Dépannage de la messagerie sécurisée " ; Echec de la mise à jour" ; Alertes

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Identifier

Résolution

- Connectivité du réseau
- Utilisation du serveur manifeste

Informations connexes

Introduction

Ce document décrit l'identification, le dépannage et la résolution des alertes relatives aux échecs de mise à jour.

Conditions préalables

Exigences

Cisco recommande que vous ayez une compréhension de base de la passerelle de messagerie sécurisée Cisco ou de la passerelle de cloud de messagerie sécurisée Cisco.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Une alerte est envoyée lorsqu'une mise à jour a échoué 3 fois ou plus pour l'un des moteurs d'analyse. Les alertes en cas d'échec peuvent concerner AMP, Case, Graymail, McAfee et Sophos. Voici un exemple de l'échec de mise à jour de Graymail.

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

Identifier

Pour identifier ce problème, vous pouvez d'abord confirmer que vous recevez toujours des alertes concernant des échecs de mise à jour. Pour cela, vous pouvez exécuter la commande displayalerts à partir de l'interface de ligne de commande.

<#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.
```

À partir de là, vous pouvez ensuite examiner les journaux de mise à jour à partir de l'interface de ligne de commande pour confirmer quand la dernière défaillance s'est produite.

<#root>

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

grep -i "update failed" updater_logs



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

Si la dernière panne remonte à un certain temps, il est probable qu'elle soit due à une certaine latence du réseau et que l'alerte puisse être ignorée en toute sécurité.

Vous pouvez enfin exécuter la commande enginestatus all à partir de l'interface de ligne de commande et confirmer que les moteurs et les règles sont effectivement mis à jour avec succès. Notez que les moteurs sont mis à jour moins souvent que les règles. Ainsi, bien que vous puissiez voir les dernières règles mises à jour au cours des 5 à 10 dernières minutes, cela peut prendre quelques jours ou quelques semaines depuis la dernière mise à jour du moteur.

<#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
```

Résolution

Connectivité du réseau

Si les défaillances sont toujours en cours, vous pouvez effectuer quelques opérations pour les dépanner.

1. Vérifiez l'index de pare-feu dans la version AsyncOS correspondante à votre build et effectuez quelques tests de connectivité réseau de base. Voici quelques tests Telnet montrant des sessions connectées réussies, ce qui est ce que vous recherchez.
    1. Reportez-vous au Guide de l'utilisateur d'AsyncOS 16.0 pour Cisco Secure Email Gateway - GD (General Deployment) pour en trouver un disponible pour AsyncOS 16.0.
2. Si un ou plusieurs de ces tests échouent, vous devez vous assurer que votre réseau a autorisé ce trafic sortant et réessayer.

<#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.
```

Utilisation du serveur manifeste



Remarque : update-manifests.ironport.com est utilisé pour les appliances physiques while update-manifests.sco.cisco.com est utilisé par les serveurs virtuels. Pour vous assurer que l'hôte approprié est utilisé, vous pouvez exécuter la commande updateconfig suivie de dynamichost. Si ce n'est pas le cas, assurez-vous de corriger le nom d'hôte : port, puis validez et enregistrez vos modifications.

<#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 vous avez suivi ces étapes et que vous rencontrez toujours des problèmes de mise à jour, veuillez ouvrir un dossier auprès du TAC Cisco, contactez le support.

Informations connexes

- Guides de l'utilisateur final de la passerelle cloud de messagerie sécurisée Cisco
- Guides d'utilisation de la passerelle de messagerie sécurisée Cisco
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.