Solucionar problemas de mensagem de alerta - Falha na atualização

Contents

[Introdução](#)

[Pré-requisitos](#)

- [Requisitos](#)
- [Componentes Utilizados](#)

[Informações de Apoio](#)

[Identificar](#)

[Resolvendo](#)

- [Conectividade de rede](#)
- [Uso do Servidor de Manifesto](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como identificar, solucionar problemas e resolver alertas relacionados a falhas de atualização.

Contribuição de Dennis McCabe Jr, líder técnico da Cisco.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha uma compreensão básica do Cisco Secure Email Gateway ou do Cisco Secure Email Cloud Gateway.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Um alerta é enviado quando uma atualização falha 3 ou mais vezes em um dos mecanismos de varredura. Este é um exemplo de falha do Graymail ao concluir uma atualização com êxito.

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

Identificar

Para identificar esse problema, primeiro podemos confirmar que ainda estamos recebendo alertas sobre falhas de atualização. Para isso, podemos executar o comando displayalerts na 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 daí, podemos revisar os updater_logs da CLI para confirmar quando ocorreu a última falha.

```
<#root>

esa.example.local (SERVICE)>

grep -i "update failed" updater_logs


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

Se a última falha ocorreu há algum tempo, provavelmente foi devido a um pouco de latência de rede, e o alerta pode ser ignorado com segurança.

Para obter mais garantias, podemos finalmente executar o comando enginestatus all a partir da CLI e confirmar que os mecanismos e as regras estão realmente sendo atualizados com sucesso. Observe que os mecanismos são atualizados com menos frequência do que as regras. Embora você possa ver as regras atualizadas pela última vez nos últimos 5 a 10 minutos, pode levar alguns dias ou semanas desde a última atualização do mecanismo.

<#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
```

Resolvendo

Conectividade de rede

Se as falhas ainda estiverem ocorrendo, há algumas coisas que podemos fazer para solucionar os problemas.

1. Examine o Índice do Firewall na respectiva versão do AsyncOS correspondente à sua compilação e execute alguns testes básicos de conectividade de rede. Aqui temos alguns testes de telnet mostrando sessões conectadas bem-sucedidas, que é o que estamos procurando.
    1. Clique aqui para um que está disponível para o AsyncOS 16.0
2. Se um ou mais desses testes estiverem falhando, verifique se a rede permitiu o tráfego de saída e tente novamente.

<#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 do Servidor de Manifesto

1. Observe que update-manifests.ironport.com é usado para dispositivos físicos enquanto update-manifests.cisco.com é usado por virtuals. Para certificar-se de que o host correto esteja em uso, podemos executar o comando updateconfig seguido por dynamichost. Se estiver incorreto, certifique-se de corrigir o nome do host:porta e, em seguida, confirme e salve suas alterações.

<#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

```
]>
```

Se você passou pelas etapas e ainda está enfrentando falhas de atualização, prossiga com a abertura de um caso do Cisco TAC e nós podemos ajudá-lo.

Informações Relacionadas

- Guias do usuário final do Cisco Secure Email Cloud Gateway
- Guias do usuário final do Cisco Secure Email Gateway
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.