# Dépannage De " ; Le Service De Réputation De Fichiers N'Est Pas Accessible" ; Erreur sur Cisco ESA

## Table des matières


Introduction

Composants utilisés

Conditions préalables et risques

Identifier l'erreur

Valider les paramètres de réputation des fichiers

- À partir de l'interface utilisateur
- À partir de la CLI

Vérifier la connectivité

- Région Amérique du Nord et États-Unis
- Région du Canada
- Région Europe
- Région Australie
- Région APJC

Analyser les journaux AMP

Inscrivez-vous à Threat Grid

Informations connexes


## Introduction

Ce document décrit comment résoudre l'alerte « File Reputation service is not reachable » sur le dispositif de sécurité de la messagerie Cisco (ESA).

## Composants utilisés

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.

## Conditions préalables et risques

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

- Appliance de sécurisation de la messagerie Cisco AsyncOS 15.x ou version ultérieure

- Licence et activation d'Advanced Malware Protection (AMP)

---

Conseil : Assurez-vous que votre pare-feu autorise les communications sortantes sur le port 443. Si vous utilisez un proxy de tunnel, vous pouvez être amené à activer l'option de relâchement de la validation des certificats pour le proxy de tunnel. Cette action ignore la validation de certificat standard si le certificat du serveur proxy n'est pas signé par une autorité racine approuvée par l'ESA. Par exemple, utilisez cette option si vous utilisez un certificat auto-signé sur un serveur proxy de tunnel interne approuvé.

---

# Identifier l'erreur

Lorsque AMP est sous licence et activé sur l'ESA, vous recevez le message suivant :

<#root>

```
The Warning message is:

The File Reputation service is not reachable.

Last message occurred 2 times between Mon Feb 23 14:15:14 2026 and Mon Feb 23 14:16:23 2026.

Version: 15.5.1-055
Serial Number: 123A82F6780XXX9E1E10-XXX5DBEFCXXX
Timestamp: 23 Feb 2026 14:19:00 -0500
```

# Valider les paramètres de réputation des fichiers

## À partir de l'interface utilisateur

Assurez-vous que le serveur File Reputation approprié est sélectionné. Pour ce faire, accédez à Services de sécurité > File Reputation and Analysis > Edit Global Settings > Advanced Settings for File Reputation > File Reputation Server dans l'interface utilisateur graphique. Sélectionnez ensuite le cloud correspondant à votre région.

Pour obtenir le nom d'hôte et les informations de port permettant de configurer votre pare-feu, consultez la section Informations sur le pare-feu du guide de l'utilisateur.

## À partir de la CLI

Utilisez la commande ampconfig dans l'interface de ligne de commande pour configurer les paramètres Advanced Malware Protection. Utilisez la sous-commande advanced pour définir les délais d'expiration des requêtes cloud et sélectionner le cloud de réputation.

<#root>

```
(Cluster example.com)>
```

**ampconfig**

```
File Reputation: Enabled
File Analysis: Enabled
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 detai
- 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?
[20]>


Choose a file reputation server:

1. US Cloud
2. EU Cloud
3. APJC Cloud
4. Private reputation cloud
[1]>
```

# Vérifier la connectivité

Vérifiez les paramètres de pare-feu et de réseau pour vous assurer que la communication SSL est ouverte pour ces ports pour la réputation des fichiers :

## Région Amérique du Nord et États-Unis

| Objectif | Nom de l'hôte | Port par défaut | Protocol | Entrée/Sortie |
|---|---|---|---|---|
| Réputation des fichiers | cloud-esa-asn<br>amp.cisco.com<br>cloud-esa-est | 443 | TCP | Dehors. |
| Analyse de fichiers | panacea.threatgrid.com | 443 | TCP | Dehors |

## Région du Canada

| Objectif | Nom de l'hôte | Port par défaut | Protocol | Entrée/Sortie |
|---|---|---|---|---|
| Analyse de fichiers | panacea.threat.ca | 443 | TCP | Dehors |

## Région Europe

| Objectif | Nom de l'hôte | Port par défaut | Protocol | Entrée/Sortie |
|---|---|---|---|---|
| Réputation des fichiers | cloud-esa-asn<br>eu.amp.cisco.com<br>cloud-esa-est | 443 | TCP | Dehors. |
| Analyse de fichiers | panacea.threat.eu | 443 | TCP | Dehors |

## Région Australie

| Objectif | Nom de l'hôte | Port par défaut | Protocol | Entrée/Sortie |
|---|---|---|---|---|
| Analyse de fichiers | panacea.threatgrid.com.au | 443 | TCP | Dehors |

## Région APJC

| Objectif | Nom de l'hôte | Port par défaut | Protocol | Entrée/Sortie |
|---|---|---|---|---|
| Réputation des fichiers | cloud-esa-asn<br>apjc.amp.cisco.com<br>cloud-esa-est | 443 | TCP | Dehors. |
| Analyse de fichiers | Peut utiliser des hôtes européens ou nord-américains. | 443 | TCP | Dehors |

Pour vous assurer que l'appliance de sécurité de la messagerie électronique (ESA) peut atteindre les services Cisco AMP, vérifiez la connectivité sur le port 443 à l'aide des commandes telnet suivantes à partir de l'interface de ligne de commande :

Exemples de tests de connectivité (région des États-Unis) :

<#root>

```
(Machine esa.example.com)>
```

**telnet amp.cisco.com 443**

<#root>

(Machine esa.example.com)>

**telnet panacea.threatgrid.com 443**

# Analyser les journaux AMP

Consultez le journal AMP actuel pour déterminer l'état du service et de la connectivité. Utilisez la commande tail amp dans la CLI pour observer les entrées du journal en temps réel.

Si le service File Reputation n'est pas accessible, les journaux affichent les entrées suivantes :

```
Mon Feb 23 10:11:16 2026 Warning: amp The File Reputation service in the cloud is unreachable.
Mon Feb 23 10:12:15 2026 Warning: amp The File Reputation service in the cloud is unreachable.
Mon Feb 23 10:13:15 2026 Warning: amp The File Reputation service in the cloud is unreachable.
```

Après avoir corrigé la configuration dans ampconfig > advanced, les journaux affichent une initialisation réussie :

```
Mon Feb 23 10:19:19 2026 Info: amp stunnel process started pid [3725]
Mon Feb 23 10:19:22 2026 Info: amp The File Reputation service in the cloud is reachable.
Mon Feb 23 10:19:22 2026 Info: amp File reputation service initialized successfully
Mon Feb 23 10:19:22 2026 Info: amp File Analysis service initialized successfully
Mon Feb 23 10:19:23 2026 Info: amp The File Analysis server is reachable
Mon Feb 23 10:20:24 2026 Info: amp File reputation query initiating. File Name =
'amp_watchdog.txt', MID = 0, File Size = 12 bytes, File Type = text/plain
Mon Feb 23 10:20:24 2026 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 s'exécute toutes les 10 minutes et est suivi dans le journal AMP. Ce fichier fait partie de l'application keep-alive pour AMP. Une requête normale sur un message avec des types de fichiers configurés apparaît comme suit :

```
Mon Feb 23 15:33:01 2026 Info: File reputation query initiating. File Name =
'securedoc_20260223T114401.html', MID = 703, File Size = 108769 bytes, File
Type = text/html
Mon Feb 23 15:33:02 2026 Info: Response received for file reputation query from
Cloud. File Name = 'securedoc_20260223T114401.html', MID = 703, Disposition = file
```

```
unknown, Malware = None, Reputation Score = 0, sha256 = c1afd8efe4eeb4e04551a8a0f5
533d80d4bec0205553465e997f9c672983346f, upload_action = 1
```

## Inscrivez-vous à Threat Grid

Si l'ESA peut établir une connexion Telnet avec le serveur de réputation de fichiers et qu'aucun proxy en amont ne déchiffre la connexion, l'appliance peut nécessiter un nouvel enregistrement auprès de Threat Grid. Utilisez la commande ampregister masquée dans le menu diagnostic pour lancer ce processus.

<#root>

```
esa.example.com>
```

**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 d'utilisation ESA
- FAQ de Cisco® Email Security Appliance : 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 ?
- Assistance 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.