Come applicare la soluzione alternativa per un aggiornamento di Cisco vESA/vSMA che non riesce a causa delle dimensioni ridotte della partizione

Sommario

Introduzione

In questo documento viene descritto il processo di sostituzione di Virtual Email Security Appliance (vESA) e Virtual Security Management Appliance (vSMA) quando un aggiornamento non riesce a causa di una partizione Nextroot di piccole dimensioni.

Difetti correlati per ESA: CSCvy69068 e SMA: CSCvy69076

Sfondo

Inizialmente, ESA virtuale e immagini SMA virtuali sono state create con una partizione Nextroot di dimensioni inferiori a 500M. Nel corso degli anni, e con le nuove versioni di AsyncOS che includono funzionalità aggiuntive, gli aggiornamenti hanno dovuto utilizzare sempre più questa partizione durante tutto il processo di upgrade. A questo punto gli aggiornamenti non riescono a causa delle dimensioni della partizione e desideravamo fornire i dettagli relativi alla soluzione, ovvero installare una nuova immagine virtuale con una dimensione della partizione Nextroot maggiore di 4 GB.

Sintomi

Un'immagine precedente vESA o vSMA con una dimensione della partizione Nextroot inferiore a 500M potrebbe non riuscire a eseguire l'aggiornamento con gli errori seguenti.

```
...
...
...
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
```

Soluzione

Per verificare che l'ESA/SMA virtuale possa essere aggiornato, è necessario verificare prima se le dimensioni della partizione principale successiva sono pari a 4 GB con il comando **ipcheck della** CLI.

```
(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 ----->
```

Se la partizione principale successiva è inferiore a 4 GB, eseguire la procedura seguente per eseguire la migrazione del modello di macchina virtuale corrente a un'immagine aggiornata più recente.

Passaggio 1.

Installazione del nuovo vESA/vSMA

Dai prerequisiti, scaricare l'immagine ESA/SMA virtuale e installarla in base alla Guida all'installazione di Cisco Content Security Virtual Appliance.

> **Nota:** La guida all'installazione fornisce informazioni su DHCP (**interfaceconfig**), imposta il gateway predefinito (**setgateway**) sull'host virtuale e carica il file di licenza del dispositivo virtuale. Assicurarsi di aver letto e distribuito come indicato.

Passaggio 2.

Concessione della licenza per il nuovo vESA/vSMA

Una volta implementata la nuova ESA virtuale o SMA, è il momento di caricare il file della licenza. Per le versioni virtuali, la licenza sarà contenuta in un file XML e deve essere caricata utilizzando la CLI. Dalla CLI, usare il comando **loadlicense** e seguire le istruzioni per completare l'importazione della licenza.

Per ulteriori informazioni su come caricare il file di licenza o ottenerne uno, consultare il seguente articolo: Procedure ottimali per le licenze Virtual ESA, Virtual WSA o Virtual SMA.

Passaggio 3.

Assicurarsi che la nuova versione di vESA/vSMA abbia la stessa versione di quella originale; in caso contrario, è necessario aggiornare la versione di vESA/vSMA con la versione precedente per avere entrambi i dispositivi sulla stessa versione. Usare il comando **upgrade** e seguire le istruzioni fino a ottenere la versione desiderata.

Passaggio 4. [Solo per vESA, salta per vSMA]

> **Nota:** In questo passaggio si presume che non sia disponibile un cluster esistente. Se nella configurazione corrente è già presente un cluster, è sufficiente aggiungere la nuova versione di vESA al cluster per copiare la configurazione corrente e quindi rimuovere il nuovo computer per avviare il processo di aggiornamento.

Crea nuovo cluster

Nel vESA originale eseguire il comando **clusterconfig** per creare un nuovo 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)>
```

Passaggio 5. [Solo per vESA, salta per vSMA]

Unire la nuova vESA al cluster ESA originale

Dalla CLI della nuova vESA, eseguire il comando **clusterconfig > Join a existing...** per aggiungere la nuova vESA al nuovo cluster configurato sulla vESA originale.

```
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)>
```

Una volta connesso e sincronizzato, il nuovo vESA ora avrebbe la stessa configurazione del vESA esistente.

Eseguire il comando **clustercheck** per convalidare la sincronizzazione e verificare eventuali incoerenze tra i computer aggiornati.

Passaggio 6. [Solo per vSMA, salta per vESA]

Esaminare i prerequisiti per il backup dei dati SMA elencati qui.

Usare il comando **backupconfig** della CLI sul dispositivo da sostituire per pianificare un backup sulla vSMA appena implementata.

Per avviare un backup immediato

1. Accedere alla CLI originale di SMA come admin.
2. **Enterbackupconfig**.
3. **Scegliere Pianificazione**.
4. Immettere l'indirizzo IP del nuovo computer in cui trasferire i dati.
5. L'SMA di origine verifica l'esistenza dell'SMA di destinazione e verifica che l'SMA di destinazione disponga di spazio sufficiente per accettare i dati.
6. Scegliere**3 (Avvia un backup singolo ora)**.
7. Immettere **viewstatus** per verificare che il backup sia stato pianificato correttamente.

   Nota: La durata del backup dei dati varia in base alle dimensioni dei dati, alla larghezza di banda della rete, ecc.

Una volta completato il backup, il nuovo vSMA avrebbe ricevuto tutti i dati dal precedente SMA.

Per configurare il nuovo computer come dispositivo principale, fare riferimento alla procedura descritta qui.

Passaggio 7.

Se è necessario installare più di un ESA/SMA, seguire i passaggi 1-6.

Informazioni correlate

Guida all'installazione di Cisco Content Security Virtual Appliance

Requisiti e configurazione del cluster ESA

Guide per l'utente finale SMA