Comment appliquer la solution de contournement pour la mise à niveau échouée de Cisco vESA/vSMA en raison d'une petite taille de partition

Contenu

Introduction

Ce document décrit le processus de remplacement de l'appliance de sécurité de la messagerie virtuelle (vESA) et de l'appliance de gestion de la sécurité virtuelle (vSMA) lorsqu'une mise à niveau échoue en raison d'une petite partition Nextroot.

Défauts connexes pour ESA : CSCvy69068 et SMA : CSCvy69076

Fond

Initialement, les images ESA et SMA virtuelles ont été construites avec une taille de partition Nextroot inférieure à 500M. Au fil des ans, et avec les nouvelles versions d'AsyncOS qui incluent des fonctionnalités supplémentaires, les mises à niveau ont dû utiliser de plus en plus de cette partition tout au long du processus de mise à niveau. Nous commençons maintenant à voir échouer les mises à niveau en raison de cette taille de partition et nous voulions fournir des détails sur la solution, qui est de déployer une nouvelle image virtuelle qui a une taille de partition Nextroot plus grande de 4 Go.

Symptômes

Une ancienne image vESA ou vSMA avec une taille de partition Nextroot inférieure à 500 M peut ne pas être mise à niveau avec les erreurs ci-dessous.

```
...
...
...
Finding partitions... done. Setting next boot partition to current partition as a precaution...
done. Erasing new boot partition... done. Extracting eapp done. Extracting scanerroot done.
Extracting splunkroot done. Extracting savroot done. Extracting ipasroot done. Extracting ecroot
done. Removing unwanted files in nextroot done. Extracting distroot /nextroot: write failed,
filesystem is full
./usr/share/misc/termcap: Write failed
./usr/share/misc/pci_vendors: Write to restore size failed
./usr/libexec/getty: Write to restore size failed
./usr/libexec/ld-elf.so.1: Write to restore size failed
./usr/lib/libBlocksRuntime.so: Write to restore size failed
./usr/lib/libBlocksRuntime.so.0: Write to restore size failed
./usr/lib/libalias.so: Write to restore size failed
./usr/lib/libarchive.so: Write to restore size failed
```

Solution

Pour vous assurer que votre ESA/SMA virtuel peut être mis à niveau, vous devez d'abord vérifier si la taille de partition racine suivante est de 4 Go avec la commande CLI **ipcheck**.

```
(lab.cisco.com) > ipcheck

<----- Snippet of relevant section from the output ----->

  Root                  4GB 7%
  Nextroot 4GB 1%
  Var                   400MB 3%
  Log                   172GB 3%
  DB                    2GB 0%
  Swap                  6GB
  Mail Queue            10GB

<----- End of snippet ----->
```

Si la partition racine suivante est inférieure à 4 Go, procédez comme suit pour migrer votre modèle de machine virtuelle actuel vers une nouvelle image mise à jour.

Étape 1.

Déployez votre nouveau vESA/vSMA

Àpartir des conditions préalables, téléchargez l'image ESA/SMA virtuelle et déployez-la conformément au Guide d'installation de l'appliance virtuelle de sécurité du contenu Cisco.

> **Note**: Le guide d'installation fournit des informations sur DHCP (**interface**) et définissez la passerelle par défaut (**setgateway**) sur votre hôte virtuel, ainsi que sur le chargement du fichier de licence de l'appliance virtuelle. Assurez-vous que vous avez lu et déployé comme indiqué.

Étape 2.

Licence du nouveau vESA/vSMA

Une fois le nouvel ESA ou SMA virtuel déployé, il est temps de charger le fichier de licence. Pour les versions virtuelles, la licence est contenue dans un fichier XML et doit être chargée à l'aide de l'interface de ligne de commande. À partir de l'interface de ligne de commande, vous utiliserez la commande **loadlicense**, puis suivez les instructions pour terminer l'importation de licence.

Si vous avez besoin de plus amples informations sur le chargement ou l'obtention du fichier de licence, vous pouvez consulter l'article suivant : Meilleures pratiques pour les licences Virtual ESA, Virtual WSA ou Virtual SMA.

Étape 3.

Assurez-vous que le nouveau vESA/vSMA a la même version que la version d'origine, si ce n'est pas le cas, vous devez mettre à niveau le vESA/vSMA avec l'ancienne version pour obtenir les deux périphériques sur la même version. Utilisez la commande **upgrade** et suivez les instructions jusqu'à obtenir la version souhaitée.

Étape 4. [Uniquement pour vESA, ignorer pour vSMA]

> **Note**: Dans cette étape, on suppose que vous n'avez pas de cluster existant, dans le cas où il y a déjà un cluster existant dans la configuration actuelle, vous ajoutez simplement le nouveau vESA au cluster pour copier la configuration actuelle, puis vous supprimez cette nouvelle machine pour démarrer le processus de mise à niveau.

Créer un nouveau cluster

Dans le vESA d'origine, exécutez la commande **clusterconfig** pour créer un nouveau cluster.

```
OriginalvESA.local> clusterconfig

Do you want to join or create a cluster?
1. No, configure as standalone.
2. Create a new cluster.
3. Join an existing cluster over SSH.
4. Join an existing cluster over CCS.
[1]> 2

Enter the name of the new cluster.
[]> OriginalCluster.local

Should all machines in the cluster communicate with each other by hostname or by IP address?
1. Communicate by IP address.
2. Communicate by hostname.
[2]> 1

What IP address should other machines use to communicate with Machine C170.local?
1. 10.10.10.58 port 22 (SSH on interface Management)
2. Enter an IP address manually
[]> 1
```

```
Other machines will communicate with Machine C195.local using IP address 10.10.10.58 port 22.
You can change this by using the COMMUNICATION subcommand of the clusterconfig command.
New cluster committed: Sat Jun 08 11:45:33 2019 GMT
Creating a cluster takes effect immediately, there is no need to commit.

Cluster OriginalCluster.local

Choose the operation you want to perform:
- ADDGROUP - Add a cluster group.
- SETGROUP - Set the group that machines are a member of.
- RENAMEGROUP - Rename a cluster group.
- DELETEGROUP - Remove a cluster group.
- REMOVEMACHINE - Remove a machine from the cluster.
- SETNAME - Set the cluster name.
- LIST - List the machines in the cluster.
- CONNSTATUS - Show the status of connections between machines in the cluster.
- COMMUNICATION - Configure how machines communicate within the cluster.
- DISCONNECT - Temporarily detach machines from the cluster.
- RECONNECT - Restore connections with machines that were previously detached.
- PREPJOIN - Prepare the addition of a new machine over CCS.
[]>

(Cluster OriginalCluster.local)>
```

Étape 5. [Uniquement pour vESA, ignorer pour vSMA]

Rejoignez votre nouveau vESA à votre cluster ESA d'origine

Àpartir de l'interface de ligne de commande sur le nouveau vESA, exécutez la commande **clusterconfig > Join an existants...** pour ajouter votre nouveau vESA à votre nouveau cluster configuré sur votre vESA d'origine.

```
NewvESA.cisco.com> clusterconfig

Do you want to join or create a cluster?
1. No, configure as standalone.
2. Create a new cluster.
3. Join an existing cluster over SSH.
4. Join an existing cluster over CCS.
[1]> 3

While joining a cluster, you will need to validate the SSH host key of the remote machine to
which you are joining.  To get the public host key fingerprint of the remote host, connect to
the cluster and run: logconfig -> hostkeyconfig -> fingerprint.

WARNING: All non-network settings will be lost. System will inherit the values set at the group
or cluster mode for the non-network settings. Ensure that the cluster settings are compatible
with your network settings (e.g. dnsconfig settings)

Exception:Centralized Policy, Virus, and Outbreak Quarantine settings are not inherited from the
cluster.  These settings on this machine will remain intact.

Do you want to enable the Cluster Communication Service on ironport.example.com? [N]> n

Enter the IP address of a machine in the cluster.
[]> 10.10.10.58

Enter the remote port to connect to.  This must be the normal admin ssh port, not the CCS port.
[22]>
```

```
Would you like to join this appliance to a cluster using pre-shared keys? Use this option if you
have enabled two-factor authentication on the appliance. [Y]> n

Enter the name of an administrator present on the remote machine
[admin]>

Enter passphrase:
Please verify the SSH host key for 10.10.10.56:
Public host key fingerprint: 80:11:33:aa:bb:44:ee:ee:22:77:88:ff:77:88:88:bb
Is this a valid key for this host? [Y]> y

Joining cluster group Main_Group.
Joining a cluster takes effect immediately, there is no need to commit.
Cluster OriginalCluster.local

Choose the operation you want to perform:
- ADDGROUP - Add a cluster group.
- SETGROUP - Set the group that machines are a member of.
- RENAMEGROUP - Rename a cluster group.
- DELETEGROUP - Remove a cluster group.
- REMOVEMACHINE - Remove a machine from the cluster.
- SETNAME - Set the cluster name.
- LIST - List the machines in the cluster.
- CONNSTATUS - Show the status of connections between machines in the cluster.
- COMMUNICATION - Configure how machines communicate within the cluster.
- DISCONNECT - Temporarily detach machines from the cluster.
- RECONNECT - Restore connections with machines that were previously detached.
- PREPJOIN - Prepare the addition of a new machine over CCS.
[]>

(Cluster OriginalCluster.local)>
```

Une fois connecté et synchronisé, votre nouveau vESA aura désormais la même configuration que votre vESA existant.

Exécutez la commande **clustercheck** pour valider la synchronisation et vérifier s'il y a des incohérences entre les machines mises à niveau.

Étape 6. [Uniquement pour vSMA, ignorer pour vESA]

Consultez les conditions préalables à la sauvegarde des données SMA répertoriées ici.

Utilisez la commande CLI **backupconfig** sur le périphérique qui doit être remplacé pour planifier une sauvegarde sur le vSMA récemment déployé.

Pour démarrer une sauvegarde immédiate

1. Connectez-vous à l'interface de ligne de commande SMA d'origine en tant qu'administrateur.
2. **Enterbackupconfig**.
3. **ChoisissezProgrammer**.
4. Saisissez l'adresse IP du nouvel ordinateur vers lequel transférer les données.
5. Le SMA source vérifie l'existence du SMA cible et s'assure que le SMA cible dispose de suffisamment d'espace pour accepter les données.
6. Choisissez **3 (Démarrer une seule sauvegarde maintenant)**.
7. Entrez **vieworstatus** pour vérifier que la sauvegarde a bien été planifiée.

Note: La durée de sauvegarde des données varie en fonction de la taille des données, de la bande passante du réseau, etc.

Une fois la sauvegarde terminée, le nouveau vSMA aurait reçu toutes les données du SMA précédent.

Pour configurer la nouvelle machine en tant que périphérique principal, reportez-vous aux étapes décrites ici.

Étape 7.

Si vous devez déployer plusieurs ESA/SMA, suivez les étapes 1 à 6.

Informations connexes

Guide d'installation de l'appliance virtuelle de sécurité du contenu Cisco

Configuration et configuration du cluster ESA

Guides de l'utilisateur final SMA