アラートメッセージのトラブルシューティング：更新に失敗しました

内容

はじめに

このドキュメントでは、アップデート障害に関連するアラートの特定、トラブルシューティング、および解決について説明します。

著者：シスコテクニカルリーダー、Dennis McCabe Jr

前提条件

要件

Cisco Secure Email GatewayまたはCisco Secure Email Cloud Gatewayに関する基本的な知識があることが推奨されます。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

いずれかのスキャンエンジンでアップデートが3回以上失敗すると、アラートが送信されます。次に、Graymailが更新を正常に完了できなかった場合の例を示します。

```
The graymail application tried and failed 3 times to successfully complete an update.
```

特定

この問題を特定するには、最初に、アップデートの失敗に関するアラートが引き続き表示されていることを確認します。このために、CLIからdisplayalertsコマンドを実行できます。

```
<#root>

(esa.example.local) (SERVICE)>

displayalerts


Date and Time Stamp Description
--------------------------------------------------------------------------------
22 Nov 2024 12:00:00 +0300 The graymail application tried and failed 3 times to successfully complete a

outage.
```

そこから、CLIからupdater_logsを確認して、最後の障害がいつ発生したかを確認できます。

```
<#root>

esa.example.local (SERVICE)>

grep -i "update failed" updater_logs


Fri Nov 22 12:00:00 2024 Warning: graymail update failed
```

最後の障害が少し前のものであった場合、ネットワーク遅延が原因である可能性があり、アラートは無視しても問題ありません。

さらに確実に更新するために、最後にCLIからenginestatus allコマンドを実行して、エンジンとルールが実際に正常に更新されていることを確認できます。エンジンの更新頻度はルールよりも少ないことに注意してください。したがって、最近の5 ~ 10分以内にルールが最終更新されたことが確認できますが、最後のエンジン更新から数日または数週間かかる可能性があります。

```
<#root>
```

```
(Machine esa.example.local)>
```

enginestatus all

```
Component      Version      Last Updated      File      Version
CASE Core Files 3.13.2-045 14 Nov 2024 04:06 (GMT +00:00) 1731414068326236
CASE Utilities 3.13.2-045 14 Nov 2024 04:06 (GMT +00:00) 1731414072027229
Structural Rules 3.13.2-20241121_201008 21 Nov 2024 23:30 (GMT +00:00) 1732231660607257
Web Reputation DB 20241016_150447 14 Nov 2024 04:06 (GMT +00:00) 1729091106299038
Web Reputation DB Update 20241016_150447-20241016_150447 14 Nov 2024 04:06 (GMT +00:00) 172909110643616
Content Rules 20241122_021309 22 Nov 2024 02:15 (GMT +00:00) 1732241625451653
Content Rules Update 20241122_022837 22 Nov 2024 02:30 (GMT +00:00) 1732242536816053
Bayes DB 20241122_004336-20241122_013648 22 Nov 2024 01:40 (GMT +00:00) 1732239454073553

SOPHOS Status: UP CPU: 0.0% RAM: 396M
Component Version Last Updated File Version
Sophos Anti-Virus Engine 3.2.07.392.0_6.12 14 Nov 2024 04:06 (GMT +00:00) 1729232666
Sophos IDE Rules 2024112103 21 Nov 2024 22:55 (GMT +00:00) 1732228972

GRAYMAIL Status: UP CPU: 0.0% RAM: 280M
Component Version Last Updated File Version
Graymail Engine 01.430.00 Never updated 143000
Graymail Rules 01.431.37#45 22 Nov 2024 02:25 (GMT +00:00) 1709881322
Graymail Tools 8.0-006 Never updated 1110080006

MCAFEE Status: UP CPU: 0.0% RAM: 670M
Component Version Last Updated File Version
McAfee Engine 6700 Never updated 6700
McAfee DATs 11263 21 Nov 2024 11:29 (GMT +00:00) 1732187479

AMP Status: UP CPU: 0.0% RAM: 163M
Component Version Last Updated File Version
AMP Client Settings 15.0.0-006 14 Nov 2024 04:06 (GMT +00:00) 100110
AMP Client Engine 1.0 Never updated 10
```

解決中

ネットワーク接続

それでも障害が発生する場合は、さらにトラブルシューティングを進めるために実施できる作業がいくつかあります。

1. ビルドに一致する各AsyncOSバージョン内のファイアウォールインデックスを確認し、基本的なネットワーク接続テストをいくつか実行します。ここでは、正常な接続セッションを示すTelnetテストをいくつか示します。これについて見ていきましょう。
    1. AsyncOS 16.0用に利用可能なものについては、ここをクリックしてください。
2. これらのテストの1つ以上が失敗した場合は、ネットワークでこのトラフィックの発信が許可されていることを確認してから、再試行する必要があります。

<#root>

```
(Machine esa.example.local)>
telnet updates.ironport.com 80


Trying 23.62.46.116...
Connected
 to a23-62-46-116.deploy.static.akamaitechnologies.com.
(Machine esa.example.local)>
telnet downloads.ironport.com 80


Trying 96.16.55.20...
Connected
 to a96-16-55-20.deploy.static.akamaitechnologies.com.
(Machine esa.example.local)>
telnet update-manifests.ironport.com 443


Trying 208.90.58.5...
Connected
 to update-manifests.ironport.com.
(Machine esa.example.local)>
telnet update-manifests.sco.cisco.com 443


Trying 208.90.58.6...
Connected
 to update-manifests.sco.cisco.com.
```

マニフェストサーバーの使用状況

1. update-manifests.ironport.comは物理アプライアンスに使用され、update-manifests.sco.cisco.comは仮想アプライアンスに使用されることに注意してください。正しいホストが使用されていることを確認するには、updateconfigコマンドを実行し、続けてdynamichostを実行します。これが正しくない場合は、hostname:portが正しいことを確認してから、変更をコミットして保存します。

```
<#root>
(Cluster esa.lab)>
updateconfig
```

```
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- CLUSTERSET - Set how updates are configured in a cluster
- CLUSTERSHOW - Display how updates are configured in a cluster
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]>
```

dynamichost

```
This command is restricted to "machine" mode. Would you like to switch to "machine" mode? [Y]>

Choose a machine.
1. esa1.lab.local
2. esa2.lab.local
[1]>

Enter new manifest hostname:port
[
```

update-manifests.sco.cisco.com:443

```
]>
```

この手順を実行してもアップデートの失敗が発生する場合は、Cisco TACケースのオープンに進んでください。サポートが必要です。

関連情報

- Cisco Secure Email Cloud Gatewayエンドユーザガイド
- Cisco Secure Email Gatewayエンドユーザガイド
- シスコのテクニカルサポートとダウンロード

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。