ESA avec AMP reçoit l'erreur « Le service File Reputation n'est pas accessible »

Contenu

Introduction

Ce document décrit l'alerte attribuée à l'appliance de sécurité de la messagerie Cisco (ESA) avec Advanced Malware Protection (AMP) activé, où le service ne peut pas communiquer via le port 32137 ou 443 pour la réputation des fichiers.

Corrigez l'erreur « Le service de réputation de fichiers n'est pas accessible » reçue pour AMP

AMP a été publié pour être utilisé sur ESA dans AsyncOS version 8.5.5 pour la sécurité de la messagerie. Avec AMP sous licence et activé sur ESA, les administrateurs reçoivent le message suivant :

```
The Warning message is:

The File Reputation service is not reachable.

Last message occurred 2 times between Tue Jul 26 10:17:15 2015 and Tue Jul 26 10:18:16 2016.

Version: 12.5.0-066
Serial Number: 123A82F6780XXX9E1E10-XXX5DBEFCXXX
Timestamp: 07 Oct 2019 14:25:13 -0400
```

Le service AMP est peut-être activé, mais il ne communique probablement pas sur le réseau via le port 32137 pour la réputation des fichiers.

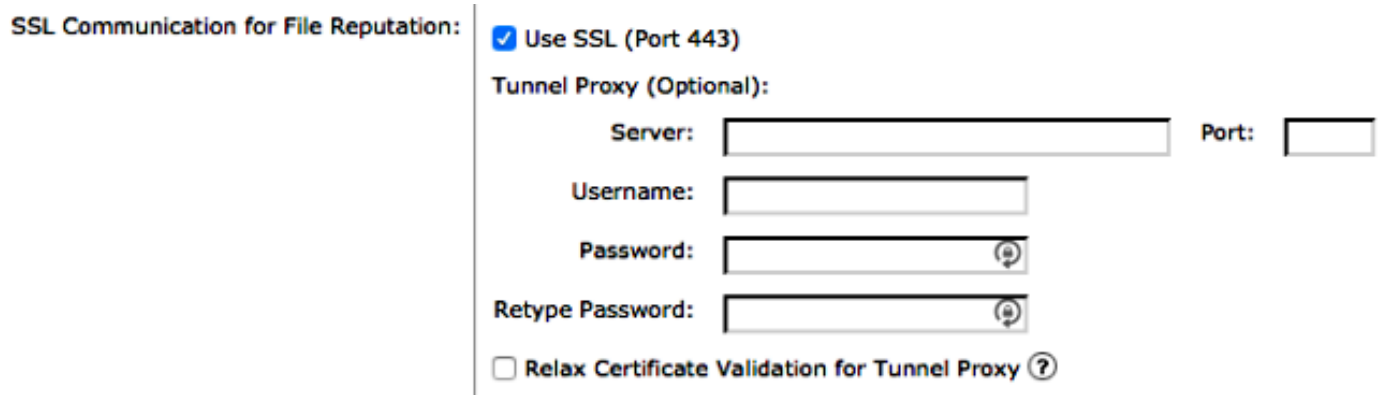
Dans ce cas, l'administrateur ESA peut choisir de faire communiquer File Reputation via le port 443.

Pour ce faire, exécutez **ampconfig > advanced** à partir de la CLI et assurez-vous que **Y** est sélectionné pour **Do you want to enable SSL communication (port 443) for file reputation ?** *[N]>* :

```
(Cluster example.com)> ampconfig

Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
```

```
- CACHESETTINGS - Configure the cache settings for AMP.
- CLUSTERSET - Set how advanced malware protection is configured in a cluster.
- CLUSTERSHOW - Display how advanced malware protection is configured in a cluster.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.cisco.com)
2. AMERICAS(Legacy) (cloud-sa.amp.sourcefire.com)
3. EUROPE (cloud-sa.eu.amp.cisco.com)
4. APJC (cloud-sa.apjc.amp.cisco.com)
5. Private reputation cloud
[1]>

Do you want use the recommended analysis threshold from cloud service? [Y]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [N]> Y

Proxy server detail:
Server :
Port :
User :

Do you want to change proxy detail [N]>

Do you want to suppress the verdict update alerts for all messages that are not delivered to the
recipient? [N]>

Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. EUROPE (https://panacea.threatgrid.eu)
3. Private analysis cloud
[1]>
```

Si vous utilisez l'interface graphique utilisateur, choisissez **Security Services > File Reputation and Analysis > Edit Global Settings > Advanced (liste déroulante)** et vérifiez que la case à cocher **Use SSL** est cochée comme indiqué ici :



Validez toutes les modifications apportées à la configuration.

Enfin, consultez le journal AMP actuel afin de connaître la réussite ou l'échec du service et de la connectivité. Vous pouvez accomplir ceci à partir de l'interface de ligne de commande avec l'**ampli arrière**.

Avant d'apporter des modifications à **ampconfig > advanced**, vous auriez vu ceci dans les journaux d'AMP :

```
Mon Jan 26 10:11:16 2015 Warning: amp The File Reputation service in the cloud
is unreachable.
Mon Jan 26 10:12:15 2015 Warning: amp The File Reputation service in the cloud
is unreachable.
Mon Jan 26 10:13:15 2015 Warning: amp The File Reputation service in the cloud
is unreachable.
```

Une fois la modification apportée à **ampconfig > advanced**, vous voyez ceci dans les journaux AMP :

```
Mon Jan 26 10:19:19 2015 Info: amp stunnel process started pid [3725]
Mon Jan 26 10:19:22 2015 Info: amp The File Reputation service in the cloud
is reachable.
Mon Jan 26 10:19:22 2015 Info: amp File reputation service initialized
successfully
Mon Jan 26 10:19:22 2015 Info: amp File Analysis service initialized
successfully
Mon Jan 26 10:19:23 2015 Info: amp The File Analysis server is reachable
Mon Jan 26 10:20:24 2015 Info: amp File reputation query initiating. File Name =
'amp_watchdog.txt', MID = 0, File Size = 12 bytes, File Type = text/plain
Mon Jan 26 10:20:24 2015 Info: amp Response received for file reputation query
from Cloud. File Name = 'amp_watchdog.txt', MID = 0, Disposition = file unknown,
Malware = None, Reputation Score = 0, sha256 = a5f28f1fed7c2fe88bcdf403710098977
fa12c32d13bfbd78bbe27e95b245f82, upload_action = 1
```

Le fichier **amp_watchdog.txt** comme indiqué dans l'exemple précédent s'exécutera toutes les 10 minutes et sera suivi dans le journal AMP. Ce fichier fait partie de l'application keep-alive pour AMP.

Une requête normale dans le journal AMP sur un message avec le ou les types de fichiers configurés pour File Reputation et File Analysis serait similaire à ceci :

```
Wed Jan 14 15:33:01 2015 Info: File reputation query initiating. File Name =
'securedoc_20150112T114401.html', MID = 703, File Size = 108769 bytes, File
Type = text/html
Wed Jan 14 15:33:02 2015 Info: Response received for file reputation query from
Cloud. File Name = 'securedoc_20150112T114401.html', MID = 703, Disposition = file
unknown, Malware = None, Reputation Score = 0, sha256 = c1afd8efe4eeb4e04551a8a0f5
533d80d4bec0205553465e997f9c672983346f, upload_action = 1
```

Grâce à ces informations de journal, l'administrateur doit pouvoir corréler l'ID de message (MID) dans les journaux de messagerie.

Dépannage

Vérifiez les paramètres du pare-feu et du réseau afin de vous assurer que la communication SSL est ouverte pour les éléments suivants :

Port	Protocol	Entrée/Sortie	Nom de l'hôte	Description
443	TCP	Dehors	Comme configuré dans Services de sécurité > File Reputation and Analysis, section Advanced.	Accès aux services cl pour l'analyse des fich

32137	TCP	Dehors	Comme configuré dans Services de sécurité > File Reputation and Analysis, section Advanced, section Advanced, paramètre Pool de serveurs cloud.	Accès aux services cl afin d'obtenir la réputa des fichiers.

Vous pouvez tester la connectivité de base entre votre ESA et le service cloud sur 443 via Telnet afin de vous assurer que votre appliance peut atteindre les services AMP, la réputation des fichiers et l'analyse des fichiers.

> **Remarque** : les adresses pour File Reputation et File Analysis sont configurées sur l'interface de ligne de commande avec **ampconfig > advanced** ou depuis l'interface utilisateur graphique avec **Security Services > File Reputation and Analysis > Edit Global Settings > Advanced (liste déroulante)**.

> **Note**: Si vous utilisez un proxy de tunnel entre le serveur ESA et le ou les serveurs File Reputation, vous devrez peut-être activer l'option Relâcher la validation de certificat pour le proxy de tunnel. Cette option est fournie pour ignorer la validation de certificat standard si le certificat du serveur proxy de tunnel n'est pas signé par une autorité racine approuvée par le serveur ESA. Par exemple, sélectionnez cette option si vous utilisez un certificat auto-signé sur un serveur proxy de tunnel interne approuvé.

Exemple de réputation de fichiers :

```
10.0.0-125.local> telnet cloud-sa.amp.sourcefire.com 443

Trying 23.21.199.158...
Connected to ec2-23-21-199-158.compute-1.amazonaws.com.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

Exemple d'analyse de fichier :

```
10.0.0-125.local> telnet panacea.threatgrid.com 443

Trying 69.55.5.244...
Connected to 69.55.5.244.
Escape character is '^]'.
^]
telnet> quit
Connection closed.
```

Si l'ESA est en mesure d'établir une connexion Telnet avec le serveur de réputation de fichiers et qu'aucun proxy en amont ne déchiffre la connexion, il se peut que l'appliance doive être réenregistrée auprès de Threat Grid. Sur l'interface de ligne de commande ESA se trouve une commande masquée :

```
10.0.0-125.local> diagnostic

Choose the operation you want to perform:
```

```
- RAID - Disk Verify Utility.
- DISK_USAGE - Check Disk Usage.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- SERVICES - Service Utilities.
[]> ampregister

AMP registration initiated.
```

Informations connexes

- Test AMP (Advanced Malware Protection) ESA
- Guides utilisateur ESA
- FAQ ESA : Qu'est-ce qu'un ID de message (MID), un ID de connexion d'injection (ICID) ou un ID de connexion de remise (DCID) ?
- Comment rechercher et afficher les journaux de messagerie sur l'ESA ?
- Support et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.