

Intégration du cloud privé virtuel AMP et de l'appliance Threat Grid

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Architecture de l'intégration](#)

[Informations de base sur l'intégration](#)

[Procédure](#)

[Régénération des certificats SSL](#)

[Téléchargement des certificats SSL](#)

[Le certificat de l'interface propre de l'appliance Threat Grid est auto-signé](#)

[Le certificat de l'interface de nettoyage de l'appliance Threat Grid est signé par une autorité de certification d'entreprise.](#)

[Exemple](#)

[Vérification](#)

[Confirmation de la mise à jour de disposition d'échantillon dans la base de données de cloud privé AMP](#)

[Exemple](#)

[Dépannage](#)

[Avertissement dans le périphérique de cloud privé AMP concernant un hôte non valide, un certificat non testé, une clé API non testée](#)

[Avertissement dans le périphérique de cloud privé AMP concernant une clé d'API Threat Grid non valide](#)

[Les scores d'échantillon \$\geq 95\$ sont reçus par le périphérique de cloud privé AMP, mais aucun changement n'est perçu dans la disposition de l'échantillon](#)

[Avertissement dans le périphérique de cloud privé AMP concernant un certificat SSL Threat Grid non valide](#)

[Avertissements dans l'appliance Threat Grid relatifs aux certificats](#)

[Message d'avertissement : la clé publique dérivée de la clé privée ne correspond pas](#)

[Message d'avertissement : la clé privée contient du contenu non PEM](#)

[Message d'avertissement - Impossible de générer la clé publique à partir de la clé privée](#)

[Message d'avertissement - erreur d'analyse : Impossible de décoder les données PEM](#)

[Message d'avertissement - pas un certificat CA client/serveur](#)

[Informations connexes](#)

Introduction

Ce document décrit la procédure à suivre pour terminer l'intégration du cloud privé virtuel AMP (Advanced Malware Protection) et de l'appliance Threat Grid. Le document fournit également des étapes de dépannage pour les problèmes liés au processus d'intégration.

Contribué par Armando Garcia, ingénieur TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Travailler et exploiter le cloud privé virtuel AMP
- Travailler et exploiter l'appliance Threat Grid

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

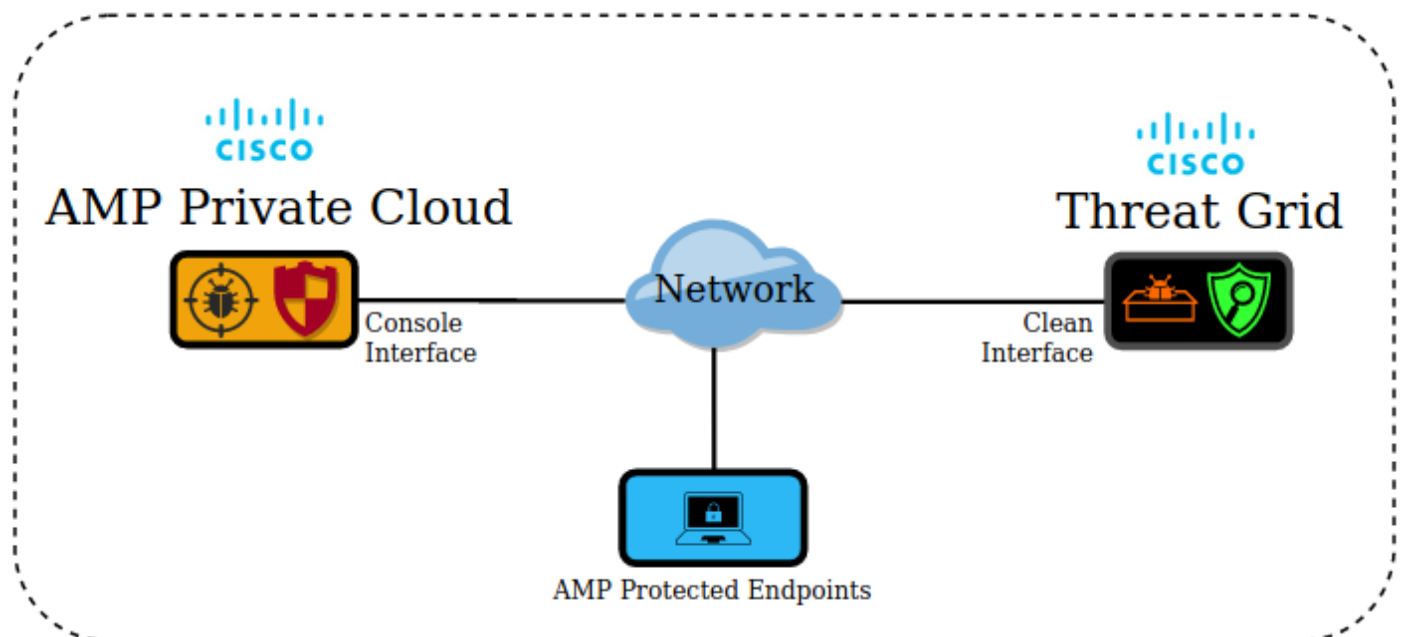
- Cloud privé AMP 3.2.0
- Appliance Threat Grid 2.12.0.1

Note: La documentation est valide pour les appliances Threat Grid et les périphériques de cloud privé AMP dans l'appliance ou la version virtuelle.

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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Architecture de l'intégration



Informations de base sur l'intégration

- L'appliance Threat Grid analyse les échantillons soumis par le périphérique de cloud privé

AMP.

- Les échantillons peuvent être envoyés manuellement ou automatiquement à l'appliance Threat Grid.
- L'analyse automatique n'est pas activée par défaut sur le périphérique de cloud privé AMP.
- L'appliance Threat Grid fournit au périphérique de cloud privé AMP un rapport et un score tirés de l'analyse de l'échantillon.
- L'appliance Threat Grid informe (poke) le périphérique de cloud privé AMP de tout échantillon ayant un score supérieur ou égal à 95.
- Si le score de l'analyse est supérieur ou égal à 95, l'exemple de la base de données AMP est marqué avec une disposition de malveillance.
- Les détections rétrospectives sont appliquées par le cloud privé AMP aux échantillons dont le score est supérieur ou égal à 95.

Procédure

Étape 1 : configuration et configuration de l'appliance Threat Grid (pas encore d'intégration)
Vérifiez les mises à jour et installez, si nécessaire.

Étape 2. Configurez et configurez le cloud privé AMP for Endpoints (pas encore d'intégration).

Étape 3. Dans l'interface d'administration de Threat Grid, sélectionnez l'onglet **Configuration** et choisissez **SSL**.

Étape 4. Générer ou télécharger un nouveau certificat SSL pour l'interface Clean (PANDEM).

Régénération des certificats SSL

Un nouveau certificat auto-signé peut être généré si le nom d'hôte de l'interface propre ne correspond pas au nom de remplacement d'objet (SAN) du certificat actuellement installé dans l'appliance pour l'interface propre. L'appliance génère un nouveau certificat pour l'interface, en configurant le nom d'hôte de l'interface actuelle dans le champ SAN du certificat auto-signé.

Étape 4.1. Dans la colonne Actions, sélectionnez (...) et dans le menu contextuel, sélectionnez **Générer un nouveau certificat**.

Étape 4.2. Dans l'interface de Threat Grid, sélectionnez **Operations**, dans l'écran suivant, sélectionnez **Activate** et **Reconfigure**.

Remarque : ce certificat généré est auto-signé.

Téléchargement des certificats SSL

Si un certificat a déjà été créé pour l'interface de nettoyage de l'appliance Threat Grid, ce certificat peut être téléchargé vers l'appliance.

Étape 4.1. Dans la colonne Actions, sélectionnez (...) et dans le menu contextuel, sélectionnez **Télécharger un nouveau certificat**.

Étape 4.2. Copiez le certificat et la clé privée correspondante au format PEM dans les zones de texte qui s'affichent à l'écran et sélectionnez **Ajouter un certificat**.

Étape 4.3. Dans l'interface de Threat Grid, sélectionnez **Operations**, dans l'écran suivant, sélectionnez **Activate** et **Reconfigure**.

Étape 5. Dans l'interface d'administration du périphérique de cloud privé AMP, sélectionnez **Intégrations** et choisissez **Threat Grid**.

Étape 6. Dans Threat Grid Configuration Details, sélectionnez **Edit**.

Étape 7. Dans Threat Grid Hostname, saisissez le nom de domaine complet de l'interface propre de l'appliance Threat Grid.

Étape 8. Dans le certificat SSL Threat Grid, ajoutez le certificat de l'interface propre de l'appliance Threat Grid. (Voir les notes ci-dessous)

Le certificat de l'interface propre de l'appliance Threat Grid est auto-signé

Étape 8.1. Dans l'interface d'administration de Threat Grid, sélectionnez la **configuration** et choisissez **SSL**.

Étape 8.2. Dans la colonne Actions, sélectionnez (...) et dans le menu contextuel, sélectionnez **Télécharger le certificat**.

Étape 8.3. Ajoutez le fichier téléchargé au périphérique privé virtuel AMP dans la page d'intégration de Threat Grid.

Le certificat de l'interface de nettoyage de l'appliance Threat Grid est signé par une autorité de certification d'entreprise.

Étape 8.1. Copiez dans un fichier texte le certificat de l'interface de nettoyage de l'appliance Threat Grid et la chaîne de certificats CA complète.

Note: Les certificats du fichier texte doivent être au format PEM.

Exemple

Si la chaîne de certificats complète est : certificat ROOT_CA > certificat Threat_Grid_Clean_Interface ; ensuite, le fichier texte doit être créé, comme le montre l'image.



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


Si la chaîne de certificats complète est : Certificat ROOT_CA > Certificat Sub_CA > Certificat Threat_Grid_Clean_Interface ; ensuite, le fichier texte doit être créé, comme le montre l'image.

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

Étape 9. Dans Threat Grid API Key, saisissez la clé API de l'utilisateur Threat Grid qui sera liée aux échantillons téléchargés.

API

API Key *****  

Disable API Key  True False Unset

Can Download Sample Content Via API  True False Unset

Note: Dans les paramètres de compte de l'utilisateur Threat Grid, vérifiez que le paramètre

Disable API Key n'a pas la valeur True.

Étape 10. Une fois toutes les modifications effectuées, sélectionnez **Enregistrer**.

Étape 11. Appliquez une reconfiguration au périphérique de cloud virtuel AMP.

Étape 12. Dans l'interface d'administration du périphérique de cloud privé AMP, sélectionnez **Intégrations** et choisissez **Threat Grid**.

Étape 13. Dans **Details**, copiez les valeurs de l'URL du service de mise à jour de disposition, de l'utilisateur du service de mise à jour de disposition et du mot de passe du service de mise à jour de disposition. Ces informations sont utilisées à l'étape 17.

Étape 14. Dans l'interface d'administration de Threat Grid, sélectionnez **Configuration** et choisissez **Certificats CA**.

Étape 15. Sélectionnez **Ajouter un certificat** et copiez au format PEM le certificat CA qui a signé le certificat AMP Private Cloud Disposition Update Service.

Note: Si le certificat de l'autorité de certification qui a signé le certificat de mise à jour AMP Private Cloud Disposition Update est une sous-autorité de certification, répétez le processus jusqu'à ce que toutes les autorités de certification de la chaîne soient téléchargées vers les **certificats de l'autorité de certification**.

Étape 16. Dans le portail Threat Grid, sélectionnez Administration et sélectionnez Manage AMP Private Cloud Integration.

Étape 17. Dans la page Disposition Update Syndication Service, saisissez les informations collectées à l'étape 13.

- URL du service : nom de domaine complet du service de mise à jour de la disposition du périphérique de cloud privé AMP.
- Utilisateur : utilisateur du service de mise à jour de la disposition du périphérique de cloud privé AMP.
- Mot de passe : mot de passe du service de mise à jour de disposition du périphérique de cloud privé AMP.

À ce stade, si toutes les étapes ont été correctement appliquées, l'intégration doit fonctionner correctement.

Vérification

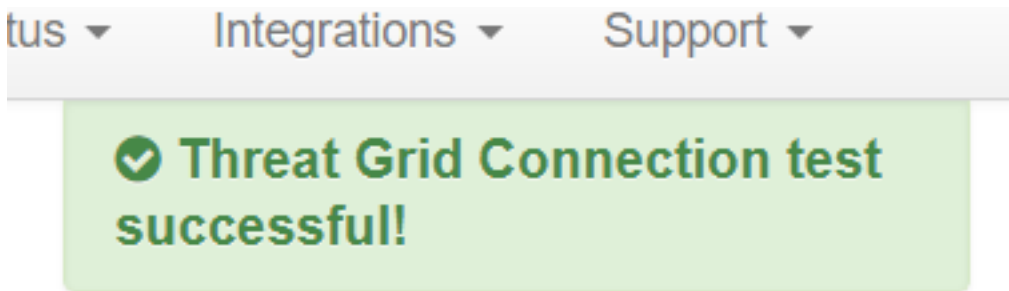
Voici les étapes à suivre pour confirmer que l'appliance Threat Grid a été correctement intégrée.

Remarque : seules les étapes 1, 2, 3 et 4 peuvent être appliquées dans un environnement de production pour vérifier l'intégration. L'étape 5 est fournie à titre d'information pour en savoir plus sur l'intégration et il n'est pas recommandé de l'appliquer dans un environnement de production.

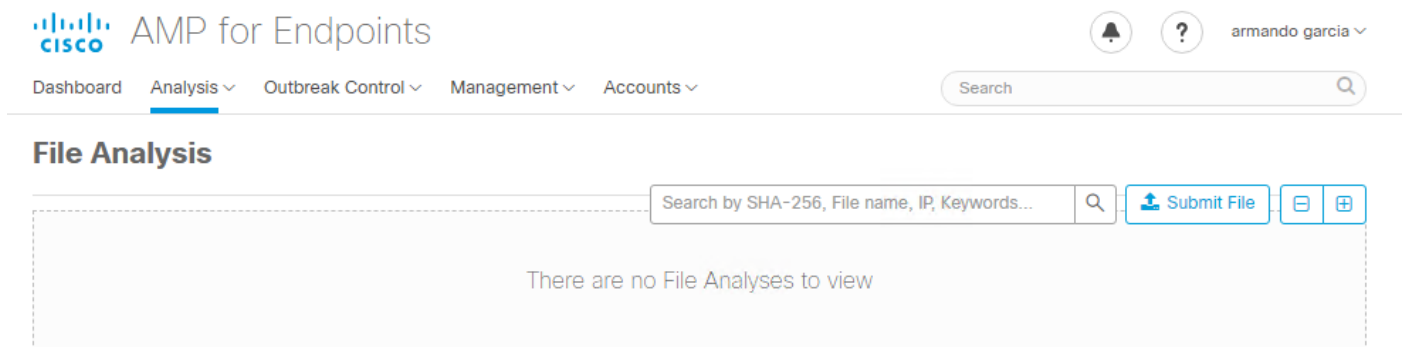
Étape 1. Sélectionnez Tester la connexion dans l'interface utilisateur d'administration des périphériques de cloud privé AMP > Intégrations > Threat Grid, et confirmez que le test de Threat Grid Connection a réussi ! est reçu.

Threat Grid Configuration Details Edit

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



Étape 2. Confirmez que la page Web Analyse de fichiers de la console de cloud privé AMP est chargée sans erreur.



Étape 3. Vérifiez que les fichiers envoyés manuellement à partir de la console de cloud privé AMP **Analysis > File Analysis** sont perçus dans l'appliance Threat Grid et qu'un rapport avec un score est retourné par l'appliance 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
-----------------------------------	-------------------------	-----------

Étape 4. Confirmez que les autorités de certification qui ont signé le certificat de service de mise à jour de la disposition du périphérique de cloud privé AMP sont installées dans l'appliance Threat Grid dans les **autorités de certification**.

Étape 5. Confirmez que tout échantillon marqué par l'appliance Threat Grid avec un score ≥ 95 est enregistré dans la base de données du cloud privé AMP avec la disposition des malwares après le rapport et l'exemple de score est fourni par l'appliance Threat Grid.

Note: Une réception réussie d'un exemple de rapport et un score d'exemple ≥ 95 dans la console de cloud privé AMP sous l'onglet **Analyse de fichiers**, ne signifie pas nécessairement que la disposition du fichier a été modifiée dans la base de données AMP. Si les autorités de certification qui ont signé le certificat de service de mise à jour de la disposition du périphérique de cloud privé AMP ne sont pas installées dans l'appliance Threat Grid dans les **autorités de certification**, les rapports et les scores sont reçus par le périphérique de cloud privé AMP, mais aucun test n'est reçu de l'appliance Threat Grid.

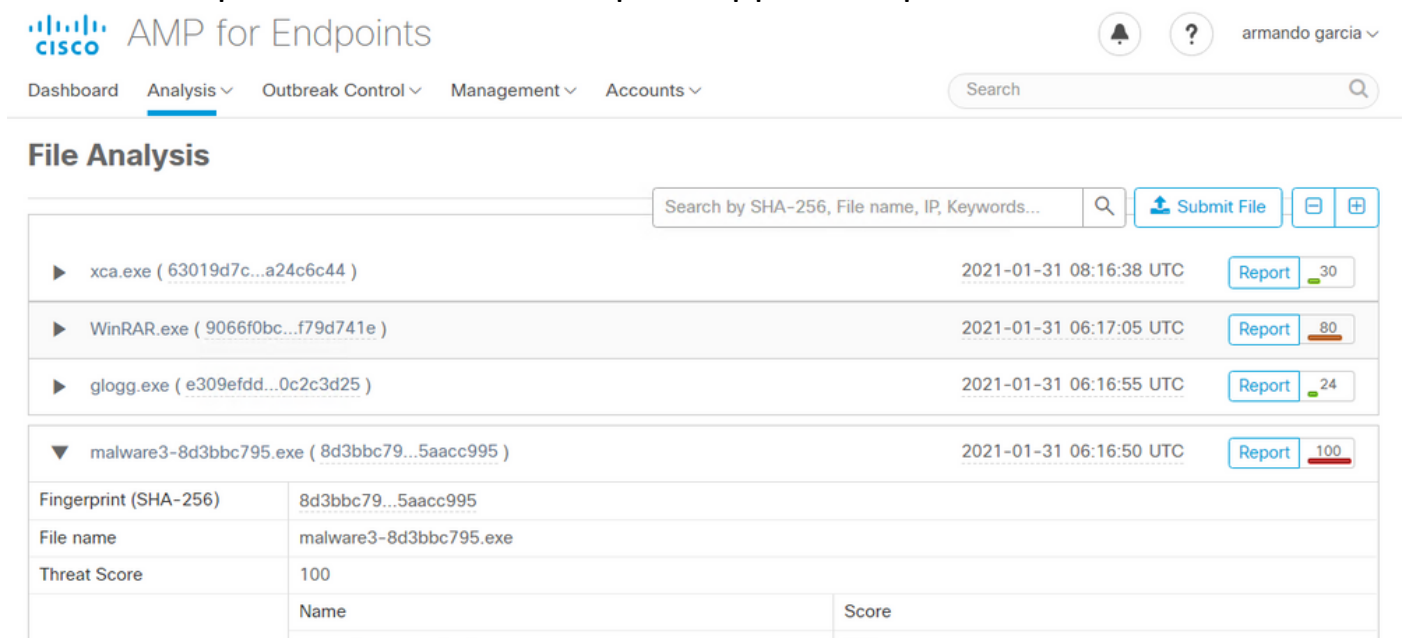
Avertissement : Le test suivant a été effectué pour déclencher un exemple de modification de disposition dans la base de données AMP après que l'appliance Threat Grid a marqué un fichier avec un score ≥ 95 . L'objectif de ce test était de fournir des informations sur les opérations internes dans le périphérique de cloud privé AMP lorsque l'appliance Threat Grid fournit un exemple de score de ≥ 95 . Afin de déclencher le processus de modification de disposition, un fichier de test d'imitation de programmes malveillants a été créé avec l'application interne makemalware.exe de Cisco. Exemple : malware3-419d23483.exeSHA256 : 8d3bbc795bb4747984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995.

Attention : Il est déconseillé de déclencher un fichier de test d'imitation de programmes

malveillants dans un environnement de production.

Confirmation de la mise à jour de disposition d'échantillon dans la base de données de cloud privé AMP

Le fichier de test des programmes malveillants a été envoyé manuellement à l'apppliance Threat Grid à partir de l'**analyse de fichiers** dans la console de cloud privé AMP. Après l'analyse de l'échantillon, un exemple de rapport et un exemple de score de 100 ont été fournis au périphérique de cloud privé AMP par l'apppliance Threat Grid. Un exemple de score ≥ 95 déclenche une modification de disposition pour l'exemple dans la base de données des périphériques de cloud privé AMP. Cette modification de la disposition de l'échantillon dans la base de données AMP basée sur un score d'échantillon ≥ 95 fourni par Threat Grid est ce qu'on appelle un poke.



The screenshot displays the 'File Analysis' section of the Cisco AMP for Endpoints console. It features a search bar at the top and a list of analyzed files. The file 'malware3-8d3bbc795.exe' is highlighted, showing a threat 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

Si :

- L'intégration s'est terminée correctement.
- Des exemples de rapports et de scores sont perçus dans l'**analyse des fichiers** après l'envoi manuel des fichiers.

Puis :

- Pour chaque exemple marqué par l'apppliance Threat Grid avec un score ≥ 95 , une entrée est ajoutée au fichier /data/poked/poked.log dans le périphérique de cloud privé AMP.
- Le fichier /data/poked/poked.log est créé dans le périphérique de cloud privé AMP après que le premier exemple de score ≥ 95 a été fourni par l'apppliance Threat Grid.
- La base de données db_Protect du cloud privé AMP contient la disposition actuelle de l'exemple. Cette information peut être utilisée pour confirmer si l'échantillon a une disposition de 3 après que l'apppliance Threat Grid a fourni le score.

Si l'exemple de rapport et le score ≥ 95 sont perçus dans l'**analyse de fichiers** dans la console de cloud privé AMP, appliquez ces étapes :

Étape 1. Connectez-vous via SSH au périphérique de cloud privé AMP.

Étape 2. Confirmez qu'une entrée de l'exemple est disponible dans /data/poked/poked.log.

La liste du répertoire /data/poked/ dans un périphérique de cloud privé AMP qui n'a jamais reçu un exemple de score ≥ 95 d'un appareil Threat Grid indique que le fichier poked.log n'a pas été créé dans le système.

Si le périphérique de cloud privé AMP n'a jamais reçu de requête ping d'une appliance Threat Grid, le fichier /data/poked/poked.log est introuvable dans le répertoire, comme l'illustre l'image.

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

La liste du répertoire /data/poked/ après la réception du premier score d'échantillon ≥ 95 indique que le fichier a été créé.

Après avoir reçu le premier échantillon avec un score ≥ 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.S8X.TG","ok":1,"time":1612031118,"hash":"8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995","engine":"sha256",
"user":"-", "mode":"tg", "score":100}
[root@fireamp ~]#
```

Des exemples d'informations provenant du segment fourni par l'appliance Threat Grid peuvent être perçus dans le fichier poked.log.

Étape 3. **Exécutez** cette commande avec l'exemple SHA256 pour extraire la disposition actuelle de la base de données du périphérique de cloud privé AMP.

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

Exemple

Une requête de base de données permettant d'obtenir la disposition de l'exemple avant le téléchargement de l'échantillon sur l'appliance Threat Grid ne fournit aucun résultat, comme l'illustre l'image.

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

Une requête de base de données pour obtenir l'exemple de disposition après la réception du rapport et du score de l'appliance Threat Grid, montre l'exemple avec une disposition de 3 qui est considérée comme malveillante.

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

Dépannage

Dans le processus d'intégration, les problèmes possibles peuvent être perçus. Dans cette partie du document, certaines des questions les plus courantes sont abordées.

Avertissement dans le périphérique de cloud privé AMP concernant un hôte non valide, un certificat non testé, une clé API non testée

Symptôme

Message d'avertissement : L'hôte Threat Grid n'est pas valide, le certificat SSL Threat Grid n'a pas pu être testé, la clé API Threat Grid n'a pas pu être testée, est reçue dans le périphérique de cloud privé AMP après avoir sélectionné le bouton **Test Connection** dans **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.

Il y a un problème au niveau du réseau dans l'intégration.

Étapes recommandées :

- Confirmez que l'interface de console du périphérique de cloud privé AMP peut atteindre l'interface propre de l'appliance Threat Grid.
- Confirmez que le périphérique de cloud privé AMP peut résoudre le nom de domaine complet de l'interface propre de l'appliance Threat Grid.
- Vérifiez qu'il n'existe pas de périphérique de filtrage dans le chemin d'accès réseau du périphérique de cloud privé AMP et de l'appliance Threat Grid.

Avertissement dans le périphérique de cloud privé AMP concernant une clé d'API Threat Grid non valide

Symptôme

Message d'avertissement : Échec du test de connexion à Threat Grid, l'API Threat Grid n'est pas valide, est reçue dans le périphérique de cloud privé AMP après avoir sélectionné le bouton **Test Connection** dans **Integrations > Threat Grid**.

Connect Threat Grid Appliance to AMP for Endpoints Appliance

Threat Grid Connection test failed.

- Threat Grid API key is invalid.

Clé d'API de l'appliance Threat Grid configurée dans le cloud privé AMP.

Étapes recommandées :

- Confirmez que dans les paramètres de compte de l'utilisateur de l'appliance Threat Grid, le

paramètre Disable API Key n'a pas la valeur True.

- Le paramètre Disable API Key doit être défini sur : False ou Unset.

API

API Key *****

Disable API Key True False Unset

Can Download Sample Content Via API True False Unset

- Confirmez que la clé d'API Threat Grid configurée dans le portail d'administration du cloud privé AMP **Integrations > Threat Grid**, est la même clé d'API dans les paramètres utilisateur de l'appliance Threat Grid.
- Vérifiez si la clé d'API Threat Grid correcte est enregistrée dans la base de données des périphériques de cloud privé AMP.

À partir de la ligne de commande du périphérique de cloud privé AMP, vous pouvez confirmer la clé d'API Threat Grid actuelle configurée dans le périphérique AMP. Connectez-vous au périphérique de cloud privé AMP via SSH et exécutez cette commande pour récupérer la clé d'API utilisateur Threat Grid actuelle :

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

Il s'agit d'une entrée correcte dans la base de données du périphérique de cloud privé AMP pour la clé API de l'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] | argarci2_samples-user | de4c23c64d3e36034bb7 ||
+-----+-----+-----+
```

Même si le nom d'utilisateur Threat Grid n'a pas été configuré directement dans le périphérique de cloud privé AMP à une étape quelconque de l'intégration, le nom d'utilisateur Threat Grid est perçu dans le paramètre tg_login de la base de données AMP si la clé API Threat Grid a été correctement appliquée.

Il s'agit d'une entrée erronée dans la base de données AMP pour la clé 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 |
+-----+-----+-----+
```

Le paramètre tg_login est NULL. Le nom d'utilisateur Threat Grid n'a pas été récupéré de l'appliance Threat Grid par le périphérique de cloud privé AMP après l'application de la reconfiguration.

Les scores d'échantillon >=95 sont reçus par le périphérique de cloud privé AMP, mais aucun changement n'est perçu dans la disposition de l'échantillon

Symptôme

Les rapports et >=95 scores d'exemple sont reçus avec succès de l'appliance Threat Grid après l'envoi d'un échantillon, mais aucun changement dans la disposition de l'échantillon n'est perçu dans le périphérique de cloud privé AMP.

Étapes recommandées :

- Confirmez dans le périphérique de cloud privé AMP si l'exemple SHA256 se trouve dans le contenu de /data/poked/poked.log.

Si le SHA256 se trouve dans /data/poked/poked.log, exécutez cette commande pour confirmer la disposition de l'exemple actuel dans la base de données AMP.

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

- Confirmez que le mot de passe d'intégration du cloud privé AMP correct a été ajouté au portail d'administration de l'appliance Threat Grid dans **Administration > Manage AMP Private Cloud Integration**.

Portail d'administration du cloud privé 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]xJYfPK"/> <input type="button" value="Change Password"/>

Portail de console de l'appliance Threat Grid.

Threat Grid Dashboard Samples **Advanced Search** Reports Indicators Administration ▾

Disposition Update Syndication Service

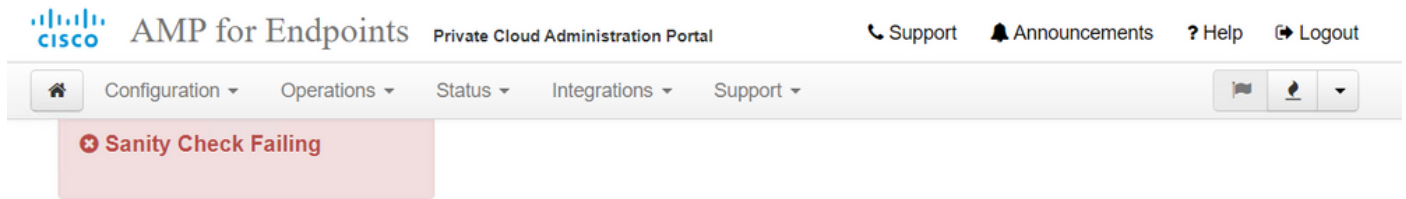
Service URL	User	Password	Action(s)
<input type="text" value="https://dupdateamp3.argarci2-lab.com/"/>	disposition_update_user	<input type="button" value="Edit"/> <input type="button" value="Remove"/>
	disposition_update_user	<input type="button" value="Edit"/> <input type="button" value="Remove"/>
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

- Confirmez que les autorités de certification qui ont signé le certificat de service de mise à jour de la disposition des périphériques de cloud privé AMP ont été installées dans le portail

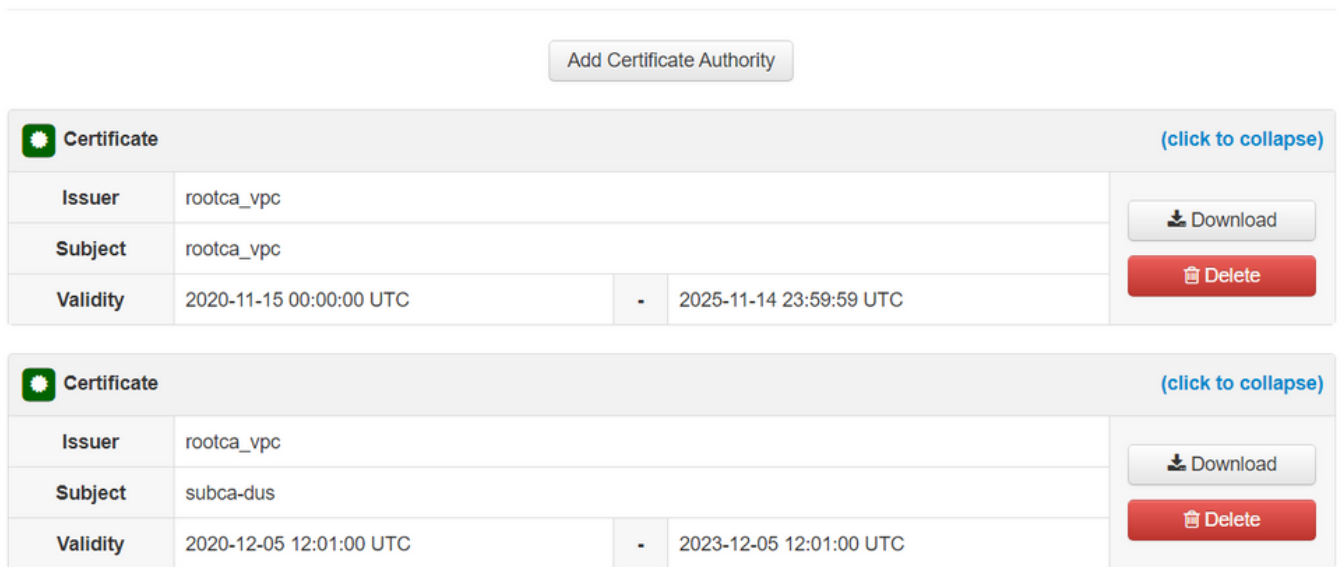
d'administration des appliances Threat Grid dans les **certificats CA**.

Dans l'exemple ci-dessous, la chaîne de certificats pour le certificat de service de mise à jour du périphérique de cloud privé AMP est **Root_CA > Sub_CA > Disposition_Update_Service** ; par conséquent, RootCA et Sub_CA doivent être installés dans les **certificats CA** de l'appliance Threat Grid.

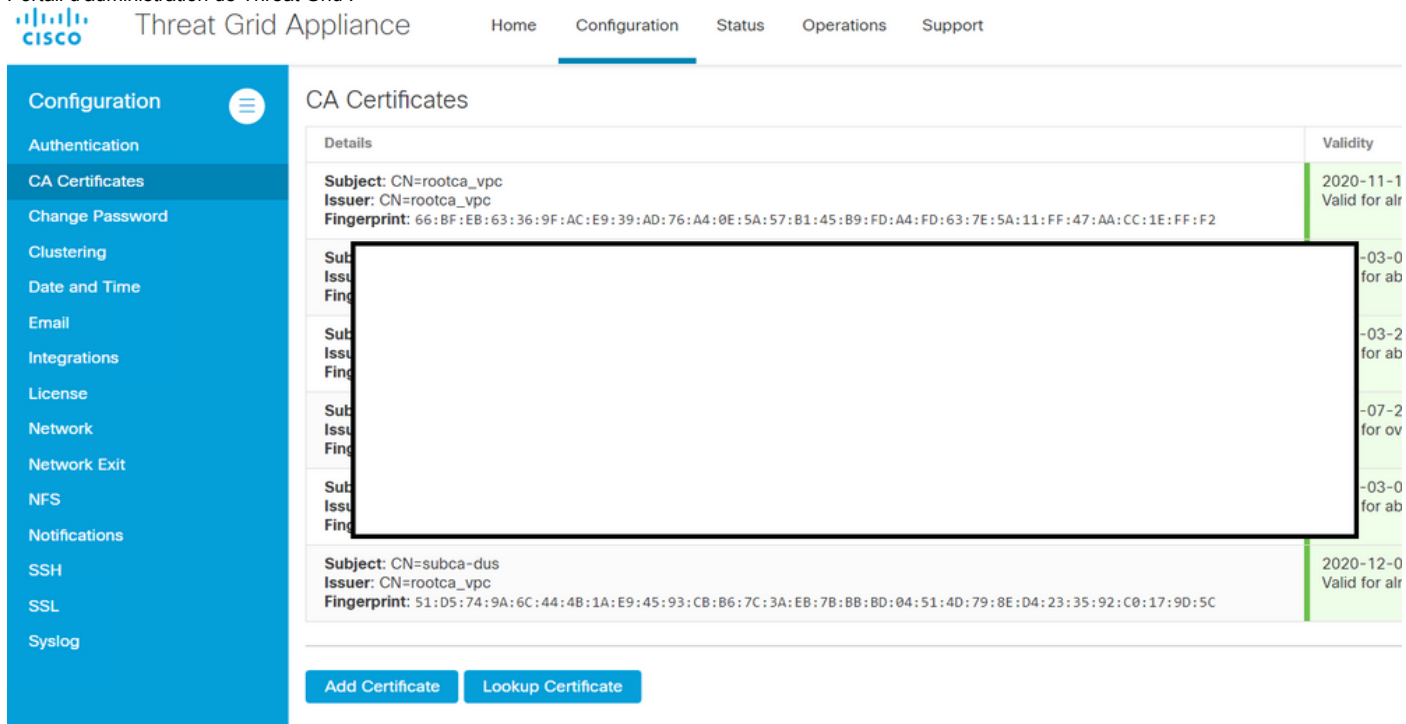
Autorités de certification dans le portail d'administration du cloud privé AMP.



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



Portail d'administration de Threat Grid :



- Confirmez que le nom de domaine complet du service de mise à jour de la mise à jour du périphérique de cloud

privé AMP a été correctement ajouté au portail d'administration des appliances Threat Grid dans **Administration > Manage AMP Private Cloud Integration**. Confirmez également que l'adresse IP de l'interface de console du périphérique de cloud privé AMP n'a pas été ajoutée au lieu du nom de domaine complet (FQDN).

disposition_update_user Ed
https://dupdateamp3.argarci2-lal: disposition_update_user ew236 [redacted] xJYfPK Sav
disposition_update_user Ed

Avertissement dans le périphérique de cloud privé AMP concernant un certificat SSL Threat Grid non valide

Symptôme

Message d'avertissement : « Le certificat SSL Threat Grid n'est pas valide », est reçu dans le périphérique de cloud privé AMP après avoir sélectionné le bouton **Test Connection** dans **Integrations > Threat Grid**.

Threat Grid Connection test failed.

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

Étapes recommandées :

- Confirmez si le certificat installé dans l'interface de nettoyage de l'appliance Threat Grid est signé par une autorité de certification d'entreprise.

Si elle est signée par une autorité de certification, la chaîne de certificats complète doit être ajoutée dans un fichier au portail d'administration de périphériques de cloud privé AMP **Integrations > Threat Grid** dans le **certificat SSL Threat Grid**.

Threat Grid Configuration Details Edit

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

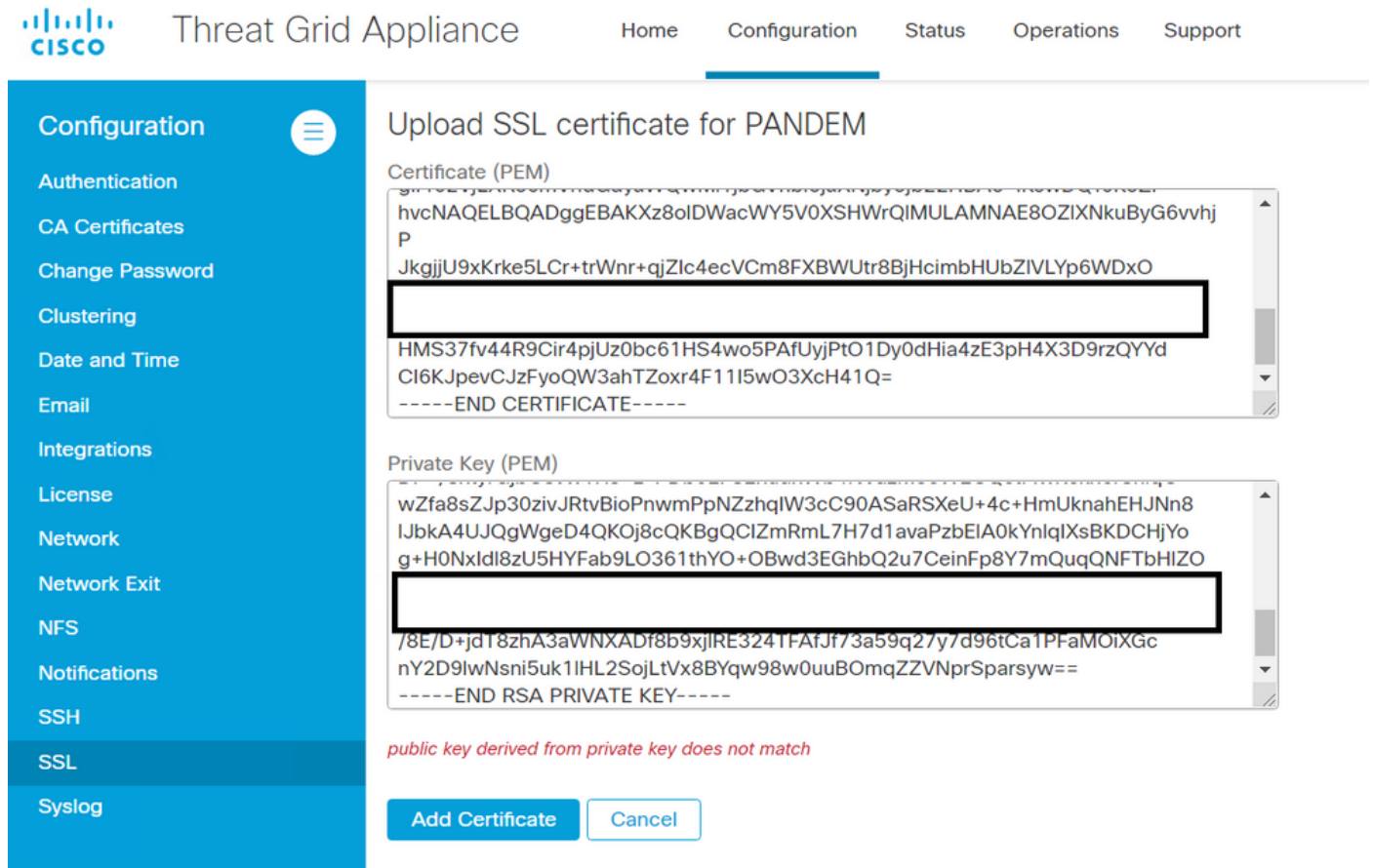
Dans le périphérique de cloud privé AMP, les certificats d'appliance Threat Grid actuellement installés se trouvent dans : `/opt/fire/etc/ssl/threat_grid.crt`.

Avertissements dans l'appliance Threat Grid relatifs aux certificats

Message d'avertissement : la clé publique dérivée de la clé privée ne correspond pas

Symptôme

Message d'avertissement : la clé publique dérivée de la clé privée ne correspond pas, est reçue dans l'appliance Threat Grid après une tentative d'ajout d'un certificat à une interface.



La clé publique exportée à partir de la clé privée ne correspond pas à la clé publique configurée dans le certificat.

Étapes recommandées :

- Confirmez si la clé privée correspond à la clé publique du certificat.

Si la clé privée correspond à la clé publique du certificat, le module et l'exposant public doivent être identiques. Pour cette analyse, il suffit de confirmer si le module a la même valeur dans la clé privée et la clé publique dans le certificat.

Étape 1. Utilisez l'outil OpenSSL pour comparer le module de la clé privée et la clé publique configurées dans le certificat.

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

Exemple . Correspondance réussie entre une clé privée et une clé publique configurées dans un certificat.


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

Message d'avertissement : la clé privée contient du contenu non PEM

Symptôme

Message d'avertissement : La clé privée contient du contenu non PEM, est reçue dans l'appliance Threat Grid après une tentative d'ajout d'un certificat à une interface.

The screenshot shows the Threat Grid Appliance configuration interface. The left sidebar contains a menu with options: 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 "Upload SSL certificate for PANDEM". It contains two text input fields. The first field is labeled "Certificate (PEM)" and contains a valid PEM certificate. The second field is labeled "Private Key (PEM)" and contains a private key with some non-PEM content. Below the private key field, a red warning message reads "private key contains non-PEM content". At the bottom of the form, there are two buttons: "Add Certificate" and "Cancel".

Les données PEM du fichier de clé privée sont endommagées.

Étapes recommandées :

- Confirmez l'intégrité des données à l'intérieur de la clé privée.

Étape 1. Utilisez l'outil OpenSSL pour vérifier l'intégrité de la clé privée.

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

Exemple . Sortie d'une clé privée avec des erreurs dans les données PEM à l'intérieur du fichier et d'une autre clé privée sans erreur dans le contenu 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 la sortie de la commande OpenSSL n'est pas **RSA Key ok**, cela signifie que des problèmes ont été détectés avec les données PEM à l'intérieur de la clé.

Si des problèmes ont été détectés avec la commande OpenSSL, alors :

- Confirmez si les données PEM à l'intérieur de la clé privée sont manquantes.

Les données PEM contenues dans le fichier de clé privée s'affichent en lignes de 64 caractères. Une vérification rapide des données PEM à l'intérieur du fichier peut indiquer si des données sont manquantes. La ligne comportant des données manquantes n'est pas alignée sur les autres lignes du fichier.

```

$ cat wrong-private-key.key
-----BEGIN PRIVATE KEY-----
MIIIEvAIBADANBgkqhkiG9w0BAQEFAASCbKYwggSiAgEAAoIBAQCvfIytwkf9UIc5
DluK9PTbKvDrShgn8/Cen9wXEUDIBNahlfizvwZb/5FL+I1ry/P0WKJMiXRhLQ52
Y0oogQsuDTw79Moa6xXYLKq1P5QRIV6tQQDniHUoHFNSLkoo0H0ubkDtGo/PW4fE
/JNGbMIU/d1DDuzxfgGze0viztT90rpCbZyQP2r+sGxaOKM0c3AEgK/pYA7aCv/G
P6rGkHc/ViM1NTuWVIWdIcLgTUX0DeHLjTiC12q/vH/i0WeIgAv10aGuBCOeg    <-----
NwOgPyY3XI8g7l          4HA6/VsM10NHKT4EhvSks
WXZW1XhNAgMBA          tU9huSCL7t4BF7VpSeKXM
Uh4/Vrdg1TYXfi          s7k0sCwmhKUaMacTYAnrg
fINIJto/x0azh          17ttvLvX3zweLCEXsDXK6
mdhzCQSTBfYbM          24M7HiocsbkLjijScTFYQ
JqSwA5BEgqeH3          1gd4kJ6ddAaSjQS7sJxaf
WtVHzbVDqJ+rb          3gQDePpxacxGRZLXfja3s
SU+TvjNWQGcUs          28y8ZQd0lqPZrV0Z6Mym2
i5S+/LS4jHB5hcCfnZpL4M0zHYvX+HPuGHm2x0Cy51K5KsfDPa/SrbhDkxZty0SG
lCgVLEycQ5t1xtI6qiBLKNmtrQKBgQDKI+BTMrHFYD50gPcBZyGXVhmSyHcZOP9k
OosXngeKtpdqL8Ck/H2QftFpOAFoHQxD/tiJA6E1eK9HfVnsq9+xbCU1fRlPxeCS
CbcflDYBwaMn8Ywp9PfZKPgu/gI3XIUWT6T0LcBGtdspYDEbApvYA091PoS0vcBn
g7LG+bcJIQKBgHFn/ZziDtrkSzJSN6fVGPhJHCutI+yZRuBkkz/8ohv1Rf+En+VY
9QG0GBq/MEBZy3TV+SUYfPX1SQ9eQDDYNQToKsfpUh0QvuQ0JeIGSm+E6jFApNeg
QauT9x0TkVDP1bP5LFkTMG27Brzr9oG95F45hrZ0gW0D+w7YdTYlGD7ZAoGASHku
b4XoeNS1771hUg5w27qR9q+LC+8EmiHnRrNxDsnCzd7zGfQw7MKbQDdFQdfQUvyn
FBDKFsrLRT1rJVDGJe2ZNaE/QmE20AVNs7PG3UBYx/RxhYV/60smGGsXz10Mn+A0
SxuwKWoARshnMsDvsTYwofm1SMwTlMmCKpbTiiECgYBi8ZjgsdFv2NtYlmb1pAYS
DHierblDtvumF42Tax+fucqUrdb3LZo6FjagvPy+LBJA3VjtrYkDjQmstvxD5jfd
V3Pq4IwaocGU8RQUJY5L6rmw+y1s6Z+iNkIcPeZtWidSgP+NZa1xvhfj8XeL560o
a+IQn0Y41zLJ22ScgyFzEQ==
-----END PRIVATE KEY-----

```

- Confirmez que la première ligne de la clé privée commence par 5 tirets, les mots **BEGIN**

PRIVATE KEY et se termine par 5 tirets.

Exemple .

—COMMENCER LA CLÉ PRIVÉE—

- Confirmez que la dernière ligne de la clé privée commence par 5 tirets, les mots **END PRIVATE KEY**, et se termine par 5 tirets.

Exemple .

—CLÉ PRIVÉE DE FIN—

Exemple . Corrigez le format PEM et les données dans une clé privée.

```
$ cat correct-private-key.key
-----BEGIN PRIVATE KEY-----
MIIIEvAIBADANBgkqhkiG9w0BAQEFAASCbKjYwggSiAgEAAoIBAQCvfIytwKf9UIc5
DluK9PTbKvDrShgn8/Cen9wXEUDIBNah1FiZvwZb/5FL+I1ry/P0WKJMIXRhLQ52
Y0oogQsuDTw79Moa6xXYLKq1P5QRIV6tQQDNiHUoHFNSLkoo0H0ubkDtGo/PW4fE
/JNGbMIU/d1DDuzxfgGze0viztT90rpCbZyQP2r+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+BTMrHFYD50gPcBZyGXVhmSyHcZ0P9k
OosXngeKtpdqL8Ck/H2QftFpOAFoHQxD/tiJA6E1eK9HfVnsq9+xbCU1fRlPxeCS
Cbcf1DYBwaMn8Ywp9PfZKpGu/gI3XIUWT6T0LcBGtdspYDEbApvYA091PoS0vcBn
g7LG+bcJIQKBGHFn/ZziDtrkSzJSN6fVGPhJHCuTI+yZRuBkkz/8ohv1Rf+En+VY
9QG0GBq/MEBZy3TV+SUYfPX1SQ9eQDDYNQToKsfpUh0QvuQ0JeIGSm+E6jFApNeg
QauT9x0TkVDP1bP5LFkTMG27Brzr9oG95F45hrZOgW0D+w7YdTYlGD7ZAoGASHku
b4XoeNS1771hUg5w27qR9q+LC+8EmiHnRrNxDsnCZd7zGfQw7MKbQDdFQdfQUvyn
FBDFsrLRT1rJVDGJe2ZNaE/QmE20AVNs7PG3UBYx/RxhYV/60smGGsXz10Mn+A0
SxuwKWoARshnMsDvsTYwofmlSMwTlMmCKpbTiiECgYBi8ZjgsdFv2NtYlmb1pAYS
DHierbltdVumF42Tax+fucqUrdB3LZo6FjagvPy+LBjA3VjtRYkDjQmstvxD5jfd
V3Pq4IwaocGU8RQUJY5L6rmw+y1s6Z+iNkIcPeZtWidSgP+NZa1xvhfj8XeL560o
a+IQn0Y41zLJ22ScgyFzEQ==
-----END PRIVATE KEY-----
```

Message d'avertissement - Impossible de générer la clé publique à partir de la clé privée

Symptôme

Message d'avertissement : ne peut pas générer de clé publique à partir de la clé privée, est reçu

dans l'appliance Threat Grid après une tentative d'ajout d'un certificat à une interface.

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//JbpWr1glIYVs1uYg==
-----END CERTIFICATE-----
```

Private Key (PEM)

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAACAQEAucb3AU15P91Ym/PvHva/xKBCbLeY7+jQJGO7wm7eruX3KTZY
EE9N6qn1+2YecCmOAA01sTqTQaHVHJdCsczgz1mGalFI6Xinl8JI9i+n2NDIcNr
XBVPvCU5f5nH2cZwKGTen/NDJhnyC5Dlb17RLy7Y+wxhMiyRCHH3aZ3lOMpl1k4X
[REDACTED]
cjSc9W8Fy/CDXbX27KncS4qWe91phsKXq0jo7wIDAQABAolBAFrH8EHRsvNTXY5v
yCSwXQtfaLYpjXGGqdduaPzdlrICrCGWbbgimKeYQByGTU9v7vXAx2EAh57Izvb2
-----END RSA PRIVATE KEY-----
```

cannot generate public key from private key

Add Certificate Cancel

La clé publique ne peut pas être générée à partir des données PEM actuelles dans le fichier de clé privée.

Étapes recommandées :

- Confirmez l'intégrité des données à l'intérieur de la clé privée.

Étape 1. Utilisez l'outil OpenSSL pour vérifier l'intégrité de la clé privée.

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

Si la sortie de la commande OpenSSL n'est pas **RSA Key ok**, cela signifie que des problèmes ont été détectés avec les données PEM à l'intérieur de la clé.

Étape 2. Utilisez l'outil OpenSSL pour vérifier si la clé publique peut être exportée à partir de la clé privée.

```
openssl rsa -in
```

Exemple . Échec de l'exportation de clé publique et succès de l'exportation de clé publique.

```
$ 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-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAz3yMrcJH/VCHOQ5bivT0
2yrw60oYJ/Pwnp/cFxFayATWoZRYmb8GW/+RS/iNa8vz9FiiTII0YS0dmNKKIEL
Lg080/TKGusV2CygqT+UESFerUEAzYh1KBxTUI5KKNB9Lm5A7RqPz1uHxPyTRmzC
FP3dQw7s8X4Bs3tL4s7U/Tq6Qm2ckD9q/rBswjiJNHNwBICv6WA02gr/xj+qxpB3
P1YjNTU71lSFnSHC4E1Fzg3hy40yHCNqv7x/4j1niIAL9dGhrgQjnoFQ1DcDoD8m
N1yPIOx3C0lWeVForZmx+Dg61+J4uIjytkVceBw0v1bDnDRyk+BIb0pLF12VtV4
TQIDAQAB
-----END PUBLIC KEY-----
```

Message d'avertissement - erreur d'analyse : Impossible de décoder les données PEM

Symptôme

Message d'avertissement : erreur d'analyse : Les données PEM n'ont pas pu être décodées. Elles sont reçues dans l'appliance Threat Grid après une tentative d'ajout d'un certificat à une interface.

The screenshot shows the Threat Grid Appliance configuration page for 'PANDEM'. The 'SSL' section is active in the left sidebar. 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'.

Le certificat ne peut pas être décodé à partir des données PEM actuelles dans le fichier de certificat. Les données PEM du fichier de certificat sont endommagées.

- Confirmez si les informations de certificat peuvent être récupérées à partir des données PEM dans le fichier de certificat.

Étape 1. Utilisez l'outil OpenSSL pour afficher les informations de certificat à partir du fichier de données PEM.

```
openssl x509 -in
```

Si les données PEM sont corrompues, une erreur s'affiche lorsque l'outil OpenSSL tente de charger les informations de certificat.

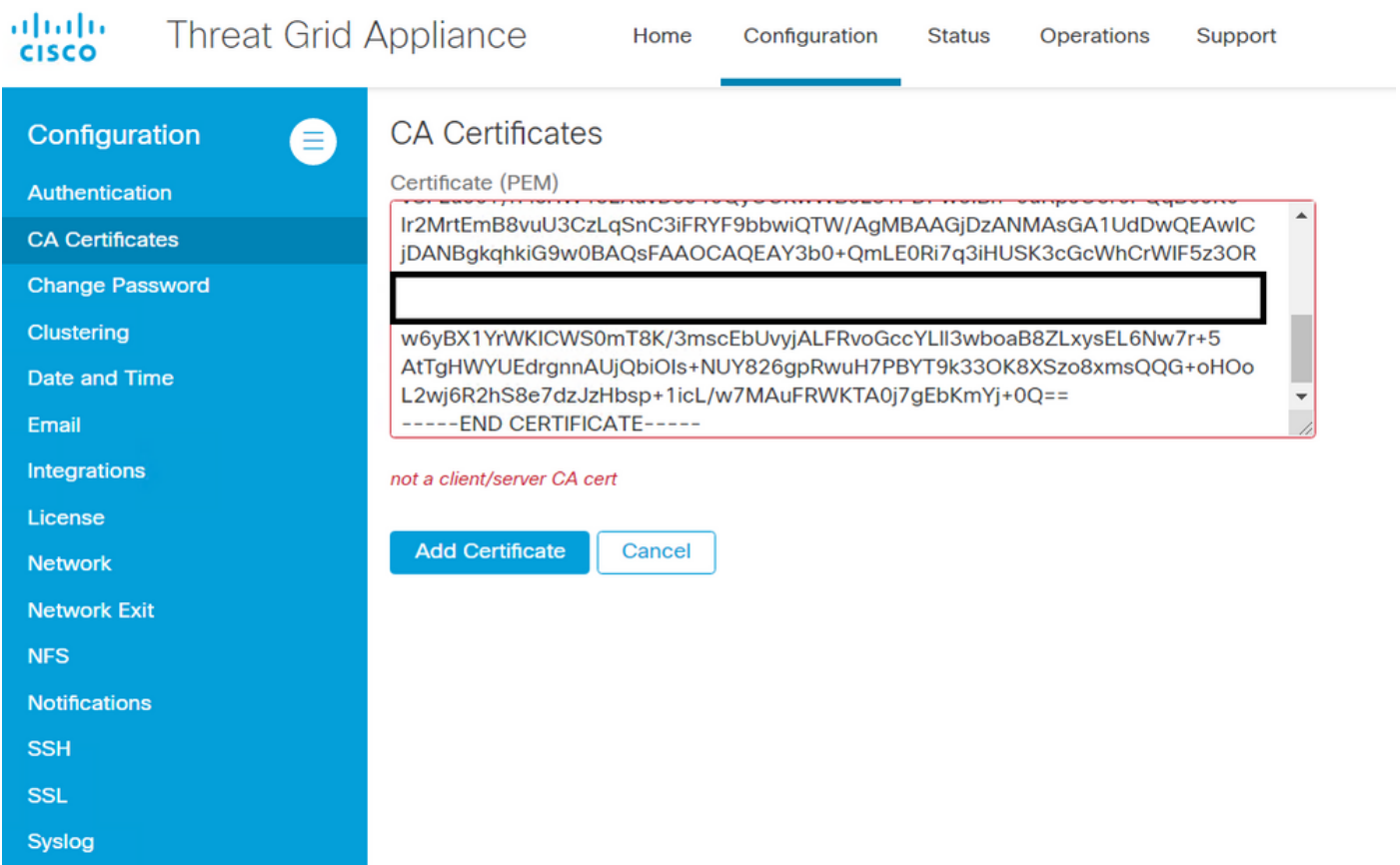
Exemple . Échec de la tentative de chargement des informations de certificat en raison de données PEM endommagées dans le fichier de certificat.

```
$ 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:
```

Message d'avertissement - pas un certificat CA client/serveur

Symptôme

Message d'avertissement : erreur d'analyse : n'est pas un certificat CA client/serveur, est reçu dans l'appliance Threat Grid après une tentative d'ajout d'un certificat CA à **Configuration > CA Certificates**.



The screenshot shows the Threat Grid Appliance interface. The left sidebar contains a menu with 'Configuration' selected. The main content area is titled 'CA Certificates' and shows a 'Certificate (PEM)' field. The certificate text is displayed in a text area, and a red error message 'not a client/server CA cert' is shown below it. The error message is highlighted with a red box. Below the error message are two buttons: 'Add Certificate' and 'Cancel'.

La valeur d'extension des contraintes de base dans le certificat de l'autorité de certification n'est pas définie comme CA : Vrai.

Confirmez avec l'outil OpenSSL si la valeur d'extension Contraintes de base est définie sur CA : True dans le certificat CA.

Étape 1. Utilisez l'outil OpenSSL pour afficher les informations de certificat à partir du fichier de données PEM.

```
openssl x509 -in
```

Étape 2. Recherchez dans les informations de certificat la valeur actuelle de l'extension **Contraintes de base**.

Exemple . Valeur de contrainte de base pour une autorité de certification acceptée par l'appliance Threat Grid.

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

Informations connexes

- [Appliance Threat Grid - Guides de configuration](#)
- [Appliance de cloud privé virtuel Cisco AMP - Exemples de configuration et notes techniques](#)
- [Support et documentation techniques - Cisco Systems](#)