与AMP的ESA接收" 文件名誉服务不是reachable"错误

目录

简介

本文描述警报归因于Cisco电子邮件安全工具(ESA)有先进的恶意软件保护的(AMP)启用，其中服务无法在文件名誉的端口32137或443通信。

更正“文件名誉服务不是为AMP接收的可及的”错误

AMP发布为在ESA的使用在电子邮件安全的AsyncOS版本8.5.5。 当AMP准许和启用在ESA，管理员收到此消息：

```
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服务在网络也许启用，但是很可能不通信通过文件名誉的端口32137。

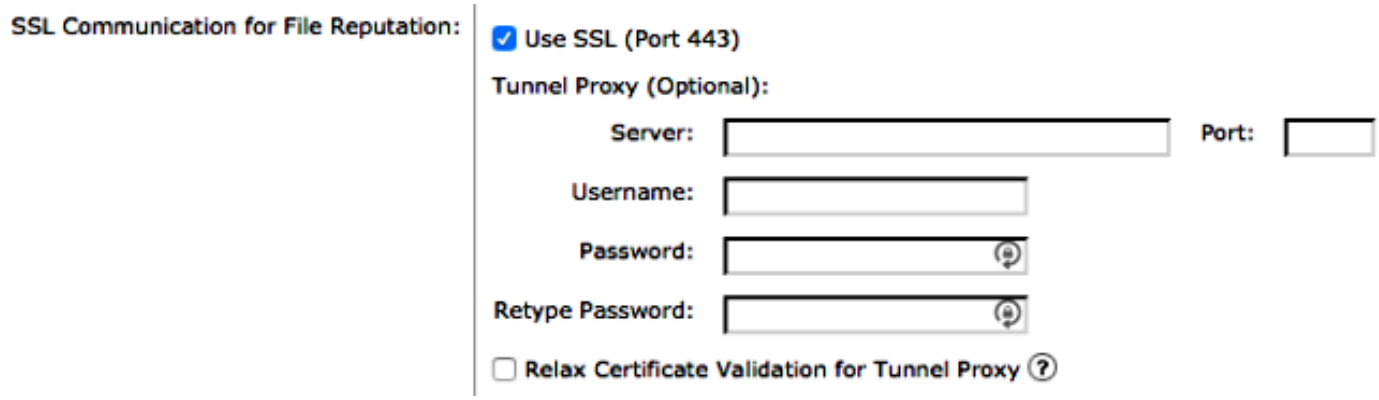
如果那是实际情形， ESA管理员能选择安排文件名誉在端口443通信。

为了执行如此，从CLI运行**ampconfig >提前**并且请务必**Y**选择为*您要启用SSL通信(端口443)文件名誉的？[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**安全服务>文件名誉和分析> Edit全局设置>Advanced (下拉式)**并且保证**使用SSL**复选框被检查如显示此处：



确认对配置的任意更改。

最后，请查看当前AMP登录顺序发现服务和连接成功或者失败。您能从与**尾标amp.的**CLI完成此。

在做的变动之前对**ampconfig >**在AMP日志**提前**，您将看到此：

```
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.
```

在变动做对**ampconfig >先进后**，您在AMP日志看到此：

```
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
```

如前一个示例所显示的**amp_watchdog.txt**文件在AMP日志将运行每10分钟和被跟踪。此文件是一部分的keep-alive AMP的。

在AMP日志的一正常查询与已配置的文件类型的一个消息文件名誉和文件分析的类似于此：

```
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
```

有此日志信息，管理员应该能关联消息ID (MID)在邮件日志。

故障排除

查看防火墙和网络设置为了保证SSL通信为这些打开：

端口	协议 In/out	主机名	说明
443	TCP	如安全服务>文件名誉和分析所配置的一样，Advanced部分。	覆盖文件分析的服务的访问。
32137	TCP	如安全服务>文件名誉和分析所配置的一样，Advanced部分，Advanced部分，Cloud服务器池参数。	覆盖服务的访问为了得到文件

您能测试从您的ESA的基本连通性到网云服务443通过Telnet为了保证您的设备能成功地到达AMP服务、文件名誉和文件分析。

> **Note**: 文件名誉和文件分析的地址在CLI配置与**ampconfig >先进**或从与**安全服务>文件名誉和分析> Edit全局设置>Advanced的**GUI **(下拉式)**。

> **Note**:如果使用在ESA和文件名誉服务器之间的一个通道代理，您会要求启用选项放松通道代理的证书确认。 如果通道代理服务器的证书没有由ESA，委托的根权限签字此选项提供跳过标准的证书确认。例如，请选择此选项，如果曾经在委托内部通道代理服务器的一自签名证书。

文件名誉示例：

```
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.
```

相关信息

- ESA提前的恶意软件保护(AMP)测验
- ESA用户指南
- ESA FAQ ：什么是消息ID (MID)，射入连接ID (ICID)，或者交付连接ID (DCID) ？
- 如何搜索，并且查看邮件注册ESA ？
- 技术支持和文档 - Cisco Systems