"；文件信誉服务不可达故障排除"Cisco ESA出错

目录

简介

使用的组件

前提条件和风险

识别错误

验证文件信誉设置

- 从GUI
- 从 CLI

检验连通性

- 美国和北美地区
- 加拿大地区
- 欧洲地区
- 澳大利亚地区
- 亚太地区

分析AMP日志

向Threat Grid注册

相关信息

简介

本文档介绍如何解决思科邮件安全设备(ESA)上的“文件信誉服务不可达”警报。

使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

前提条件和风险

本文档中的信息基于以下软件和硬件版本：

- 思科邮件安全设备AsyncOS 15.x或更高版本
- 高级恶意软件防护(AMP)已获许可并已启用



提示：确保您的防火墙允许端口443上的出站通信。如果您使用隧道代理，则可能要求您启用“放宽隧道代理的证书验证”选项。如果代理服务器证书未由ESA信任的根颁发机构签名，则此操作跳过标准证书验证。例如，如果您在受信任的内部隧道代理服务器上使用自签

名证书，请使用此选项。

识别错误

当AMP在ESA上获得许可并启用时，您将收到以下消息：

<#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
```

验证文件信誉设置

从GUI

确保选择了正确的文件信誉服务器。您可以在GUI中执行此操作，方法是导航到安全服务(Security Services)>文件信誉和分析(File Reputation and Analysis)>编辑全局设置(Edit Global Settings)>文件信誉的高级设置(Advanced Settings for File Reputation)>文件信誉服务器(File Reputation Server)。从此处选择适合您所在地区的云。

有关配置防火墙的主机名和端口信息，请参阅用户指南中的防火墙信息部分。

从 CLI

在CLI中使用ampconfig命令配置高级恶意软件防护参数。使用advanced子命令设置云查询超时并选择信誉云。

<#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]>
```

检验连通性

检查防火墙和网络设置，确保文件信誉的以下端口打开SSL通信：

美国和北美地区

目的	主机名	默认端口	协议	输入/输出
文件信誉	cloud-esa-asn amp.cisco.com 云 — esa-est	443	TCP	出去。
文件分析	panacea.threatgrid.com	443	TCP	出站

加拿大地区

目的	主机名	默认端口	协议	输入/输出
文件分析	panacea.threatgrid.ca	443	TCP	出站

欧洲地区

目的	主机名	默认端口	协议	输入/输出
文件信誉	cloud-esa-asn eu.amp.cisco.com	443	TCP	出去。

	云 — esa-est			
文件分析	panacea.threatgrid.eu	443	TCP	出站

澳大利亚地区

目的	主机名	默认端口	协议	输入/输出
文件分析	panacea.threatgrid.com.au	443	TCP	出站

亚太地区

目的	主机名	默认端口	协议	输入/输出
文件信誉	cloud-esa-asn apjc.amp.cisco.com 云 — esa-est	443	TCP	出去。
文件分析	可以利用欧洲或北美主持人。	443	TCP	出站

为确保邮件安全设备(ESA)可以访问思科AMP服务，请从CLI使用以下telnet命令验证端口443上的连接：

连接测试示例（美国地区）：

```
<#root>

(Machine esa.example.com)>

telnet amp.cisco.com 443
```

```
<#root>

(Machine esa.example.com)>

telnet panacea.threatgrid.com 443
```

分析AMP日志

查看当前AMP日志以确定服务和连接状态。在CLI中使用tail amp命令观察实时日志条目。

如果文件信誉服务无法访问，日志将显示以下条目：

```
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.
```

在ampconfig > advanced中更正配置后，日志将显示成功的初始化：

```
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
```

amp_watchdog.txt文件每10分钟运行一次，并在AMP日志中进行跟踪。此文件是AMP的“保持连接”的一部分。对具有配置文件类型的消息进行常规查询如下所示：

```
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
```

向Threat Grid注册

如果ESA可以telnet到文件信誉服务器，并且没有上游代理解密连接，则设备可能需要向Threat Grid重新注册。使用diagnostic菜单中的hidden ampregister命令启动此过程。

```
<#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.

相关信息

- ESA高级恶意软件防护(AMP)测试
- ESA用户指南
- ESA 常见问题解答：什么是消息ID(MID)、注入连接ID(ICID)或传送连接ID(DCID)?
- 如何搜索和查看ESA上的邮件日志？
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。