警報消息故障排除 — 更新失敗

目錄

簡介

本文檔介紹與更新失敗相關的警報的識別、故障排除和解決。

作者：思科技術主管Dennis McCabe Jr。

必要條件

需求

思科建議您基本瞭解思科安全電子郵件網關或思科安全電子郵件雲網關。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

當其中一個掃描引擎的更新失敗了3次或更多次時，將傳送警報。以下是未能成功完成更新的Graymail示例。

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

識別

要識別此問題，我們可以首先確認我們仍然收到有關更新失敗的警報。為此，我們可以從CLI運行displayalerts命令。

```
<#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.
```

然後，我們可以在此處檢視CLI中的updater_logs，以確認上次故障發生的時間。

```
<#root>

esa.example.local (SERVICE)>

grep -i "update failed" updater_logs


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

如果上一次故障發生在稍早之前，那麼很可能是由於網路延遲過長，因此可以安全地忽略警報。

為了進一步確保安全，我們最終可以從CLI運行enginestatus all命令，並確認引擎和規則確實已成功更新。請注意，引擎更新頻率低於規則。因此，雖然您可以看到規則上次更新是在最近5-10分鐘內，但是它可能是在引擎上次更新後的幾天或幾週內。

```
<#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

網路連線

如果故障仍然存在，我們可以做一些進一步故障排除的事情。

1. 檢視與您的構建相匹配的各個AsyncOS版本中的防火牆索引，並執行一些基本的網路連線測試。此處我們通過一些telnet測試顯示了成功的Connected會話，這正是我們所尋求的。
    1. 按一下此處，獲取可用於AsyncOS 16.0的版本
2. 如果其中一個或多個測試失敗，則必須確保您的網路已允許此流量出站並重試。

<#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.
```

清單伺服器使用情況

1. 請注意，update-manifests.ironport.com用於物理裝置，update-manifests.sco.cisco.com用於虛擬裝置。要確保正確的主機正在使用中，我們可以運行updateconfig命令，然後運行dynamichost。如果不正確，請確保更正hostname:port，然後提交並儲存更改。

```
<#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

```
]>
```

如果您已經完成這些步驟並且仍然遇到更新失敗，請繼續開啟Cisco TAC案例，我們可以為您提供幫助。

相關資訊

- Cisco Secure Email Cloud Gateway最終使用手冊
- Cisco Secure Email Gateway最終使用手冊
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。