带有AMP的ESA收到“The File Reputation service is not reachable”错误

目录

简介

本文档介绍归因于启用高级恶意软件防护(AMP)的思科邮件安全设备(ESA)的警报，其中服务无法通过端口32137或443进行文件信誉通信。

更正AMP收到的“The File Reputation service is not reachable”错误

AMP已发布用于邮件安全的AsyncOS版本8.5.5中的ESA。 在ESA上许可并启用AMP后，管理员会收到以下消息：

```
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
```

AMP服务可能已启用，但可能不会通过文件信誉的端口32137在网络上通信。

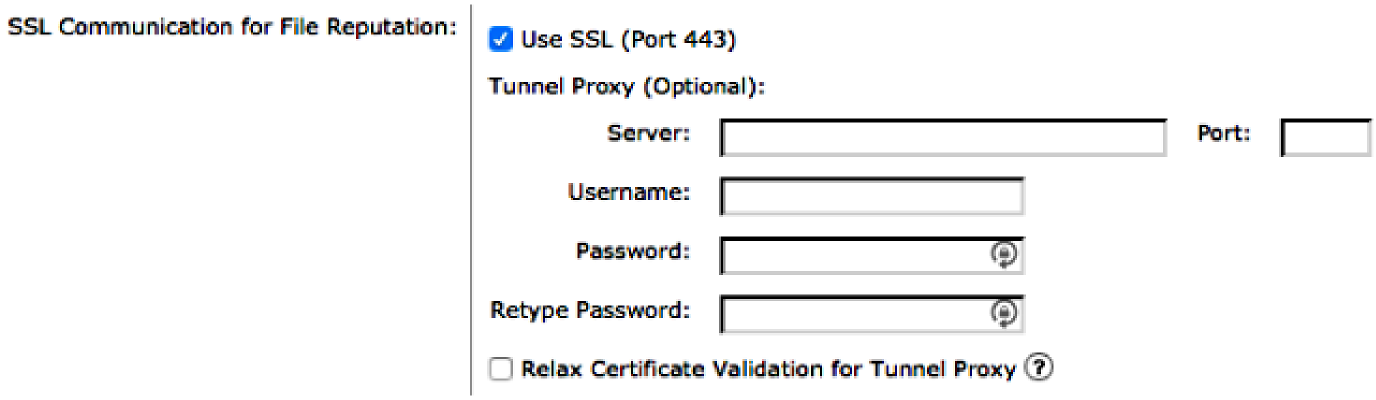
如果是这种情况，ESA管理员可以选择让文件信誉通过端口443进行通信。

要执行此操作，请从CLI运行**ampconfig > advanced**，并确保为**是否要启用SSL通信（端口443）以实现文件信誉？***[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]>
```

如果使用GUI，请选择**Security Services > File Reputation and Analysis > Edit Global Settings > Advanced（下拉列表），并确保选中Use SSL**复选框，如下所示：



SSL Communication for File Reputation:

☑ Use SSL (Port 443)

Tunnel Proxy (Optional):

Server: Port:

Username:

Password:

Retype Password:

☐ Relax Certificate Validation for Tunnel Proxy ?

提交对配置的所有更改。

最后，查看当前的AMP日志，以查看服务和连接是否成功。您可以通过**tail amp**从CLI完成此操作。

在对**ampconfig > advanced**进行更改之前，您会在AMP日志中看到以下内容：

```
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.
```

对**ampconfig > advanced**进行更改后，您将在AMP日志中看到以下内容：

```
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
```

上例中显示的**amp_watchdog.txt**文件每10分钟运行一次，并且将在AMP日志中对其进行跟踪。此文件是AMP的保活文件的一部分。

AMP日志中针对具有文件信誉和文件分析配置文件类型的消息的常规查询类似于以下内容：

```
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
```

使用此日志信息，管理员应该能够关联邮件日志中的邮件ID(MID)。

故障排除

检查防火墙和网络设置，以确保为以下各项打开SSL通信：

端口	协议	输入/输出	主机名	描述
443	TCP	出站	如在“安全服务”(Security Services)>“文件信誉和分析”(File Reputation and Analysis)的“高级”(Advanced)部分中所配置。	访问云服务进行文件分
32137	TCP	出站	如在“安全服务”(Security Services)>“文件信誉和分析”(File Reputation and Analysis)、“高级”(Advanced)部分、“高级”(Advanced)部分、“云服务器池”(Cloud Server Pool)参数中所配置。	访问云服务以获取文件 。

您可以通过Telnet测试从ESA到443以上云服务的基本连接，以确保设备可以成功访问AMP服务、文件信誉和文件分析。

> **注意**：文件信誉和文件分析的地址在CLI上使用**ampconfig > advanced配置，或者从GUI使用Security Services > File Reputation and Analysis > Edit Global Settings > Advanced（下拉列表）配置**。

注意：如果在ESA和文件信誉服务器之间使用隧道代理，可能需要启用“放宽隧道代理的证书验证”选项。如果隧道代理服务器的证书未由ESA信任的根颁发机构签名，则提供此选项以跳过标准证书验证。例如，如果在受信任的内部隧道代理服务器上使用自签名证书，请选择此选项。

文件信誉示例：

```
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.
```

文件分析示例：

```
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.
```

如果ESA能够telnet到文件信誉服务器，并且没有解密连接的上游代理，则可能需要向Threat Grid重新注册设备。在ESA CLI上，有一个隐藏命令：

```
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.
```

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）。