en los datos PEM dentro del archivo y de otra clave privada sin errores en el contenido PEM.

```
$ 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
```

Si el resultado del comando OpenSSL no es **RSA Key ok**, esto significa que se encontraron problemas con los datos PEM dentro de la clave.

Si se encontraron problemas con el comando OpenSSL, entonces:

- Confirme si faltan datos PEM dentro de la clave privada.

Los datos PEM dentro del archivo de clave privada se muestran en líneas de 64 caracteres. Una revisión rápida de los datos PEM dentro del archivo puede mostrar si faltan datos. La línea con datos que faltan no está alineada con otras líneas del archivo.

```

$ 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
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
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-----

```

- Confirme que la primera línea de la clave privada comienza con 5 guiones, las palabras **BEGIN PRIVATE KEY** y finaliza con 5 guiones.

Ejemplo.

—COMENZAR CLAVE PRIVADA—

- Confirme que la última línea de la clave privada comience con 5 guiones, las palabras **END PRIVATE KEY** y termine con 5 guiones.

Ejemplo.

—FINALIZAR CLAVE PRIVADA—

Ejemplo. Formato PEM y datos correctos dentro de una clave privada.

```
$ cat correct-private-key.key
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCvfIytwKf9UIc5
DluK9PTbKvDrShgn8/Cen9wXEUDIBNahlFiZvwZb/5FL+I1ry/P0WKJMiXRhLQ52
Y0oogQsuDTw79Moa6xXYLKq1P5QRIV6tQQDNiHUoHFNSLkoo0H0ubkDtGo/Pw4fE
/JNGbMIU/d1DDuzxfGze0viztT90rpCbZyQP2r+sGxa0KM0c3AEgK/pYA7aCv/G
P6rGkHc/ViM1NTuWVIWdIcLgTUX0DeHLjTicI2q/vH/i0WeIgAv10aGuBC0egVDU
NwOgPyY3XI8g7H 4HA6/VsM10NHKT4EhvSks
WXZW1XhNAgMBAAtU9huSCL7t4BF7VpSeKXM
Uh4/Vrdg1TYXFBs7k0sCwmhKUaMAcTYAnrg
fINIJto/x0azhe47ttvLvX3zweLCEXsDXK6
mdhzCQSTBfYbM4R4M7HiocsbkLjijScTFYQ
JqSwA5BEgqeH3ahgd4kJ6ddAaSjQS7sJxaf
WtVHzbVDqJ+rb9BgQDePpxacxGRZLXfja3s
SU+TvjNWQGcUsXa8y8ZQd0lqPZrV0Z6Mym2
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/60smGGsXz10Mn+A0
SxuwKWoARshnMsDvsTYwofmlSMwTlMmCKpbTiiECgYBi8ZjgsdFv2NtYlmb1pAYS
DHierbltdVumF42Tax+fucqUrdB3LZo6FjagvPy+LBjA3VjtRYkDjQmstvxD5jfd
V3Pq4IwaocGU8RQUJY5L6rmw+y1s6Z+iNkIcPeZtwidSgP+NZa1xvhfj8XeL560o
a+IQn0Y41zLJ22ScgyFzEQ==
-----END PRIVATE KEY-----
```

Mensaje de advertencia: no se puede generar la clave pública a partir de la clave privada

Síntoma

El mensaje de advertencia: no se puede generar una clave pública a partir de la clave privada. Se recibe en el dispositivo Threat Grid después de intentar agregar un certificado a una interfaz.

- 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-----
MIIEpAIBAAKCAQEaucb3AU15P91Ym/PvHva/xKBCbLeY7+jQJGO7wm7eruX3KTZY
EE9N6qn1+2YecCmOAA01sTqTQaHVVHJdCsczgz1mGalFI6Xinl8JI9i+n2NDIcNr
XBVPvCUs5fnH2cZwKGTen/NDJhnyC5DIb17RLy7Y+wxhMiyRCHH3aZ3I0Mpl1k4X
[Redacted]
cjSc9W8Fy/CDXbX27KncS4qWe91phsKXq0jo7wIDAQABAolBAFrH8EHRsvNTXY5v
yCSwXQtfalYpjXGGqdduaPzdlrICrCGWbbgimKeYQByGTU9v7vXAx2EAh57Izvb2
```

cannot generate public key from private key

La clave pública no se puede generar a partir de los datos PEM actuales dentro del archivo de clave privada.

Pasos recomendados:

- Confirme la integridad de los datos dentro de la clave privada.

Paso 1. Utilice la herramienta OpenSSL para verificar la integridad de la clave privada.

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

Si el resultado del comando OpenSSL no es **RSA Key ok**, esto significa que se encontraron problemas con los datos PEM dentro de la clave.

Paso 2. Utilice la herramienta OpenSSL para verificar si la clave pública se puede exportar desde la clave privada.

```
openssl rsa -in
```

Ejemplo. Exportación fallida de clave pública y exportación correcta de clave pública.


```
$ 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-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3yMrcJH/VCH0Q5bivT0
2yrw60oYJ/Pwnp/cFxFayATWoZRYmb8GW/+RS/iNa8vz9FiiTII0YS0dmNKKIEL
Lg080/TKGusV2CygqT+UESFerUEAzYh1KBxTUI5KKNB9Lm5A7RqPz1uHxPyTRmzC
FP3dQw7s8X4Bs3tL4s7U/Tq6Qm2ckD9q/rBswjiJNHNwBICv6WA02gr/xj+qxpB3
P1YjNTU711SFnSHC4E1Fzg3hy40yHCNqv7x/4j1niIAL9dGhrGQjnoFQ1DcDoD8m
N1yPIOx3C0lWeVForZmx+Dg61+J4uIjytkVceBw0v1bDnDRyk+BIB0pLF12VtV4
TQIDAQAB
-----END PUBLIC KEY-----
```

Mensaje de advertencia - error de análisis: No se pudieron decodificar los datos PEM

Síntoma

El mensaje de advertencia: error de análisis: No se pudieron decodificar los datos PEM; se reciben en el dispositivo Threat Grid después de intentar agregar un certificado a una interfaz.

The screenshot shows the Cisco Threat Grid Appliance interface. The left sidebar contains a navigation menu with options: Configuration, Authentication, CA Certificates, Change Password, Clustering, Date and Time, Email, Integrations, License, Network, Network Exit, NFS, Notifications, SSH, SSL (highlighted), and Syslog. The main content area is titled "Upload SSL certificate for PANDEM". It has two input fields: "Certificate (PEM)" and "Private Key (PEM)". Both fields contain base64-encoded data. Below the "Certificate (PEM)" field, a red error message reads: "parse error: PEM data could not be decoded". At the bottom of the form are two buttons: "Add Certificate" and "Cancel".

El certificado no se puede decodificar a partir de los datos PEM actuales dentro del archivo de certificado. Los datos PEM dentro del archivo de certificado están dañados.

- Confirme si la información del certificado se puede recuperar de los datos PEM dentro del archivo de certificado.

Paso 1. Utilice la herramienta OpenSSL para mostrar la información del certificado del archivo de datos PEM.

```
openssl x509 -in
```

Si los datos PEM están dañados, se percibe un error cuando la herramienta OpenSSL intenta cargar la información del certificado.

Ejemplo. Error al intentar cargar la información del certificado debido a los datos PEM dañados en el archivo de certificado.

```
$ 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:
```

Mensaje de advertencia: no es un certificado de CA de cliente/servidor

Síntoma

El mensaje de advertencia: error de análisis: no se recibe un certificado de CA cliente/servidor en el dispositivo Threat Grid después de intentar agregar un certificado de CA a **Configuration > CA Certificates**.

The screenshot shows the Threat Grid Appliance web interface. The top navigation bar includes 'Home', 'Configuration', 'Status', 'Operations', and 'Support'. The left sidebar is blue and contains a menu with 'Configuration' at the top, followed by 'Authentication', 'CA Certificates' (which is highlighted), '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 certificate text is partially obscured by a red box and a black redaction bar. The visible text includes: 'Ir2MrtEmB8vuU3CzLqSnC3iFRYF9bbwiQTw/AgMBAAGjDzANMAsGA1UdDwQEAwICjDANBgkqhkiG9w0BAQsFAAOCAQEAY3b0+QmLE0Ri7q3iHUSK3cGcWhCrWIF5z3ORw6yBX1YrWKICWS0mT8K/3mscEbUvyjALFRvoGccYLlI3wboaB8ZLxysEL6Nw7r+5AtTgHWYUEdrgnnAUjQbiOls+NUY826gpRwuH7PBYT9k33OK8XSzo8xmsQQG+oHOoL2wj6R2hS8e7dzJzHbsp+1icL/w7MAuFRWkTA0j7gEbKmYj+0Q=='. Below the certificate, a red message reads 'not a client/server CA cert'. At the bottom of the page, there are two buttons: 'Add Certificate' and 'Cancel'.

El valor de extensión de restricciones básicas del certificado de CA no se define como CA: Verdadero.

Confirme con la herramienta OpenSSL si el valor de extensión de restricciones básicas está establecido en CA: True en el certificado de CA.

Paso 1. Utilice la herramienta OpenSSL para mostrar la información del certificado del archivo de datos PEM.

```
openssl x509 -in
```

Paso 2. Busque en la información del certificado el valor actual de la extensión **restricciones básicas**.

Ejemplo. Valor de restricción básico para una CA aceptada por el dispositivo Threat Grid.

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

Información Relacionada

- [Appliance Threat Grid: Guías de configuración](#)
- [Appliance de nube privada virtual AMP de Cisco: ejemplos de configuración y notas técnicas](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)