AMPを使用したESAで「The File Reputation service is not reachable」エラーが表示される

内容

概要

このドキュメントでは、Advanced Malware Protection(AMP)が有効になっているCisco Eメールセキュリティアプライアンス(ESA)に起因するアラートについて説明します。ESAでは、ファイルレピュテーションのポート32137または443を介してサービスが通信できません。

AMPに対して受信した「The File Reputation service is not reachable」エラーの修正

AMPは、AsyncOSバージョン8.5.5のESAでEメールセキュリティ用にリリースされました。 ESAでAMPのライセンスを取得して有効にすると、管理者は次のメッセージを受信します。

```
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サービスは有効になっていても、ファイルレピュテーションのポート32137を介してネットワーク上で通信しない可能性があります。

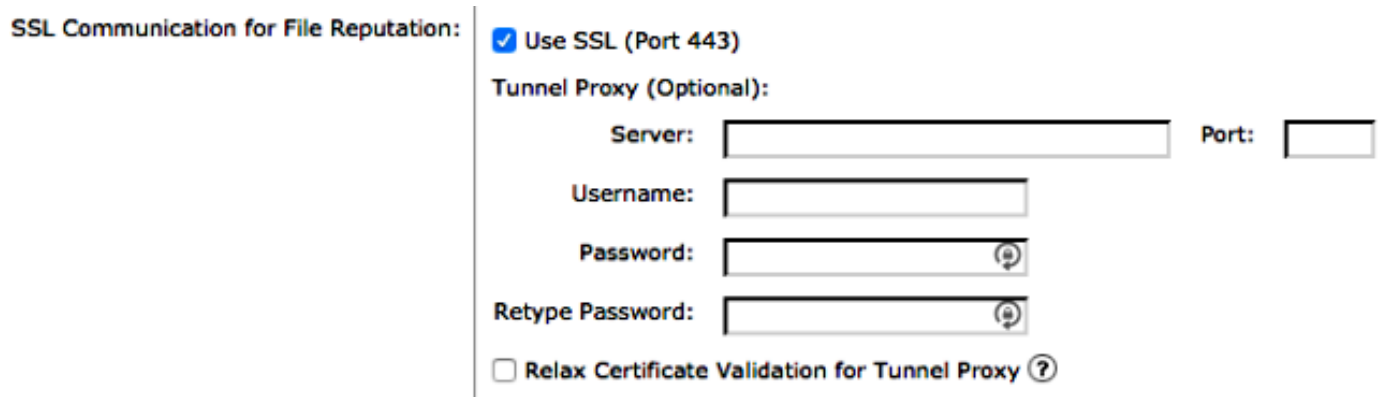
この場合、ESA管理者はファイルレピュテーションをポート443経由で通信するように選択できます。

これを行うには、CLIから**ampconfig > advanced**を実行し、[Do you want to enable SSL communication (port 443) for file reputation?] に[Y] が選択されていることを確認します。*[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]>
```

GUIを使用する場合は、[Security Services] > [File Reputation and Analysis] > [Edit Global Settings] > [Advanced] (ドロップダウン) の順に選択し、[Use SSL] チェックボックスが次のようにオンになっていることを確認します。



設定に対するすべての変更を**コミット**します。

最後に、現在のAMPログを確認して、サービスと接続の成功または失敗を確認します。これは、**tail amp**を使用してCLIから実行できます。

ampconfig > advancedに変更を加える前は、AMPログに次のように記録されていました。

```
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.
```

ampconfig > advancedに変更を加えると、AMPログに次のように表示されます。

```
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
```

前の例に示した**amp_watchdog.txt**ファイルは10分ごとに実行され、AMPログで追跡されます。このファイルは、AMPのキープアライブの一部です。

ファイルレピュテーションとファイル分析のファイルタイプが設定されたメッセージに対するAMPログの通常のクエリーは、次のようになります。

```
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
```

このログ情報を使用して、管理者はメールログのメッセージID(MID)を関連付けることができます。

トラブルシュート

ファイアウォールとネットワークの設定を見直して、次のSSL通信が開いていることを確認します。

ポート	プロトコル	イン/アウト	[hostname]	説明
443	TCP	アウト	[セキュリティサービス(Security Services)] > [ファイルレピュテーションと分析(File Reputation and Analysis)]の[詳細(Advanced)]セクションで設定します。	ファイル分析のためのウドサービスへのア。
32137	TCP	アウト	[Security Services] > [File Reputation and Analysis]、[Advanced]セクション、[Advanced]セクション、[Cloud Server Pool]パラメータで設定します。	ファイルレピュテーを取得するためのクサービスへのアクセ

アプライアンスがAMPサービス、ファイルレピュテーション、およびファイル分析に正常に到達できることを確認するために、Telnetを介して443を介してESAからクラウドサービスへの基本的な接続をテストできます。

> **注**：ファイルレピュテーションとファイル分析のアドレスは、CLIで**ampconfig > advanced**を使用して設定するか、GUIから**Security Services > File Reputation and Analysis > Edit Global Settings > Advanced（ドロップダウン）**を使用して設定します。

> **注**：ESAとファイルレピュテーションサーバの間でトンネルプロキシを使用する場合、トンネルプロキシの証明書検証をリラックスするオプションを有効にする必要がある場合があります。このオプションは、トンネルプロキシサーバの証明書がESAによって信頼されるルート機関によって署名されていない場合に、標準の証明書検証をスキップするために提供されます。たとえば、信頼できる内部トンネルプロキシサーバで自己署名証明書を使用する場合は、このオプションを選択します。

ファイルレピュテーションの例：

```
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.
```

ファイル分析の例：

```
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.
```

ESAがファイルレピュテーションサーバにTelnet接続でき、接続を復号化するアップストリームプロキシがない場合は、アプライアンスをThreat Gridに再登録する必要があります。ESA CLIには隠しコマンドがあります。

```
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.
```

関連情報

- ESA の Advanced Malware Protection (AMP) のテスト
- ESAユーザガイド
- ESA に関する FAQ：メッセージ ID (MID)、インジェクション接続 ID (ICID)、または送信接続 ID (DCID) とは何ですか。
- ESA でメール ログを検索して表示するにはどうしますか。
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。