排除安全电子邮件故障"；更新失败"风险通告

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

识别

分辨率

- 网络连接
- 清单服务器使用情况

相关信息

简介

本文档介绍与更新失败相关的风险通告的识别、故障排除和解决。

先决条件

要求

思科建议您对思科安全邮件网关或思科安全邮件云网关有基本的了解。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

当其中一个扫描引擎的更新失败3次或更多次时，将发送警报。AMP、Case、Graymail、McAfee和

Sophos可能会出现失败警报。以下是Graymail未能成功完成更新的示例。

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

识别

要识别此问题，您可以首先确认您仍然收到有关更新失败的警报。为此，您可以从CLI运行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.
```

然后，您可以从CLI查看updater_logs以确认上次故障发生的时间。

```
<#root>

esa.example.local (SERVICE)>

grep -i "update failed" updater_logs



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

如果上一次故障发生在稍早之前，则很可能是因为网络延迟，因此可以安全地忽略警报。

您最终可以从CLI运行enginestatus all命令，并确认引擎和规则确实已成功更新。请注意，引擎的更新频率低于规则。因此，虽然您可以看到规则上一次更新是在最近5-10分钟内，但是它可能要比上次引擎更新晚几天或几周。

```
<#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
```

分辨率

网络连接

如果仍然发生故障，您可以做一些进一步排除故障的工作。

1. 查看与您的版本相匹配的相应AsyncOS版本中的防火墙索引，并执行一些基本网络连接测试。这里有一些Telnet测试显示了成功的Connected会话，这正是您要查找的内容。
    1. 有关可用于AsyncOS 16.0的指南，请参阅AsyncOS 16.0 for Cisco Secure Email Gateway - GD(General Deployment)。
2. 如果一个或多个测试失败，则必须确保您的网络已允许此流量出站并重试。

<#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.
```

清单服务器使用情况

注意：update-manifests.ironport.com用于物理设备while update-manifests.sco.cisco.com用于虚拟设备。要确保使用正确的主机，可以运行updateconfig命令，然后运行dynamichost。如果不正确，请确保更正hostname:port，然后提交并保存更改。

<#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


]>
```

如果您已经完成这些步骤并且仍然遇到更新失败，请继续提交思科TAC支持请求，请联系支持部门。

相关信息

- 思科安全电邮云网关最终用户指南
- 思科安全邮件网关最终用户指南

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。