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

Conditions requises

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 :

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

Ceci indique que l'URL dynamique d'hôte associé à 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 :

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 :

- update-manifests.sco.cisco.com:443
- Utilisation : VESA de client, vWSA, vSMA

  Remarque: Les appliances de matériel (C1x0, C3x0, C6x0, et X10x0) devraient SEULEMENT utiliser l'URL dynamique ofupdate-manifests.ironport.com:443 d'hôte. 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.

- stage-stg-updates.ironport.com:443
- Utilisation : Friendlies, bêtas appliances virtuelles et de matériel

  Remarque: Les clients devraient seulement utiliser le serveur URLs de mise à jour de mise en place s'ils ont accédé à preprovisioning 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 :

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 mettre au point**.
2. Exécutez une mise à jour de force sur le courrier indésirable (**force d'antispamupdate**) ou l'antivirus (**force d'antivirusupdate**).
3. En conclusion, les **updater_logs de queue** et s'assurent que l'appliance peut atteindre le dynamichost comme indiqué :

Dépannez

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 :

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