具有AMP的ESA收到「檔案信譽服務無法訪問」錯誤

目錄

簡介
更正AMP收到的「The File Reputation service is not reachable」錯誤
疑難排解
相關資訊

簡介

本檔案介紹歸因於已啟用進階惡意軟體防護(AMP)的思科電子郵件安全裝置(ESA)的警報，其中服務無法透過連線埠32137或443通訊檔案信譽。

更正AMP收到的「The File Reputation service is not reachable」錯誤

AMP在AsyncOS版本8.5.5中發佈用於郵件安全。 在ESA上許可並啟用AMP後，管理員會收到以下消息：

```
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服務可能已啟用，但可能不會通過檔案信譽的埠32137在網路上通訊。

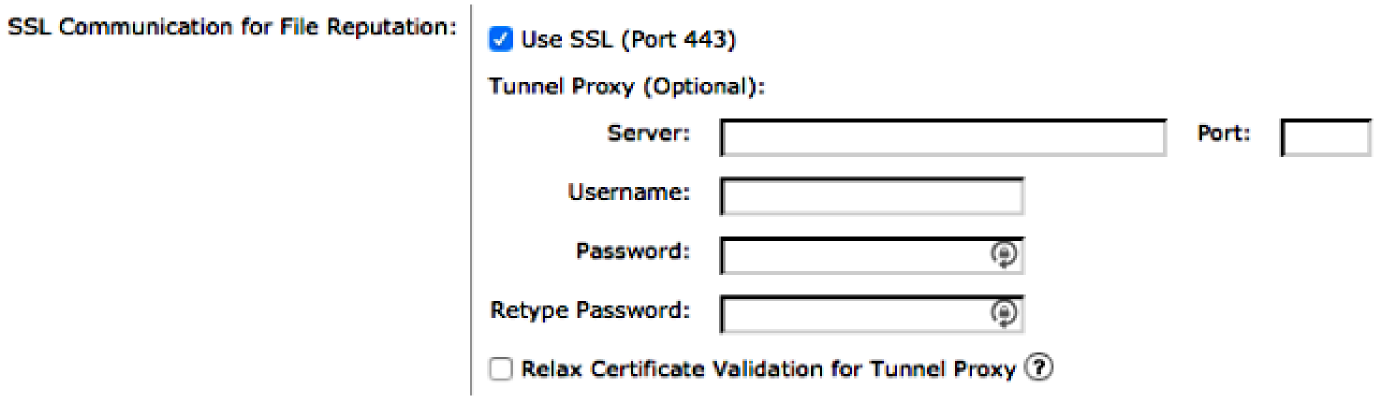
如果是這種情況，ESA管理員可以選擇讓檔案信譽通過埠443進行通訊。

若要執行此操作，請從CLI運行**ampconfig > advanced**，並確保為**Do you want to enable SSL communication(port 443)for file reputation？（是否要為檔案信譽啟用SSL通訊（埠443）？）***[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，請選擇**Security Services > File Reputation and Analysis > Edit Global Settings > Advanced（下拉選單），並確保選中Use SSL**覈取方塊，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 ?

提交對配置所做的所有更改。

最後，檢視當前的AMP日誌，以檢視服務和連線的成敗。您可以通過尾部放大器從CLI完成**此操作**
。

對**ampconfig > advanced**進行變更之前，您應該已經在AMP日誌中看到以下內容：

```
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.
```

對**ampconfig > advanced**進行變更後，您可以在AMP記錄中看到以下內容：

```
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
```

上例中顯示的**amp_watchdog.txt**檔案將每10分鐘運行一次，並在AMP日誌中進行跟蹤。此檔案是AMP的keep-alive的一部分。

AMP日誌中針對檔案信譽和檔案分析配置檔案型別的消息的常規查詢類似於以下內容：

```
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
```

使用此日誌資訊，管理員應該能夠關聯郵件日誌中的郵件ID(MID)。

疑難排解

檢查防火牆和網路設定，以確保為以下各項開啟SSL通訊：

連接埠	通訊協定	輸入/輸出	主機名	說明
443	TCP	外寄	如在「安全服務」>「檔案信譽和分析」、「高級」部分中配置。	訪問雲服務以進行檔案。
32137	TCP	外寄	如在「安全服務」>「檔案信譽和分析」、「高級」部分、「高級」部分、「雲伺服器池」引數中配置。	訪問雲服務以獲取檔案。

您可以通過Telnet測試從ESA到443以上雲服務的基本連線，以確保您的裝置能夠成功訪問AMP服務、檔案信譽和檔案分析。

> **注意**：檔案信譽和檔案分析的地址在CLI上使用**ampconfig > advanced**配置，或者在GUI上使用**Security Services > File Reputation and Analysis > Edit Global Settings > Advanced（下拉選單）配置**。

附註：如果在ESA和檔案信譽伺服器之間使用隧道代理，可能需要啟用放寬隧道代理的證書驗證選項。如果隧道代理伺服器的證書未由ESA信任的根頒發機構簽名，則提供此選項以跳過標準證書驗證。例如，如果在受信任的內部隧道代理伺服器上使用自簽名證書，請選擇此選項。

檔案信譽示例：

```
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.
```

檔案分析示例：

```
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能夠telnet到檔案信譽伺服器，並且沒有解密連線的上游代理，則可能需要向Threat Grid重新註冊裝置。在ESA CLI上，有一個隱藏的命令：

```
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.
```

相關資訊

- ESA高級惡意軟體防護(AMP)測試
- ESA使用手冊
- ESA常見問題：什麼是消息ID(MID)、注入連線ID(ICID)或傳遞連線ID(DCID)?
- 如何搜尋和檢視ESA上的郵件日誌？
- 技術支援與文件 - Cisco Systems

關於此翻譯