le vESA ne peut pas télécharger et appliquer des mises à jour pour le courrier indésirable ou l'antivirus

Contenu

Introduction

Ce document décrit quand une appliance virtuelle de sécurité du courrier électronique (vESA) ne télécharge pas et applique des mises à jour pour l'engine de courrier indésirable de Cisco (CAS) ou l'antivirus de Sophos et/ou de McAfee, quoique l'appliance virtuelle soit autorisée correctement.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Appliance de sécurité du courrier électronique (ESA)
- vESA, appliance virtuelle de sécurité Web (vWSA), appliance virtuelle de Gestion de la sécurité (vSMA)
- AysncOS

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- le vESA, ce exécute AsyncOS 8.0.0 et plus tard
- le vWSA, ce exécute AsyncOS 7.7.5 et plus tard
- le vSMA, ce exécute AsyncOS 9.0.0 et plus tard

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont

démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

le vESA ne peut pas télécharger et appliquer des mises à jour pour le courrier indésirable ou l'antivirus

Quand vous mettez à jour le courrier indésirable ou l'antivirus, les processus ne peuvent pas atteindre et mettre à jour l'engine ou les rulesets de service, même si vous sélectionnez la commande de **force de mise à jour**.

Une de ces commandes pourrait avoir été sélectionnée directement du CLI sur le vESA :

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

Quand vous exécutez des **updater_logs de queue**, les erreurs vues sont semblables à ces derniers :

```
Mon Oct 21 17:48:43 2013 Info: Dynamic manifest fetch failure: Received invalid update manifest
response
```

Ceci indique que l'URL dynamique d'hôte associé avec la configuration de mise à jour ne peut pas atteindre l'updater approprié manifeste correctement. L'URL dynamique d'hôte est placé dans la commande d'**updateconfig**. La commande secondaire, **dynamichost,** est une commande masquée dans l'**updateconfig**, comme mis en valeur ici :

```
myesa.local> updateconfig
Service (images): Update URL:
-------------------------------------------------------------------------------
Feature Key updates http://downloads.ironport.com/asyncos
McAfee Anti-Virus definitions Cisco IronPort Servers
RSA DLP Engine Updates Cisco IronPort Servers
PXE Engine Updates Cisco IronPort Servers
Sophos Anti-Virus definitions Cisco IronPort Servers
IronPort Anti-Spam rules Cisco IronPort Servers
Intelligent Multi-Scan rules Cisco IronPort Servers
Outbreak Filters rules Cisco IronPort Servers
Timezone rules Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades Cisco IronPort Servers
IMS Secondary Service rules Cisco IronPort Servers
Service (list): Update URL:
-------------------------------------------------------------------------------
McAfee Anti-Virus definitions Cisco IronPort Servers
RSA DLP Engine Updates Cisco IronPort Servers
PXE Engine Updates Cisco IronPort Servers
Sophos Anti-Virus definitions Cisco IronPort Servers
IronPort Anti-Spam rules Cisco IronPort Servers
Intelligent Multi-Scan rules Cisco IronPort Servers
Outbreak Filters rules Cisco IronPort Servers
Timezone rules Cisco IronPort Servers
Service (list): Update URL:
-------------------------------------------------------------------------------
Cisco IronPort AsyncOS upgrades Cisco IronPort Servers
Update interval: 5m
```

```
Proxy server: not enabled
HTTPS Proxy server: not enabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
[]> dynamichost

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

Placez l'appliance pour utiliser l'URL dynamique correct d'hôte

Il y a deux l'hôte dynamique différent URLs qui sont utilisés pour des clients basés sur la façon dont ils sont associés par Cisco :

1. update-manifests.sco.cisco.com:443 Utilisation : VESA de client, vWSA, vSMA
2. stage-stg-updates.ironport.com:443 Utilisation : Friendlies, bêtas appliances virtuelles et de matériel

   Remarque: Les appliances de matériel (C1x0, C3x0, C6x0, et X10x0) devraient SEULEMENT utiliser l'URL dynamique d'hôte d'*update-manifests.ironport.com:443*. S'il y a une configuration du cluster avec l'ESA et le vESA, l'**updateconfig** doit être configuré au niveau d'ordinateur et puis confirmer que le **dynamichost** est placé en conséquence.

   Remarque: Les clients devraient seulement utiliser le serveur URLs de mise à jour de mise en place s'ils ont accédé au pré-provisionnement par Cisco pour la bêta utilisation seulement. Si vous n'avez pas un permis valide appliqué pour le bêta usage, votre appliance ne recevra pas des mises à jour des serveurs de mise à jour de mise en place.

Comme suite d'**updateconfig** et de la commande secondaire de **dynamichost**, écrivez l'URL dynamique d'hôte comme nécessaire, retour à la demande principale CLI, et commettez les modifications :

```
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>>>

myesa.local> commit
```

Vérifiez

Afin de vérifier que l'appliance atteint maintenant à l'URL d'hôte et aux mises à jour dynamiques appropriés sont réussie, terminez-vous ces étapes :

1. Augmentez les **updater_logs pour déboguer**.
   ```
   Currently configured logs:> logconfig

   Log Name Log Type Retrieval Interval
   ----------------------------------------------------------------------------
   1. antispam Anti-Spam Logs Manual Download None
   [SNIP FOR BREVITY]
   28. updater_logs Updater Logs Manual Download None
   29. upgrade_logs Upgrade Logs Manual Download None
   Choose the operation you want to perform:
   - NEW - Create a new log.
   ```

```
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]> edit
Enter the number of the log you wish to edit.
[]> 28 [NOTE, log # will be different on a per/appliance basis]
Please enter the name for the log:
[updater_logs]>
Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]> 4
[SNIP FOR BREVITY]

myesa_2.local> commit
```

2. Exécutez une mise à jour de force sur le courrier indésirable (**force d'antispamupdate**) ou l'antivirus (**force d'antivirusupdate**).
```
myesa.local> antivirusupdate force

Sophos Anti-Virus updates:
Requesting forced update of Sophos Anti-Virus.
```
3. En conclusion, les **updater_logs de queue** et s'assurent que l'appliance peut atteindre le dynamichost comme indiqué :
```
Mon Oct 21 18:19:12 2013 Debug: Acquiring dynamic manifest from stage-stg-
updates.ironport.com:443
```

Dépanner

Terminez-vous ces étapes afin de dépanner toutes les questions :

1. Assurez-vous que l'**updateconfig** par défaut est utilisé. Si le vESA ou l'hôte est derrière un Pare-feu, assurez-vous que les mises à jour avec un serveur statique sont en service.
2. Assurez-vous que vous pouvez **telnet à l'**URL dynamique d'hôte comme choisi :
```
> telnet
Please select which interface you want to telnet from.
1. Auto
2. Management (172.16.6.165/24: myesa_2.local)
3. new_data (192.168.1.10/24: myesa.local_data1)
[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 jour ou mises à jour d'appareils de sécurité du contenu avec un serveur statique
- Support et documentation techniques - Cisco Systems