Dépannage de vESA : impossible de télécharger et d'appliquer les mises à jour antispam ou antivirus

Table des matières

Introduction

Conditions préalables et avertissements

- Exigences
- Composants utilisés
- Remarques importantes

Symptômes

Définition de l'URL d'hôte dynamique correcte

Vérifier la fonctionnalité de mise à jour

Étapes de dépannage

Informations connexes

Introduction

Ce document explique pourquoi vESA ne parvient pas à mettre à jour les moteurs antispam ou antivirus, bien qu'il dispose d'une licence valide.

Conditions préalables et avertissements

Exigences

Familiarisez-vous avec ces produits et concepts :

- Appliance de sécurité de la messagerie (ESA)
- vESA, appliance de sécurité Web virtuelle (vWSA), appliance de gestion de la sécurité virtuelle (vSMA)
- AsyncOS

Composants utilisés

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.

Remarques importantes

- Les appliances matérielles (C190, C195, C390, C395, C690 et C695) doivent utiliser l'URL d'hôte dynamique update-manifests.ironport.com:443 uniquement.
- Utilisez uniquement les URL du serveur de mise à jour intermédiaire si Cisco a configuré l'accès pour une utilisation bêta. Sans licence bêta valide, les mises à jour ne seront pas reçues des serveurs intermédiaires.
- Dans les configurations de cluster avec ESA et vESA, configurez updateconfig au niveau de la machine et confirmez que l'hôte dynamique est défini en conséquence.

Symptômes

vESA ne parvient pas à télécharger ni à appliquer les mises à jour des moteurs antispam ou antivirus, même si leur licence est correcte. Exécution de commandes de mise à jour telles que :

```
> antispamupdate ironport
> antispamupdate ironport force
> antivirusupdate force
> updatenow force
```

ne résout pas le problème. L'examen des journaux avec tail updater_logs affiche des erreurs similaires à :

```
Mon Oct 21 17:48:43 2025 Info: Dynamic manifest fetch failure: Received invalid update manifest respons
```

Cela indique que l'appliance ne peut pas atteindre le manifeste de mise à jour correct à l'URL d'hôte dynamique configurée via la commande updateconfig. La sous-commande dynamichost, disponible dans updateconfig, définit le serveur de mise à jour que l'appliance utilisera.

Définition de l'URL d'hôte dynamique correcte

Configurez l'URL d'hôte dynamique en fonction du type d'appliance et de l'état de support :

1. update-manifests.sco.cisco.com:443
    - À utiliser pour les appliances vESA, vWSA et vSMA.
2. stage-stg-updates.ironport.com:443
    - À utiliser pour les appareils amicaux, virtuels et matériels bêta avec une autorisation explicite Cisco bêta uniquement.

Pour définir l'URL d'hôte dynamique, utilisez la commande updateconfig, accédez à la sous-commande masquée dynamic host, entrez l'hôte et le port souhaités, puis validez les modifications.

<#root>

```
esa.example.com>
```

updateconfig

```
[]>
```

dynamichost

```
Enter new manifest hostname : port
[update-manifests.sco.cisco.com:443]>
```

stage-stg-updates.ironport.com:443

```
[]> <<<HIT RETURN TO GO BACK TO THE MAIN CLI PROMPT>>>

esa.example.com> commit
```

Vérifier la fonctionnalité de mise à jour

Procédez comme suit pour confirmer la mise à jour de l'appliance à partir de l'URL d'hôte dynamique correcte :

1. Augmentez le niveau de journal updater_logs pour déboguer afin de capturer l'activité de mise à jour détaillée :

<#root>

```
esa.example.com>
```

logconfig

```
[...]
28.
```

updater_logs

```
 Updater Logs Manual Download None
[...]
[]>
```

edit

```
Enter the number of the log you wish to edit.
[]>
```

28

```
Please enter the name for the log:
[updater_logs]>
Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]>
```

4

```
[...]
esa.example.com>

commit
```

Remarque : Le numéro de journal peut varier sur chaque appliance.

---

2. Exécutez une mise à jour forcée pour tester la connectivité et la fonctionnalité de mise à jour :

<#root>

```
esa.example.com>

updatenow force


Success - Force update for all components requested
```

3. Vérifiez updater_logs pour confirmer une connexion réussie à l'hôte dynamique correct :

```
Mon Oct 21 18:19:12 2025 Debug: Acquiring dynamic manifest from stage-stg-updates.ironport.com:443
```

Étapes de dépannage

1. Vérifiez que la configuration de mise à jour par défaut est utilisée. Si vESA ou son hôte se trouve derrière un pare-feu, assurez-vous que les mises à jour sont configurées pour utiliser un serveur statique, comme décrit dans le document Content Security Appliance Upgrades or Updates with a Static Server.
2. Testez la connectivité à l'URL d'hôte dynamique à l'aide de Telnet pour vérifier l'accessibilité du réseau :
   <#root>

   ```
   esa.example.com>

   telnet

   Please select which interface you want to telnet from.
   1. Auto
   2. Management (172.16.6.165/24: esa-mgmt.example.com)
   3. Data (192.168.1.10/24: esa-data.example.com)
   [1]>
   Enter the remote hostname or IP address.
   []>

   stage-stg-updates.ironport.com
   ```

```
Enter the remote port.
[25]>
```

443

```
Trying 208.90.58.24...
Connected to stage-stg-updates.ironport.com.
Escape character is '^]'.
^] ["CTRL + ]"]
telnet> quit
Connection closed.
```

Informations connexes

- Mises à niveau ou mises à jour de Content Security Appliance avec un serveur statique
- Assistance et documentation techniques - Cisco Systems

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.