与安培的ESA得到“在网云的文件名誉服务是不可得到的”错误

目录

简介

本文描述警报归因于思科电子邮件安全工具(ESA)有先进的恶意软件保护的(安培)启用，其中服务不在文件名誉的端口32137通信。

更正在网云的“文件名誉服务是为安培接收的不可得到的”错误

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

```
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
```

安培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。

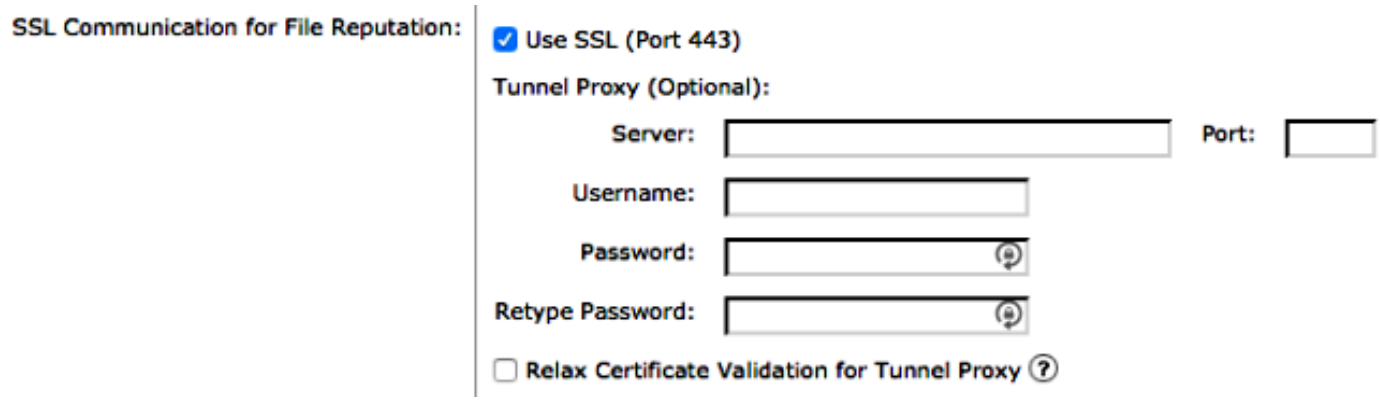
如果那是实际情形， ESA管理员能选择安排文件名誉在端口443通信。

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] >* ：

```
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
```

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，请查看当前安培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 >**在安培日志**提前**，您将看到此：

```
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
```

在变动做对**ampconfig >先进后**，您在安培日志看到此：

```
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
```

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

在安培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：

```
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
```

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：

波尔特	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名

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安培服务、文件名誉和文件分析。

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

文件名誉示例：

```
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
```

文件分析示例：

```
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
```

相关信息

- ESA提前的恶意软件保护(安培)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