L'ESA avec l'AMPÈRE reçoit « le service de réputation de fichier dans le nuage est » erreur inaccessible

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 (AMPÈRE) activée, où le service ne communique pas au-dessus du port 32137 pour la réputation de fichier.

Corrigez « le service de réputation de fichier dans le nuage est » erreur inaccessible reçue pour l'AMPÈRE

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

```
The Warning message is:

amp The File Reputation service in the cloud is unreachable.

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

Version: 10.0.0-125
Serial Number: 123A82F6780EEE9E1E10-AAA5DBEFCEEE
Timestamp: 26 Jul 2016 10:56:28 -0600
```

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

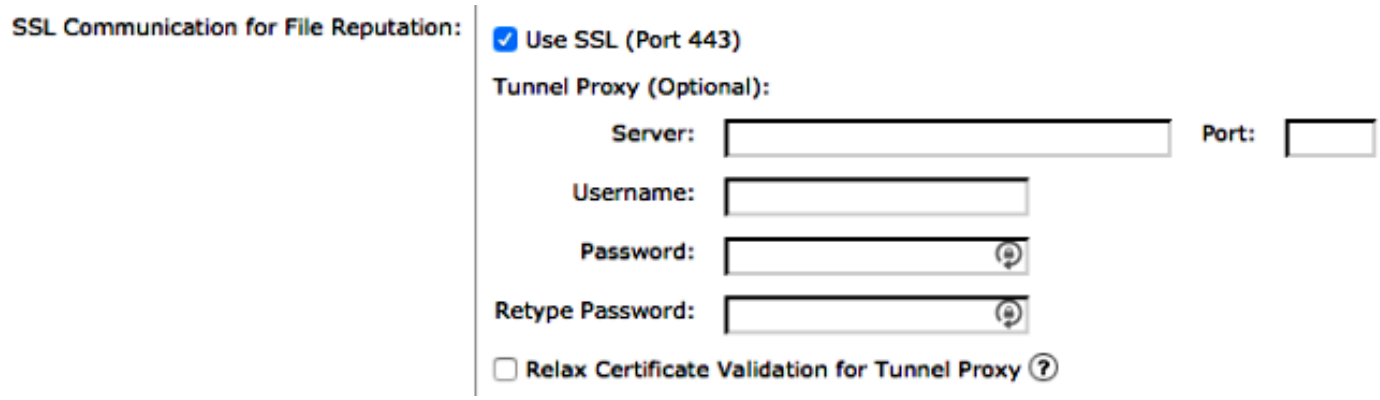
Si c'est le cas, l'administrateur ESA peut choisir de faire communiquer la réputation de fichier au-dessus du port 443.

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] >* :

```
10.0.0-125.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
```

```
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet


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.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[1]>

Enter cloud domain?
[a.immunet.com]>

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

Enter heartbeat interval?
[15]>

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

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

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
```

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 **SSL d'utilisation** est cochée 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'AMPÈRE 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'AMPÈRE :

```
10.0.0-125.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet


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.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[1]>

Enter cloud domain?
[a.immunet.com]>

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

Enter heartbeat interval?
[15]>

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

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

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
```

Après que la modification soit apportée à l'**ampconfig > avancé**, vous voyez ceci dans les logs d'AMPÈRE :

```
10.0.0-125.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet


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.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[1]>

Enter cloud domain?
[a.immunet.com]>

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

Enter heartbeat interval?
[15]>

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

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

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
```

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'AMPÈRE. Ce fichier fait partie de la keep-alive pour l'AMPÈRE.

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

```
10.0.0-125.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet


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.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
```

```
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[1]>

Enter cloud domain?
[a.immunet.com]>

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

Enter heartbeat interval?
[15]>

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

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

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
```

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

Dépannez

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

Port	Protocol	Entrée/sortie	Adresse Internet	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, section avancée, paramètre de groupe de serveur de nuage.	Access aux services e nuage afin d'obtenir la 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'AMPÈRE, 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)**.

Exemple de réputation de fichier :

```
10.0.0-125.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
```

```
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet


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.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[1]>

Enter cloud domain?
[a.immunet.com]>

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

Enter heartbeat interval?
[15]>

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

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

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
```

Exemple d'analyse de fichier :

```
10.0.0-125.local> ampconfig

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet


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.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
```

```
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[1]>

Enter cloud domain?
[a.immunet.com]>

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

Enter heartbeat interval?
[15]>

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

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

File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
```

Informations connexes

- Test de protection de malware avancé par ESA (AMPÈRE)
- 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