

Integrazione di AMP Virtual Private Cloud e Threat Grid Appliance

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Architettura dell'integrazione](#)

[Informazioni di base sull'integrazione](#)

[Procedura](#)

[Rigenerazione dei certificati SSL](#)

[Caricamento dei certificati SSL](#)

[Il certificato nell'interfaccia pulita dell'accessorio Threat Grid è autofirmato](#)

[Il certificato nell'interfaccia pulita dell'accessorio Threat Grid è firmato da un'autorità di certificazione \(CA\) aziendale](#)

[Esempio](#)

[Verifica](#)

[Conferma dell'aggiornamento della disposizione del campione nel database cloud privato AMP](#)

[Esempio](#)

[Risoluzione dei problemi](#)

[Avviso nel dispositivo cloud privato AMP: host non valido, certificato non testato, chiave API non testata](#)

[Avviso nel dispositivo cloud privato AMP relativo alla chiave API Threat Grid non valida](#)

[I punteggi dei campioni >=95 vengono ricevuti dal dispositivo AMP Private Cloud, ma la disposizione del campione non cambia](#)

[Avviso nel dispositivo cloud privato AMP relativo a un certificato SSL della griglia delle minacce non valido](#)

[Avvisi relativi ai certificati nell'accessorio Threat Grid](#)

[Messaggio di avviso - La chiave pubblica derivata dalla chiave privata non corrisponde](#)

[Messaggio di avviso - La chiave privata contiene contenuto non PEM](#)

[Messaggio di avviso - Impossibile generare la chiave pubblica dalla chiave privata](#)

[Messaggio di avviso - errore di analisi: Impossibile decodificare i dati PEM](#)

[Messaggio di avviso - nessun certificato CA client/server](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritta la procedura per completare l'integrazione di Advanced Malware Protection (AMP) Virtual Private Cloud e Threat Grid Appliance. Nel documento viene descritto come risolvere i problemi relativi al processo di integrazione.

Contributo di Armando Garcia, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Funzionamento di AMP Virtual Private Cloud
- Funzionamento e funzionamento di Threat Grid Appliance

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

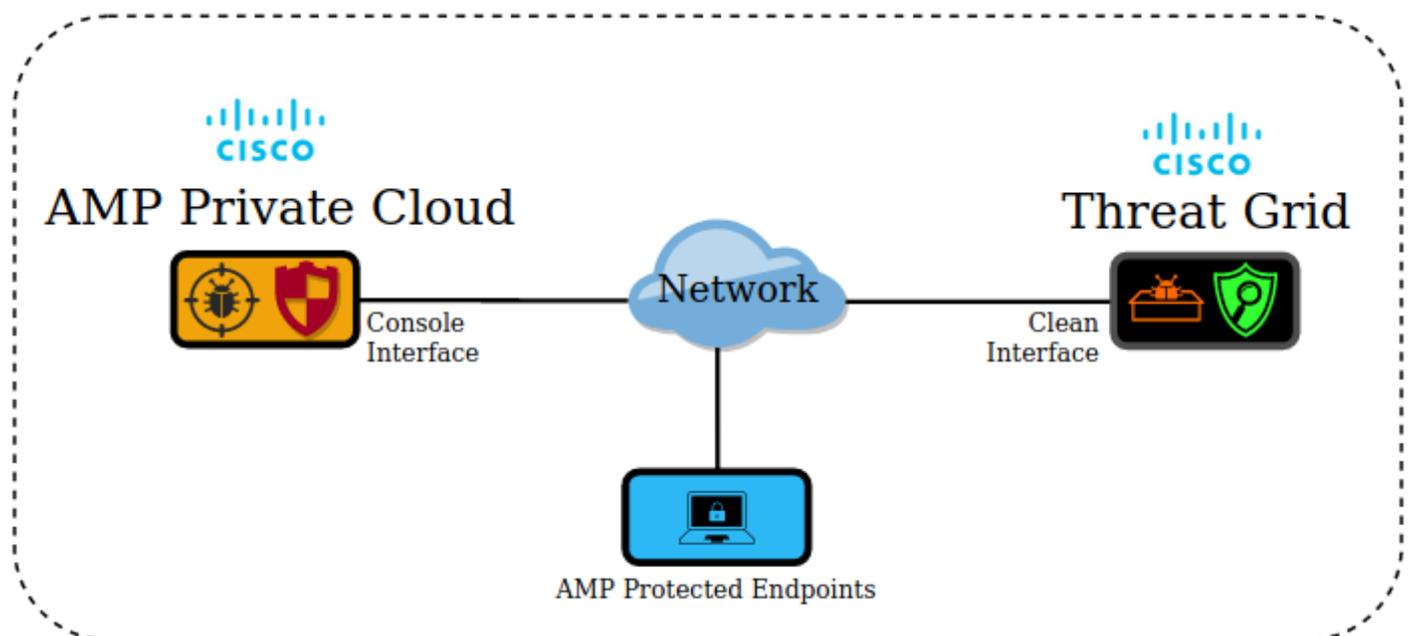
- AMP Private Cloud 3.2.0
- Appliance Threat Grid 2.12.0.1

Nota: La documentazione è valida per gli accessori Threat Grid e i dispositivi AMP Private Cloud nell'accessorio o nella versione virtuale.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Architettura dell'integrazione



Informazioni di base sull'integrazione

- L'appliance Threat Grid analizza gli esempi inviati dal dispositivo AMP Private Cloud.
- Gli esempi possono essere inviati manualmente o automaticamente all'accessorio Threat Grid.

- L'analisi automatica non è abilitata per impostazione predefinita nel dispositivo AMP Private Cloud.
- L'appliance Threat Grid fornisce al dispositivo AMP Private Cloud un report e un punteggio dall'analisi dell'esempio.
- L'accessorio Threat Grid comunica al dispositivo AMP Private Cloud qualsiasi campione con un punteggio maggiore o uguale a 95.
- Se il punteggio dell'analisi è maggiore o uguale a 95, il campione nel database AMP viene contrassegnato con una disposizione di dannoso.
- I rilevamenti retrospettivi vengono applicati da AMP Private Cloud a campioni con un punteggio maggiore o uguale a 95.

Procedura

Passaggio 1. Configurare e configurare l'appliance Threat Grid (non ancora integrata). Verificare la disponibilità di aggiornamenti e installarli, se necessario.

Passaggio 2. Configurare e configurare AMP for Endpoints Private Cloud (non ancora integrato).

Passaggio 3. Nell'interfaccia utente di amministrazione di Threat Grid, selezionare la scheda **Configuration** e scegliere **SSL**.

Passaggio 4. Generare o caricare un nuovo certificato SSL per l'interfaccia Clean (PANDEM).

Rigenerazione dei certificati SSL

È possibile generare un nuovo certificato autofirmato se il nome host dell'interfaccia pulita non corrisponde al nome alternativo del soggetto (SAN) nel certificato attualmente installato nell'accessorio per l'interfaccia pulita. L'accessorio genera un nuovo certificato per l'interfaccia, configurando il nome host dell'interfaccia corrente nel campo SAN del certificato autofirmato.

Passaggio 4.1. Dalla colonna Azioni selezionare (...) e dal menu a comparsa selezionare **Genera nuovo certificato**.

Passaggio 4.2. Nell'interfaccia utente di Threat Grid, selezionare **Operations**, nella schermata successiva selezionare **Activate** (Attiva) e scegliere **Reconfigure** (Riconfigura).

Nota: questo certificato generato è autofirmato.

Caricamento dei certificati SSL

Se è già stato creato un certificato per l'interfaccia di pulizia dell'accessorio Threat Grid, è possibile caricare il certificato nell'accessorio.

Passaggio 4.1. Dalla colonna Azioni selezionare (...) e dal menu a comparsa selezionare **Carica nuovo certificato**.

Passaggio 4.2. Copiare il certificato e la chiave privata corrispondente in formato PEM nelle

caselle di testo visualizzate sullo schermo e selezionare **Aggiungi certificato**.

Passaggio 4.3. Nell'interfaccia utente di Threat Grid, selezionare **Operations**, nella schermata successiva selezionare **Activate** (Attiva) e scegliere **Reconfigure** (Riconfigura).

Passaggio 5. Nell'interfaccia utente di amministrazione del dispositivo AMP Private Cloud, selezionare **Integrations** e scegliere **Threat Grid**.

Passaggio 6. In Dettagli configurazione griglia minacce, selezionare **Modifica**.

Passaggio 7. In Nome host griglia minacce immettere il nome di dominio completo (FQDN) dell'interfaccia pulita dell'accessorio Threat Grid.

Passaggio 8. Nel certificato SSL per la griglia delle minacce aggiungere il certificato dell'interfaccia pulita dell'accessorio Threat Grid. (Vedere le note seguenti)

Il certificato nell'interfaccia pulita dell'accessorio Threat Grid è autofirmato

Passaggio 8.1. Nell'interfaccia utente di amministrazione di Threat Grid, selezionare la **configurazione** e **scegliere SSL**.

Passaggio 8.2. Dalla colonna Azioni selezionare (...) e dal menu a comparsa selezionare **Scarica certificato**.

Passaggio 8.3. Continuare ad aggiungere il file scaricato al dispositivo VPN AMP nella pagina di integrazione di Threat Grid.

Il certificato nell'interfaccia pulita dell'accessorio Threat Grid è firmato da un'autorità di certificazione (CA) aziendale

Passaggio 8.1. Copiare in un file di testo il certificato dell'interfaccia di pulizia dell'accessorio Threat Grid e la catena di certificati CA completa.

Nota: I certificati nel file di testo devono essere in formato PEM.

Esempio

Se la catena di certificati completa è: certificato ROOT_CA > certificato Threat_Grid_Clean_Interface; quindi è necessario creare il file di testo, come mostrato nell'immagine.

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

Se la catena di certificati completa è: Certificato ROOT_CA > Certificato Sub_CA > Certificato Threat_Grid_Clean_Interface; quindi è necessario creare il file di testo, come mostrato nell'immagine.

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

Passaggio 9. In Chiave API Griglia minacce immettere la chiave API dell'utente Griglia minacce che verrà collegata agli esempi caricati.

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

Nota: Nelle impostazioni dell'account dell'utente Threat Grid, confermare che il parametro **Disable API Key** non è impostato su True.

Passaggio 10. Dopo aver completato tutte le modifiche, selezionare **Salva**.

Passaggio 11. Applicare una riconfigurazione al dispositivo cloud virtuale AMP.

Passaggio 12. Dall'interfaccia utente di amministrazione del dispositivo AMP Private Cloud, selezionare **Integrations** e scegliere **Threat Grid**.

Passaggio 13. In **Dettagli** copiare i valori dell'URL del servizio di aggiornamento dell'eliminazione, dell'utente del servizio di aggiornamento dell'eliminazione e della password del servizio di aggiornamento dell'eliminazione. Queste informazioni sono utilizzate nel passo 17.

Passaggio 14. Nell'interfaccia utente di amministrazione di Threat Grid, selezionare **Configuration** (Configurazione) e scegliere **CA Certificates (Certificati CA)**.

Passaggio 15. Selezionare **Add Certificate** e copiare in formato PEM il certificato CA che ha firmato il certificato del servizio di aggiornamento dell'eliminazione del cloud privato AMP.

Nota: Se il certificato CA che ha firmato il certificato AMP Private Cloud Disposition Update è una CA secondaria, ripetere il processo fino a quando tutte le CA della catena non vengono caricate nei **certificati CA**.

Passaggio 16. Nel portale Threat Grid, selezionare Amministrazione e selezionare Gestisci integrazione cloud privata AMP.

Passaggio 17. Nella pagina Servizio Syndication di aggiornamento della disposizione immettere le informazioni raccolte nel Passo 13.

- URL servizio: FQDN del servizio di aggiornamento della disposizione del dispositivo cloud privato AMP.
- Utente: utente del servizio di aggiornamento della disposizione del dispositivo cloud privato AMP.
- Password: password per il servizio di aggiornamento della disposizione del dispositivo cloud privato AMP.

A questo punto, se tutti i passaggi sono stati applicati correttamente, l'integrazione deve funzionare correttamente.

Verifica

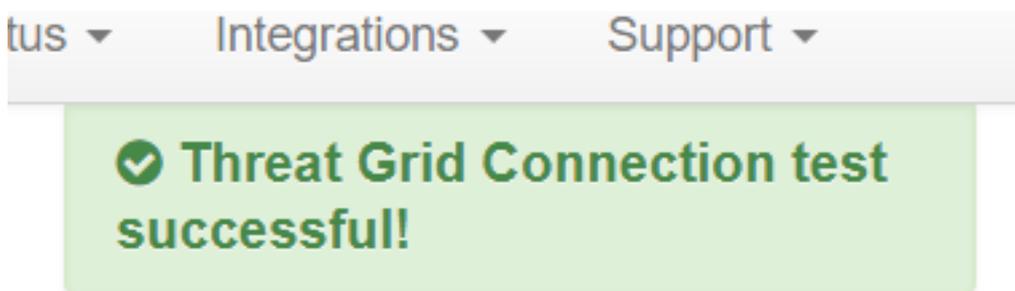
Di seguito viene riportata la procedura per verificare che l'accessorio Threat Grid sia stato integrato correttamente.

Nota: solo i passi 1, 2, 3 e 4 possono essere applicati in un ambiente di produzione per verificare l'integrazione. Il passo 5 viene fornito come informazione per ulteriori informazioni sull'integrazione e non è consigliabile applicarlo in un ambiente di produzione.

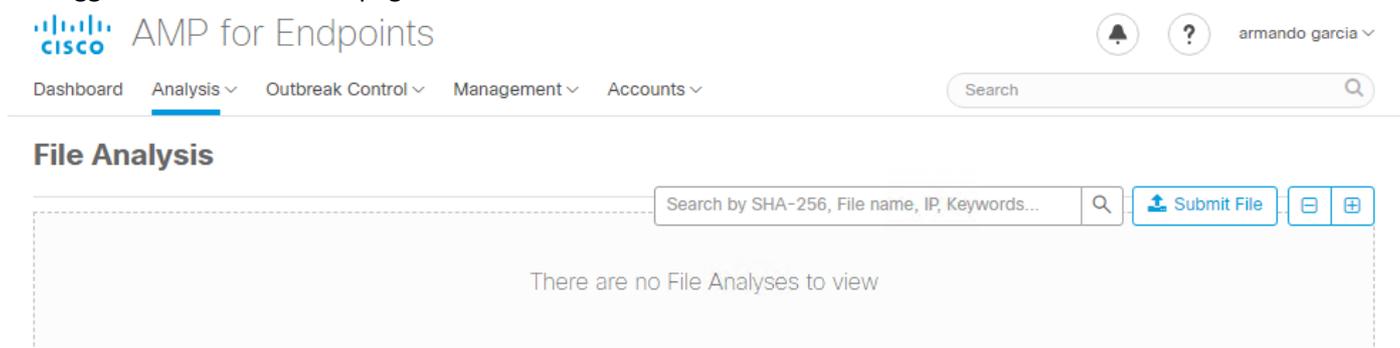
Passaggio 1. Selezionare Test Connection in AMP Private Cloud Device Admin UI > Integrations > Threat Grid e confermare il messaggio di test Threat Grid Connection riuscito. ricevuto.

Threat Grid Configuration Details Edit

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



Passaggio 2. Verificare che la pagina Web Analisi file nella console di AMP Private Cloud sia caricata senza errori.



Passaggio 3. Verificare che i file inviati manualmente da **Analisi** console cloud privato AMP > **Analisi file** vengano percepiti nell'accessorio Threat Grid e che venga restituito un report con un punteggio dall'accessorio Threat Grid.

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

Passaggio 4. Verificare che le CA che hanno firmato il certificato del servizio di aggiornamento dell'eliminazione del dispositivo cloud privato AMP siano installate nell'appliance Threat Grid in **Autorità di certificazione**.

Passaggio 5. Confermare che tutti i campioni contrassegnati dall'accessorio Threat Grid con un punteggio ≥ 95 vengano registrati nel database di AMP Private Cloud con la disposizione dei dati dannosi dopo il report e che il punteggio di esempio venga fornito da Threat Grid Appliance.

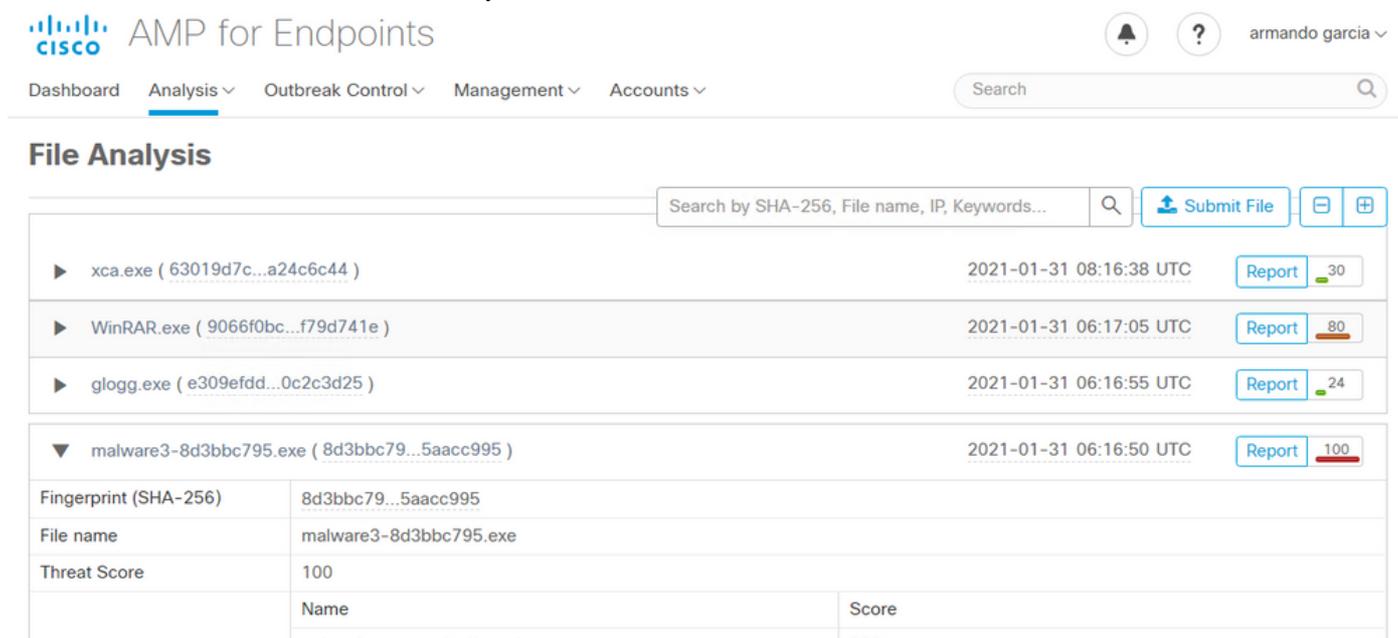
Nota: La ricezione di un report di esempio e di un punteggio di esempio ≥ 95 nella console AMP Private Cloud nella scheda **Analisi file** non significa necessariamente che la disposizione dei file sia stata modificata nel database AMP. Se le CA che hanno firmato il certificato del servizio di aggiornamento dell'eliminazione del dispositivo cloud privato AMP non sono installate nell'appliance Threat Grid in **Autorità di certificazione**, il dispositivo cloud privato AMP riceverà i report e i punteggi, ma l'appliance Threat Grid non riceverà alcun poke.

Avviso: Il test successivo è stato completato per attivare una modifica della disposizione del campione nel database AMP dopo che l'accessorio Threat Grid ha contrassegnato un file con un punteggio ≥ 95 . Lo scopo di questo test era quello di fornire informazioni sulle operazioni interne nel dispositivo cloud privato AMP quando l'appliance Threat Grid fornisce un punteggio di esempio ≥ 95 . Per attivare il processo di modifica dell'eliminazione, è stato creato un file di test di imitazione del malware con l'applicazione makemalware.exe interna di Cisco. Esempio: malware3-419d23483.exeSHA256: 8d3bbc795bb4747984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995.

Attenzione: Si sconsiglia di far esplodere qualsiasi file di test di imitazione del malware in un ambiente di produzione.

Conferma dell'aggiornamento della disposizione del campione nel database cloud privato AMP

Il file del malware di test è stato inviato manualmente all'appliance Threat Grid da **File Analysis** nella console AMP Private Cloud. Dopo l'analisi dell'esempio, l'appliance Threat Grid ha fornito un report di esempio e un punteggio di esempio di 100 al dispositivo AMP Private Cloud. Un punteggio di esempio ≥ 95 attiva una modifica della disposizione per il campione nel database dei dispositivi AMP Private Cloud. Questa modifica della disposizione del campione nel database AMP in base a un punteggio di esempio ≥ 95 fornito da Threat Grid è ciò che è noto come poke.



The screenshot displays the 'File Analysis' section of the Cisco AMP for Endpoints console. At the top, there is a navigation bar with 'AMP for Endpoints' and a user profile 'armando garcia'. Below the navigation bar, there is a search bar and a 'Submit File' button. The main content area shows a list of analyzed files with columns for file name, date, and threat score. The file 'malware3-8d3bbc795.exe' is highlighted with a score of 100. Below the list, a detailed view of this file is shown, including its fingerprint (SHA-256), file name, and threat score.

Name	Score
malware3-8d3bbc795.exe	100

Se:

- Integrazione completata.
- I report e i punteggi di esempio vengono percepiti in **Analisi file** dopo l'invio manuale dei file.

Quindi:

- Per ogni esempio contrassegnato con un punteggio ≥ 95 dall'accessorio Threat Grid, viene aggiunta una voce al file `/data/poked/poked.log` nel dispositivo AMP Private Cloud.
- Il `/data/poked/poked.log` viene creato nel dispositivo AMP Private Cloud dopo che il primo punteggio di esempio ≥ 95 è stato fornito dall'accessorio Threat Grid.
- Il database `db_protect` nel cloud privato AMP contiene la disposizione corrente per l'esempio. Queste informazioni possono essere utilizzate per verificare se il campione ha una disposizione di 3 dopo che l'accessorio Threat Grid ha fornito il punteggio.

Se il report di esempio e il punteggio ≥ 95 vengono percepiti in **File Analysis** nella console AMP Private Cloud, applicare i seguenti passaggi:

Passaggio 1. Accedere tramite SSH al dispositivo cloud privato AMP.

Passaggio 2. Verificare che sia presente una voce in `/data/poked/poked.log` per il campione.

L'elenco della directory /data/poked/ in un dispositivo cloud privato AMP che non ha mai ricevuto un punteggio di esempio >=95 da un accessorio Threat Grid indica che il file poked.log non è stato creato nel sistema.

Se il dispositivo AMP Private Cloud non ha mai ricevuto un poke da un accessorio Threat Grid, il file /data/poked/poked.log non viene trovato nella directory, come mostrato nell'immagine.

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

Se si elenca la directory /data/poked/ dopo aver ricevuto il primo punteggio di esempio >=95, il file viene creato.

Dopo aver ricevuto il primo campione con un punteggio >=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": "W32.80388C7958-100.SBX.TG", "ok": 1, "time": 1612031118, "hash": "8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995", "engine": "sha256", "user": "-", "mode": "tg", "score": 100}
[root@fireamp ~]#
```

Nel file poked.log è possibile percepire informazioni di esempio provenienti dal dispositivo Threat Grid.

Passaggio 3. **Eseguire** questo comando con l'esempio SHA256 per recuperare la disposizione corrente dal database del dispositivo AMP Private Cloud.

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

Esempio

Una query di database per ottenere la disposizione dell'esempio prima che l'esempio venga caricato in Threat Grid Appliance non restituisce alcun risultato, come mostrato nell'immagine.

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

Una query di database per ottenere la disposizione del campione dopo la ricezione del report e del punteggio dall'accessorio Threat Grid mostra il campione con una disposizione pari a 3, considerata dannosa.

```
[root@fireamp ~]# mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995;"
+-----+-----+
| hex(fingerprint) | disposition_id |
+-----+-----+
| 8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995 | 3 |
+-----+-----+
[root@fireamp ~]#
```

Risoluzione dei problemi

Nel processo di integrazione si possono percepire i problemi possibili. In questa parte del documento vengono affrontati alcuni dei problemi più comuni.

Avviso nel dispositivo cloud privato AMP: host non valido, certificato non testato,

chiave API non testata

Sintomo

Il messaggio di avviso: L'host Threat Grid non è valido, il certificato SSL Threat Grid non può essere verificato, la chiave API Threat Grid non può essere verificata, viene ricevuta nel dispositivo cloud privato AMP dopo la selezione del pulsante **Test connessione** 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.

A livello di rete esiste un problema di integrazione.

Fasi consigliate:

- Verificare che l'interfaccia della console del dispositivo AMP Private Cloud possa raggiungere l'interfaccia pulita dell'accessorio Threat Grid.
- Verificare che il dispositivo AMP Private Cloud sia in grado di risolvere il nome di dominio completo dell'interfaccia clean dell'appliance Threat Grid.
- Verificare che il percorso di rete del dispositivo AMP Private Cloud e dell'accessorio Threat Grid non contenga un dispositivo di filtraggio.

Avviso nel dispositivo cloud privato AMP relativo alla chiave API Threat Grid non valida

Sintomo

Il messaggio di avviso: Il test della connessione alla rete delle minacce non è riuscito, l'API della griglia delle minacce non è valida, viene ricevuta nel dispositivo cloud privato AMP dopo la selezione del pulsante **Test connessione** in **Integrations > Threat Grid**.

Connect Threat Grid Appliance to AMP for Endpoints Appliance

Threat Grid Connection test failed.

- Threat Grid API key is invalid.

Chiave API dell'appliance Threat Grid configurata nel cloud privato AMP.

Fasi consigliate:

- Verificare che nelle impostazioni dell'account dell'utente dell'accessorio Threat Grid il parametro Disable API Key non sia impostato su True.
 - Il parametro Disable API Key deve essere impostato su: False o Unset.

API

API Key *****  

Disable API Key  True False Unset

Can Download Sample Content Via API  True False Unset

- Verificare che la chiave API Threat Grid configurata nel portale di amministrazione di AMP Private Cloud **Integrations > Threat Grid** sia la stessa chiave API nelle impostazioni utente nell'accessorio Threat Grid.
- Verificare che la chiave API Threat Grid corretta sia stata salvata nel database dei dispositivi AMP Private Cloud.

Dalla riga di comando del dispositivo AMP Private Cloud, è possibile confermare la chiave API Threat Grid corrente configurata nel dispositivo AMP. Accedere al dispositivo AMP Private Cloud tramite SSH ed eseguire questo comando per recuperare la chiave API utente Threat Grid corrente:

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

Questa è una voce corretta nel database del dispositivo AMP Private Cloud per la chiave API dell'appliance 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] nnjae7 | argarci2_samples-user | de4c23c64d3e36034bb7 ||
+-----+-----+-----+
```

Anche se il nome utente Threat Grid non è stato configurato direttamente nel dispositivo cloud privato AMP in nessuna fase dell'integrazione, il nome utente Threat Grid viene percepito nel parametro `tg_login` nel database AMP se la chiave API Threat Grid è stata applicata correttamente.

Voce errata nel database AMP per la chiave 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 |
+-----+-----+-----+
```

Il parametro `tg_login` è NULL. Il nome utente Threat Grid non è stato recuperato dall'accessorio Threat Grid dal dispositivo AMP Private Cloud dopo l'applicazione della riconfigurazione.

I punteggi dei campioni ≥ 95 vengono ricevuti dal dispositivo AMP Private Cloud,

ma la disposizione del campione non cambia

Sintomo

Dopo l'invio di un campione, i report e i punteggi ≥ 95 vengono ricevuti correttamente dall'accessorio Threat Grid, ma il dispositivo AMP Private Cloud non rileva alcuna modifica nella disposizione del campione.

Fasi consigliate:

- Verificare nel dispositivo AMP Private Cloud se l'esempio SHA256 è presente nel contenuto di `/data/poked/poked.log`.

Se SHA256 è presente in `/data/poked/poked.log`, eseguire questo comando per confermare la disposizione del campione corrente nel database AMP.

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

- Verificare che la password corretta per l'integrazione con AMP Private Cloud sia stata aggiunta al portale di amministrazione dell'appliance Threat Grid in **Amministrazione > Gestisci integrazione con AMP Private Cloud**.

Portale di amministrazione AMP Private Cloud.

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	<code>https://dupdateamp3.argarci2-lab.com/</code>
User	<code>disposition_update_user</code>
Password	<code>ew236 [redacted] xJYfPK</code> Change Password

Portale della console dell'appliance Threat Grid.

Threat Grid Submit Sample Dashboard Samples Advanced Search Beta Reports Indicators Administration

Disposition Update Syndication Service

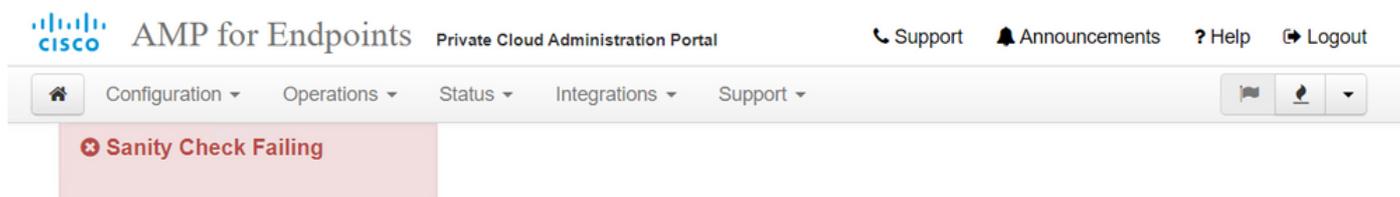
Service URL	User	Password	Action(s)
[redacted]	<code>disposition_update_user</code>	Edit Remove
[redacted]	<code>disposition_update_user</code>	Edit Remove
[redacted]	<code>disposition_update_user</code>	Edit Remove
[redacted]	<code>disposition_update_user</code>	Edit Remove
[redacted]	<code>disposition_update_user</code>	Edit Remove
<code>https://dupdateamp3.argarci2-lab.com/</code>	<code>disposition_update_user</code>	<code>ew236 [redacted] xJYfPK</code>	Save Cancel
[redacted]	<code>disposition_update_user</code>	Edit Remove

- Verificare che le CA che hanno firmato il certificato del servizio di aggiornamento dell'eliminazione del dispositivo del cloud privato AMP siano state installate nel portale di amministrazione dell'accessorio Threat Grid nei **certificati CA**.

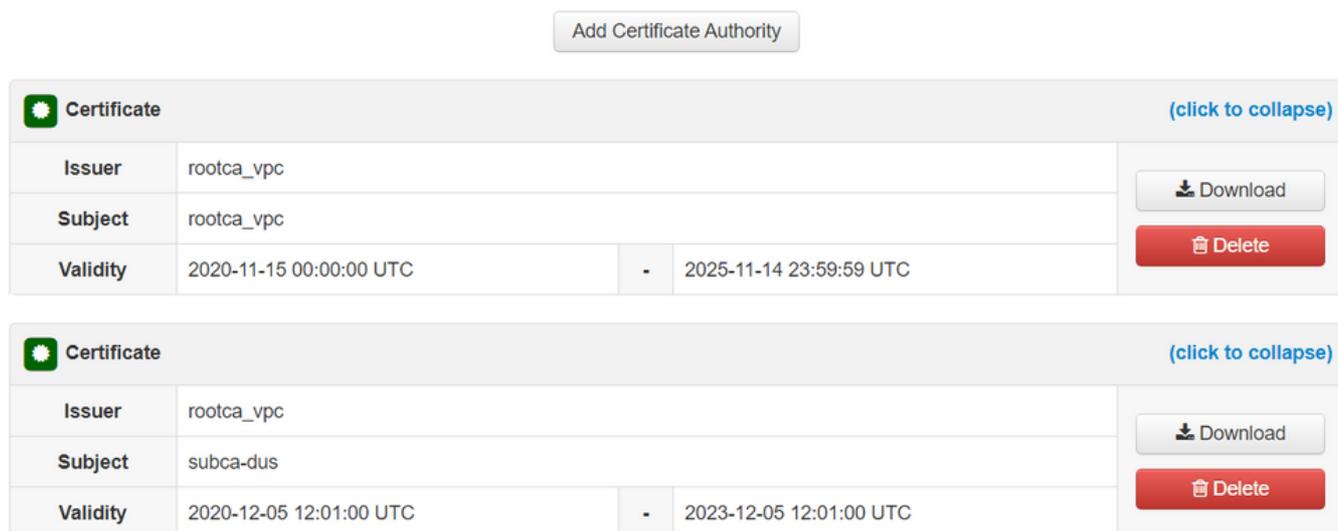
Nell'esempio seguente la catena di certificati per il certificato del servizio di aggiornamento della

disposizione del dispositivo del cloud privato AMP è **Root_CA > Sub_CA > Disposition_Update_Service certificate**; pertanto, RootCA e Sub_CA devono essere installati in **CA Certificates** in Threat Grid Appliance.

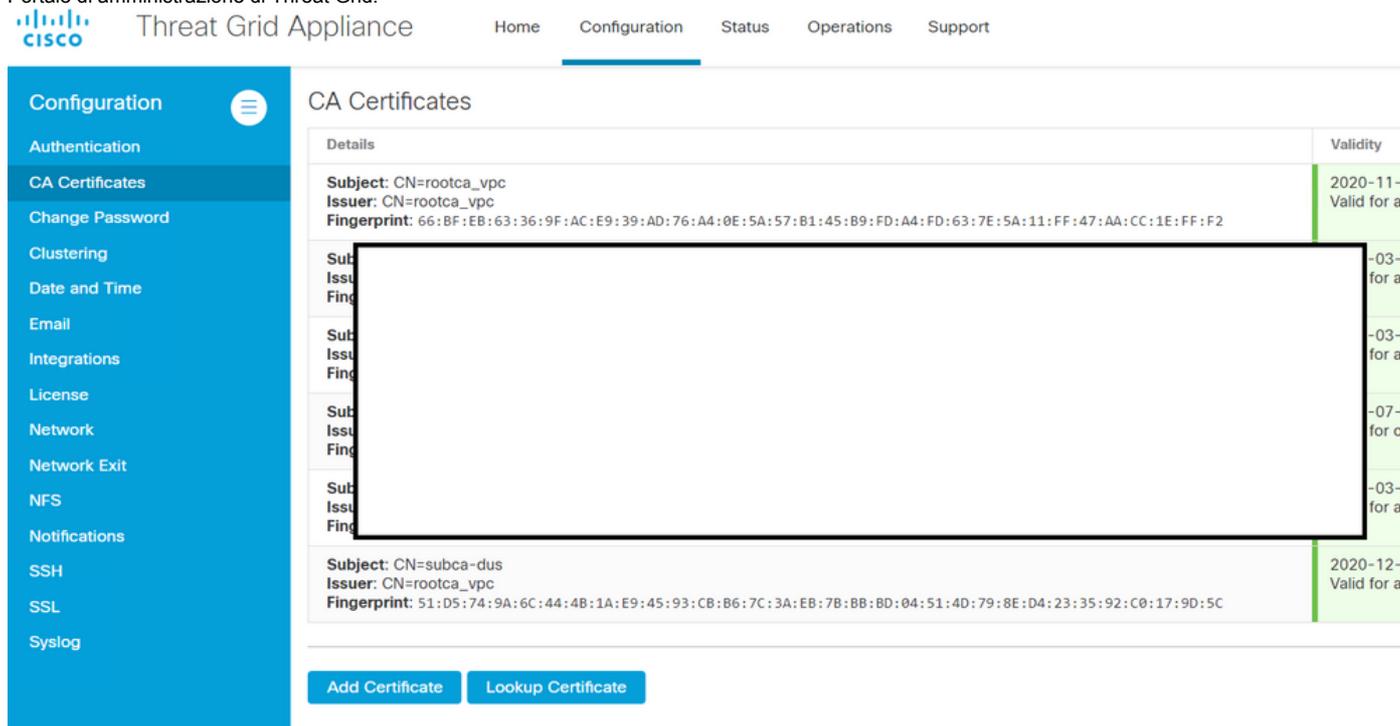
Autorità di certificazione nel portale di amministrazione AMP Private Cloud.



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



Portale di amministrazione di Threat Grid:



- Verificare che l'FQDN del servizio di aggiornamento della disposizione del dispositivo cloud privato AMP sia stato aggiunto correttamente al portale di amministrazione dell'appliance Threat Grid in **Amministrazione > Gestisci integrazione cloud privato AMP**. Verificare inoltre che l'indirizzo IP dell'interfaccia della console del

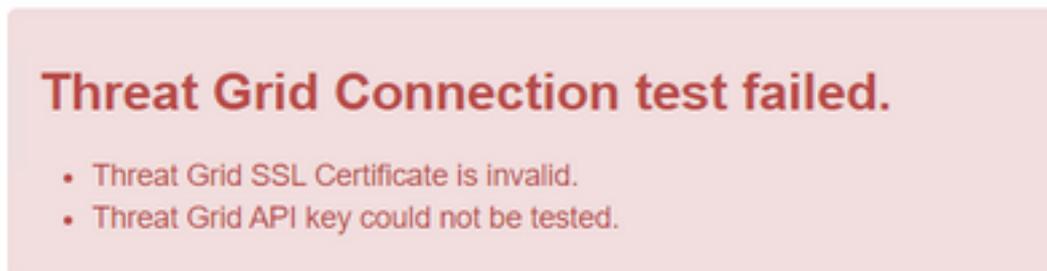
dispositivo AMP Private Cloud non sia stato aggiunto al posto dell'FQDN.

A screenshot of a configuration form. A red rectangular box highlights a text input field containing the URL "https://dupdateamp3.argarci2-lal:". To the right of this field are other input fields, one containing "ew236" and another containing "xJYfPK". There are also "Edit" and "Save" buttons visible on the right side of the form.

Avviso nel dispositivo cloud privato AMP relativo a un certificato SSL della griglia delle minacce non valido

Sintomo

Il messaggio di avviso: "Threat Grid SSL certificate is invalid", ricevuto nel dispositivo AMP Private Cloud dopo aver selezionato il pulsante **Test connessione** in **Integrations > Threat Grid**.



Fasi consigliate:

- Verificare che il certificato installato nell'interfaccia di pulizia dell'accessorio Threat Grid sia firmato da una CA aziendale.

Se è firmato da una CA, la catena di certificati completa deve essere aggiunta all'interno di un file al portale di amministrazione del dispositivo AMP Private Cloud **Integrations > Threat Grid** in **Threat Grid SSL Certificate**.

A screenshot of the "Threat Grid Configuration Details" page. The "Threat Grid SSL Certificate" section is highlighted with a red box. It shows the following details:

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

Other visible fields include "Hostname" (with a red box around the input) and "API Key" (with a search icon and an eye icon). There is an "Edit" button in the top right corner and a "Test Connection" button on the right side of the certificate section.

Nel dispositivo AMP Private Cloud i certificati attualmente installati dell'accessorio Threat Grid sono disponibili in: `/opt/fire/etc/ssl/threat_grid.crt`.

Avvisi relativi ai certificati nell'accessorio Threat Grid

Messaggio di avviso - La chiave pubblica derivata dalla chiave privata non corrisponde

Sintomo

Il messaggio di avviso: la chiave pubblica derivata dalla chiave privata non corrisponde. Viene ricevuta nell'accessorio Threat Grid dopo un tentativo di aggiungere un certificato a un'interfaccia.

The screenshot shows the Cisco Threat Grid Appliance configuration page for 'Upload SSL certificate for PANDEM'. The interface includes a navigation menu on the left 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' and contains two text input fields: 'Certificate (PEM)' and 'Private Key (PEM)'. Both fields contain long alphanumeric strings. Below the fields, a red error message states: 'public key derived from private key does not match'. At the bottom of the form, there are two buttons: 'Add Certificate' and 'Cancel'.

La chiave pubblica esportata dalla chiave privata non corrisponde alla chiave pubblica configurata nel certificato.

Fasi consigliate:

- Verificare che la chiave privata corrisponda alla chiave pubblica nel certificato.

Se la chiave privata corrisponde alla chiave pubblica nel certificato, il modulo e l'esponente pubblico devono essere uguali. Per questa analisi è sufficiente verificare se il modulo contiene lo stesso valore nella chiave privata e nella chiave pubblica nel certificato.

Passaggio 1. Utilizzare lo strumento OpenSSL per confrontare il modulo nella chiave privata e la chiave pubblica configurate nel certificato.

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

Esempio. Corrispondenza riuscita tra una chiave privata e una chiave pubblica configurate in un certificato.

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

Messaggio di avviso - La chiave privata contiene contenuto non PEM

Sintomo

Il messaggio di avviso: La chiave privata contiene contenuto non PEM e viene ricevuta nell'accessorio Threat Grid dopo un tentativo di aggiungere un certificato a un'interfaccia.

The screenshot shows the Threat Grid Appliance configuration page for uploading an SSL certificate for PANDEM. The interface includes a navigation menu on the left 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' and contains two text input fields. The first field, labeled 'Certificate (PEM)', contains a valid PEM certificate. The second field, labeled 'Private Key (PEM)', contains a private key with a red error message below it: 'private key contains non-PEM content'. At the bottom of the form are 'Add Certificate' and 'Cancel' buttons.

I dati PEM all'interno del file di chiave privata sono danneggiati.

Fasi consigliate:

- Confermare l'integrità dei dati all'interno della chiave privata.

Passaggio 1. Utilizzare lo strumento OpenSSL per verificare l'integrità della chiave privata.

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

Esempio. Eseguire l'output da una chiave privata con errori nei dati PEM all'interno del file e da un'altra chiave privata senza errori nel contenuto 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
```

Se l'output del comando OpenSSL non è **RSA Key ok**, significa che sono stati rilevati problemi con i dati PEM all'interno della chiave.

Se sono stati rilevati problemi con il comando OpenSSL:

- Verificare se nella chiave privata mancano i dati PEM.

I dati PEM all'interno del file di chiave privata vengono visualizzati in righe di 64 caratteri. Un rapido controllo dei dati PEM all'interno del file può mostrare se i dati mancano. La riga con i dati mancanti non è allineata alle altre righe nel file.

```
$ 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/xOazh
mdhzCQSTBfYbM
JqSwA5BEgqeH3
WtVHzbVDqJ+rb
SU+TvjNWQGcUs
4HA6/VsM10NHKT4EhvSks
tU9huSCL7t4BF7VpSeKXM
s7k0sCwmhKUaMacTYAnrg
17ttvLvX3zweLCEXSdXK6
r4M7HiocsbkLjijScTFYQ
rgd4kJ6ddAaSjQS7sJxaf
3gQDePpxacxGRZLXfja3s
a8y8ZQd0lqPZrV0Z6Mym2
i5S+/LS4jHB5hcCfnZpL4M0zHYvX+HPuGHm2xOCy51K5KsfDPa/SrbhDkxZty0SG
lCgVLEycQ5t1xtI6qiBLKNmtrQKBgQDKI+BTMrHFYD50gPcBZyGXVhmSyHcZOP9k
OosXngeKtpdqL8Ck/H2QftFpOAFoHQxD/tiJA6E1eK9HfVnsq9+xbCU1fRlPxeCS
CbcflDYBwaMn8Ywp9PfZKpgu/gI3XIUWT6T0LcBGtdspYDEbApvYA091PoS0vcBn
g7LG+bcJIQKBgHFn/ZziDtrkSzJSN6fVGPhJHCuTI+yZRuBkkz/8ohv1Rf+En+VY
9QG0GBq/MEBZy3TV+SUYfPX1SQ9eQDDYNQToKsfpUHQvuQ0JeIGSm+E6jFApNeg
QauT9x0TkVDP1bP5LFkTMG27Brzr9oG95F45hrZ0gW0D+w7YdTYlGD7ZAoGASHku
b4XoeNS1771hUg5w27qR9q+LC+8EmiHnRrNxDsnCzd7zGfQw7MKbQDdFQdfQUvyn
FBDKFsrLRT1rJVDGJe2ZNaE/QmE20AVNs7PG3UBYx/RxhYV/60smGGsXz10Mn+A0
SxuwKWoARshnMsDvsTYwofm1SMwTlMmCKpbTiiECgYBi8ZjgsdFv2NtYlmb1pAYS
DHierblDtVumF42Tax+fucqUrdb3LZo6FjagvPy+LBJA3VjtrYkDjQmstvxD5jfd
V3Pq4IwaocGU8RQUJY5L6rmw+y1s6Z+iNkIcPeZtWidSgP+NZa1xvhfj8XeL560o
a+IQn0Y41zLJ22ScgyFzEQ==
-----END PRIVATE KEY-----
```

- Confermare che la prima riga della chiave privata inizia con 5 trattini, le parole **BEGIN PRIVATE KEY** e termina con 5 trattini.

Esempio.

—BEGIN PRIVATE KEY—

- Confermare che l'ultima riga della chiave privata inizia con 5 trattini, le parole **END PRIVATE KEY** e termina con 5 trattini.

Esempio.

—END PRIVATE KEY—

Esempio. Correggere il formato PEM e i dati all'interno di una chiave privata.

```
$ 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
WXZW1XhNAgMBAA  tU9huSCL7t4BF7VpSeKXM
Uh4/Vrdg1TYXfB  s7k0sCwmhKUaMAcTYAnrg
fINIJto/x0azhe  47ttvLvX3zweLCEXsDXK6
mdhzCQSTBfYbM4  R4M7HiocsbkLjijScTFYQ
JqSwA5BEgqeH3a  hgd4kJ6ddAaSjQS7sJxaf
WtVHzbVDqJ+rb9  BgQDePpxacxGRZLXfja3s
SU+TvjNWQGcUsX  a8y8ZQd0lqPZrV0Z6Mym2
i5S+/LS4jHB5hcCfnZpL4M0zHYvX+HPuGHm2x0Cy51K5KsfdPa/SrbhDkxZty0SG
lCgVLEycQ5t1xtI6qiBLKNmtrQKBgQDKI+BTMrHFYD50gPcBZyGXVhmSyHcZOP9k
OosXngeKtpdqL8Ck/H2QftFp0AFoHQxD/tiJA6E1eK9HfVnsq9+xbCU1fRLPxeCS
CbcflDYBwaMn8Ywp9PfZKpgu/gI3XIUWT6T0LcBGtdspYDEbApvYA091PoS0vcBn
g7LG+bcJIQKBGHFn/ZziDtrkSzJSN6fVGPhJHCutI+yZRuBkkz/8ohv1Rf+En+VY
9QG0GBq/MEBZy3TV+SUYfPX1SQ9eQDDYNQToKsfpUh0QvuQ0JeIGSm+E6jFApNeg
QauT9x0TkVDP1bP5LFkTMG27Brzr9oG95F45hrZ0gWOD+w7YdTYlGD7ZAoGASHku
b4XoeNS1771hUg5w27qR9q+LC+8EmiHnRrNxDsnCZd7zGfQw7MKbQDdFQdfQUvyn
FBDKFsrLRT1rJVDGJe2ZNaE/QmE20AVNs7PG3UBYx/RxhYV/60smGGsXz10Mn+A0
SxuwKWoARshnMsDvsTYwofmlSMwTlMmCKpbTiiECgYBi8ZjgsdFv2NtYlmb1pAYS
DHierblDtVumF42Tax+fucqUrdB3LZo6FjagvPy+LbjA3VjtRYkDjQmstvxD5jfd
V3Pq4IwaocGU8RQUJY5L6rmw+y1s6Z+iNkIcPeZtWidSgP+NZa1xvhfj8XeL560o
a+IQn0Y41zLJ22ScgyFzEQ==
-----END PRIVATE KEY-----
```

Messaggio di avviso - Impossibile generare la chiave pubblica dalla chiave privata

Sintomo

Il messaggio di avviso: impossibile generare la chiave pubblica dalla chiave privata, viene ricevuto nell'accessorio Threat Grid dopo un tentativo di aggiungere un certificato a un'interfaccia.

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

Private Key (PEM)

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAACAQEAucb3AU15P91Ym/PvHva/xKBCbLeY7+jQJGO7wm7eruX3KTZY
EE9N6qn1+2YecCmOAA01sTqTQaHVVHJdCsczgz1mGalFI6Xinl8JI9i+n2NdlcNr
XBVPvCUs5fnH2cZwKGTen/NDJhnyC5Dlb17RLy7Y+wxhMiyRCHH3aZ3l0Mpl1k4X
[Redacted]
cjSc9W8Fy/CDXbX27KncS4qWe91phsKXq0jo7wIDAQABAoIBAFrH8EHRsvNTXY5v
yCSwXQtfalYpjXGGqdduaPzdlrICrCGWbbgimKeYQByGTU9v7vXAx2EAh57Izvb2
```

cannot generate public key from private key

Impossibile generare la chiave pubblica dai dati PEM correnti nel file di chiave privata.

Fasi consigliate:

- Confermare l'integrità dei dati all'interno della chiave privata.

Passaggio 1. Utilizzare lo strumento OpenSSL per verificare l'integrità della chiave privata.

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

Se l'output del comando OpenSSL non è **RSA Key ok**, significa che sono stati rilevati problemi con i dati PEM all'interno della chiave.

Passaggio 2. Utilizzare lo strumento OpenSSL per verificare se la chiave pubblica può essere esportata dalla chiave privata.

```
openssl rsa -in
```

Esempio. Esportazione della chiave pubblica non riuscita ed esportazione della chiave pubblica completata.

```
$ 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/iNa8vz9FiiTII0YS00dmNKKIEL
Lg080/TKGusV2CygqT+UESFerUEAzYh1KBxTUi5KKNB9Lm5A7RqPz1uHxPyTRmzC
FP3dQw7s8X4Bs3tL4s7U/Tq6Qm2ckD9q/rBswjiJNHNwBICv6WA02gr/xj+qxpB3
P1YjNTU711SFnSHC4E1Fzg3hy40yHCNqv7x/4j1niIAL9dGhrgQjnoFQ1DcDoD8m
N1yPIOx3C0lWeVForZmx+Dg61+J4uIjytkVceBw0v1bDnDRyk+BIb0pLF12VtV4
TQIDAQAB
-----END PUBLIC KEY-----
```

Messaggio di avviso - errore di analisi: Impossibile decodificare i dati PEM

Sintomo

Il messaggio di avviso: errore di analisi: Impossibile decodificare i dati PEM. Tali dati vengono ricevuti nell'accessorio Threat Grid dopo un tentativo di aggiungere un certificato a un'interfaccia.

The screenshot shows the Threat Grid Appliance configuration interface. The left sidebar lists various configuration options, with 'SSL' selected. 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 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, there are two buttons: 'Add Certificate' and 'Cancel'.

Impossibile decodificare il certificato dai dati PEM correnti all'interno del file di certificato. I dati PEM all'interno del file di certificato sono danneggiati.

- Verificare se è possibile recuperare le informazioni sul certificato dai dati PEM all'interno del file di certificato.

Passaggio 1. Utilizzare lo strumento OpenSSL per visualizzare le informazioni sul certificato dai dati PEM.

```
openssl x509 -in
```

Se i dati PEM sono danneggiati, viene rilevato un errore quando lo strumento OpenSSL tenta di caricare le informazioni sul certificato.

Esempio. Tentativo non riuscito di caricare le informazioni sul certificato a causa di dati PEM danneggiati nel file del certificato.

```
$ 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:
```

Messaggio di avviso - nessun certificato CA client/server

Sintomo

Il messaggio di avviso: errore di analisi: non è un certificato CA client/server, viene ricevuto nell'accessorio Threat Grid dopo un tentativo di aggiungere un certificato CA a **Configurazione > Certificati CA**.

The screenshot shows the Cisco Threat Grid Appliance web interface. The left sidebar contains a navigation menu with options 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 certificate text is partially visible, including the header '-----BEGIN CERTIFICATE-----' and the footer '-----END CERTIFICATE-----'. A red box highlights the error message 'not a client/server CA cert' below the certificate text. Below the error message are two buttons: 'Add Certificate' and 'Cancel'.

Il valore dell'estensione Limiti di base nel certificato CA non è definito come CA: Vero.

Verificare con lo strumento OpenSSL se il valore dell'estensione Basic Constraints è impostato su CA: True nel certificato CA.

Passaggio 1. Utilizzare lo strumento OpenSSL per visualizzare le informazioni sul certificato dai file di dati PEM.

```
openssl x509 -in
```

Passaggio 2. Cercare nelle informazioni sul certificato il valore corrente dell'estensione **Basic Constraints**.

Esempio. Valore del vincolo di base per una CA accettata dall'accessorio Threat Grid.

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

Informazioni correlate

- [Appliance Threat Grid - Guide alla configurazione](#)
- [Cisco AMP Virtual Private Cloud Appliance - Esempi di configurazione e note tecniche](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)