L'ESA avec l'AMP reçoit le " ; Le service de réputation de fichier n'est pas reachable" ; Erreur

Contenu

Introduction

Ce document décrit l'alerte attribuée à l'appliance de sécurité du courrier électronique de Cisco (ESA) avec la protection avancée de malware (AMP) activée, où le service ne peut pas communiquer au-dessus du port 32137 ou 443 pour la réputation de fichier.

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

L'AMP a été libéré pour l'usage sur l'ESA dans la version 8.5.5 d'AsyncOS pour la sécurité du courrier électronique. L'AMP autorisé et étant activé sur l'ESA, les administrateurs reçoivent ce message :

```
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 d'AMP pourrait être activé, mais ne communique pas probablement sur le réseau par l'intermédiaire du port 32137 pour la réputation de fichier.

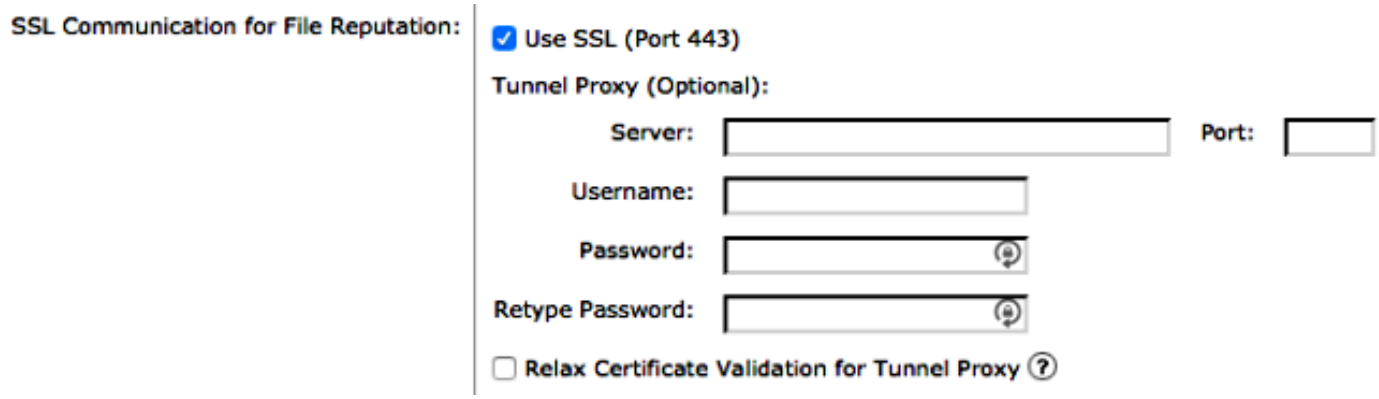
Si c'est le cas, l'administrateur ESA peut choisir de faire communiquer la réputation de fichier au-dessus du port 443.

Afin de faire ainsi, exécutez l'**ampconfig > avancé du** CLI et soyez sûr que **Y** est sélectionné pour *vous veulent activer la transmission SSL (port 443) pour la réputation de fichier ? [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 le GUI, choisissez les **Services de sécurité > la réputation de fichier et l'analyse > éditent des paramètres généraux > a avancé (déroulant)** et s'assure que la case à cocher **SSL d'utilisation** est vérifiée comme affiché ici :



Commettez l'intégralité de modifications à la configuration.

En conclusion, passez en revue la commande en cours de procédure de connexion d'AMP pour voir le succès ou échec de service et de Connectivité. Vous pouvez accomplir ceci du CLI avec l'**Ampère de queue.**

Avant des modifications apportées à l'**ampconfig > a avancé**, vous aurait vu ceci dans les logs 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.
```

Après que la modification soit apportée à l'**ampconfig > avancé**, vous voyez ceci dans les logs d'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 d'**amp_watchdog.txt** suivant les indications de l'exemple précédent exécutera toutes les 10 minutes et sera dépisté dans le log d'AMP. Ce fichier fait partie de la keep-alive pour l'AMP.

Une requête normale dans le log d'AMP contre un message avec le type de fichier configuré pour la réputation de fichier et l'analyse de fichier serait semblable 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
```

Avec ces informations de log, l'administrateur devrait pouvoir corréler l'ID de message (MID) dans les logs de messagerie.

Dépanner

Pare-feu et paramètres réseau d'examen afin de s'assurer que la transmission SSL est ouverte pour ces derniers :

Port	Protocol	Entrée/sortie	Nom de l'hôte	Description
443	TCP		Comme configuré dans les Services de sécurité > la réputation et l'analyse de fichier, section avancée.	Access aux services e nuage pour l'analyse c fichier.
32137	TCP		Comme configuré dans les Services de sécurité > la réputation et l'analyse de fichier, section avancée,	Access aux services e nuage afin d'obtenir la

	section avancée, paramètre de groupe de serveur de nuage.	réputation de fichier.

Vous pouvez tester la Connectivité de base de votre ESA au service en nuage plus de 443 par l'intermédiaire du telnet afin de s'assurer que votre appliance peut avec succès atteindre les services d'AMP, classer la réputation, et classer l'analyse.

> Remarque: Les adresses pour la réputation de fichier et l'analyse de fichier sont configurées sur le CLI avec l'**ampconfig > avancé** ou du GUI avec des **Services de sécurité > la réputation et l'analyse de fichier > éditez les paramètres généraux > avancé (déroulant)**.

> Remarque: Si utilisant un proxy de tunnel entre l'ESA et les serveurs de réputation de fichier, vous pouvez être requis d'activer l'option de détendre la validation de certificat pour le proxy de tunnel. Cette option est fournie d'ignorer la validation standard de certificat si le certificat du serveur proxy de tunnel n'est pas signé par une autorité de racine faite confiance par l'ESA. Par exemple, sélectionnez cette option si utilisant un certificat auto-signé sur un serveur proxy interne de confiance de tunnel.

Exemple de réputation de fichier :

```
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.
```

Informations connexes

- Test de protection de malware avancé par ESA (AMP)
- Guides utilisateurs ESA
- FOIRE AUX QUESTIONS ESA : Quel est un ID de message (MID), l'ID de connexion d'injection (ICID), ou l'ID de connexion de la livraison (DCID) ?
- Comment est-ce que je le recherche et visualiser la messagerie ouvre une session l'ESA ?
- Support et documentation techniques - Cisco Systems