Resolución de problemas de mensaje de alerta: actualización fallida

Contenido

Introducción

Este documento describe la identificación, solución de problemas y resolución de alertas relacionadas con fallas de actualización.

Colaboración de Dennis McCabe Jr, líder técnico de Cisco.

Prerequisites

Requirements

Cisco recomienda tener conocimientos básicos de Cisco Secure Email Gateway o Cisco Secure Email Cloud Gateway.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Se envía una alerta cuando una actualización ha fallado 3 o más veces para uno de los motores de análisis. Este es un ejemplo de error de Graymail al completar con éxito una actualización.

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

Identificar

Para identificar este problema, en primer lugar podemos confirmar que seguimos recibiendo alertas sobre fallos de actualización. Para esto, podemos ejecutar el comando displayalerts desde la CLI.

<#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.
```

A partir de ahí, podemos revisar los updater_logs desde la CLI para confirmar cuándo ocurrió el último error.

<#root>

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

grep -i "update failed" updater_logs

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

Si la última falla se produjo hace un tiempo, es probable que se deba a un poco de latencia de red y que la alerta se pueda ignorar de forma segura.

Para mayor seguridad, finalmente podemos ejecutar el comando enginestatus all desde la CLI y confirmar que los motores y las reglas se están actualizando con éxito. Tenga en cuenta que los motores se actualizan con menos frecuencia que las reglas. Por lo tanto, aunque puede ver las reglas actualizadas por última vez en los últimos 5-10 minutos, podrían pasar unos días o

semanas desde la última actualización del motor.

<#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
```

Resolviendo

Conectividad de red

Si los fallos siguen produciéndose, hay algunas cosas que podemos hacer para solucionar los problemas.

1. Revise el índice de firewall en la versión de AsyncOS correspondiente a su compilación y realice algunas pruebas básicas de conectividad de red. Aquí tenemos algunas pruebas de Telnet que muestran sesiones conectadas exitosas, que es lo que buscamos.
    1. Haga clic aquí para ver uno que tenemos disponible para AsyncOS 16.0
2. Si una o más de estas pruebas fallan, debe asegurarse de que su red ha permitido este

tráfico saliente e intentarlo de nuevo.

```
<#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.
```

Uso del servidor de manifiestos

1. Tenga en cuenta que update-manifiests.ironport.com se utiliza para los dispositivos físicos, mientras que update-manifiests.sco.cisco.com se utiliza para los dispositivos virtuales. Para asegurarnos de que el host correcto está en uso, podemos ejecutar el comando updateconfig seguido de dynamic host. Si es incorrecto, asegúrese de corregir el nombre de host:puerto y, a continuación, confirme y guarde los cambios.

<#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

```
]>
```

Si ha seguido los pasos y sigue experimentando errores de actualización, continúe con la apertura de un caso de Cisco TAC y podremos ayudarle.

Información Relacionada

- Guías para usuarios finales de Cisco Secure Email Cloud Gateway
- Guías para usuarios finales de Cisco Secure Email Gateway
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).