# Cómo aplicar la solución temporal para la actualización fallida de vESA/vSMA de Cisco debido al tamaño de partición pequeño

## Contenido



## Introducción

Este documento describe el proceso para sustituir el dispositivo de seguridad virtual Email Security Appliance (vESA) y el dispositivo de administración de seguridad virtual (vSMA) cuando falla una actualización debido a una pequeña partición Nextroot.

Defectos relacionados para ESA: CSCvy69068 y SMA: CSCvy69076

## Background

Inicialmente, las imágenes ESA virtuales y SMA virtuales se construyeron con un tamaño de partición Nextroot inferior a 500 millones. A lo largo de los años, y con las nuevas versiones de AsyncOS que incluyen funciones adicionales, las actualizaciones han tenido que utilizar cada vez más esta partición a lo largo del proceso de actualización. Ahora estamos empezando a ver que las actualizaciones fallan debido a este tamaño de partición y queríamos proporcionar detalles acerca de la solución, que es implementar una nueva imagen virtual con un tamaño de partición Nextroot más grande de 4 GB.

## Síntomas

Una imagen anterior vESA o vSMA con un tamaño de partición Nextroot inferior a 500M puede no poder actualizar con los siguientes errores.

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

# Solución

Para asegurarse de que su ESA/SMA virtual se puede actualizar, primero debe verificar si el siguiente tamaño de partición raíz es de 4GB con el comando 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 siguiente partición raíz es inferior a 4GB, siga los siguientes pasos para migrar su plantilla de VM actual a una imagen actualizada más reciente.

## Paso 1.

### Implemente su nuevo vESA/vSMA

De los requisitos previos, descargue la imagen ESA/SMA virtual e impleméntelo de acuerdo con la Guía de Instalación de Cisco Content Security Virtual Appliance.

> **Nota:** La guía de instalación proporciona información relacionada con DHCP (**interfaceconfig**) y establece el gateway predeterminado (**setgateway**) en su host virtual, y también carga el archivo de licencia del dispositivo virtual. Asegúrese de que ha leído e implementado tal como se le ha indicado.

## Paso 2.

### Licencia del nuevo vESA/vSMA

Una vez que se ha implementado el nuevo ESA virtual o SMA, es el momento de cargar el archivo de licencia. En el caso de los virtuales, la licencia se incluirá en un archivo XML y se debe cargar mediante la CLI. Desde la CLI, utilizará el comando **loadlicense** y, a continuación, siga las indicaciones para completar la importación de la licencia.

Si necesita más detalles sobre la carga del archivo de licencia o la obtención de uno, puede revisar el siguiente artículo: Prácticas recomendadas para licencias ESA virtuales, WSA virtual o SMA virtual.

## Paso 3.

Asegúrese de que el nuevo vESA/vSMA tenga la misma versión que el original, si no es así, debe actualizar el vESA/vSMA con la versión anterior para que ambos dispositivos tengan la misma versión. Utilice el comando **upgrade** y siga las indicaciones hasta obtener la versión deseada.

## Paso 4. [Solo para vESA, omita para vSMA]

> **Nota:** En este paso, se supone que no tiene un clúster existente, en el caso de que ya haya un clúster existente en la configuración actual, simplemente se agrega el nuevo vESA al clúster para copiar la configuración actual y, a continuación, se elimina esa nueva máquina para iniciar el proceso de actualización.

### Crear un nuevo clúster

En el vESA original, ejecute el comando **clusterconfig** para crear un nuevo clúster.

```
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)>
```

## Paso 5. [Solo para vESA, omita para vSMA]

### Únase a su nuevo vESA en su clúster ESA original

Desde la CLI en el nuevo vESA, ejecute el comando **clusterconfig > Join an existing...** para agregar su nuevo vESA al nuevo clúster configurado en su vESA original.

```
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 vez conectado y sincronizado, su nuevo vESA ahora tendría la misma configuración que su vESA existente.

Ejecute el comando **clustercheck** para validar la sincronización y verificar si hay alguna inconsistencia entre las máquinas actualizadas.

## Paso 6. [Solo para vSMA, omita para vESA]

Revise los requisitos previos para la copia de seguridad de datos SMA que se enumeran aquí.

Use el comando CLI **backupconfig** en el dispositivo que debe reemplazarse para programar una copia de seguridad en el vSMA recientemente implementado.

Para iniciar una copia de seguridad inmediata

1. Inicie sesión en la CLI SMA original como admin.
2. **Enterbackupconfig**.
3. **ElijaProgramar**.
4. Introduzca la dirección IP de la nueva máquina a la que desea transferir los datos.
5. El SMA de "origen" verifica la existencia del SMA de "destino" y se asegura de que el SMA de destino tenga suficiente espacio para aceptar los datos.
6. Elija **3 (Iniciar una única copia de seguridad ahora)**.
7. Ingrese **vieworstatus** para verificar que la copia de seguridad se programó correctamente.

   **Nota:** La duración que se tarda en completar la copia de seguridad de los datos varía en función del tamaño de los datos, el ancho de banda de la red, etc.

Una vez que se complete la copia de seguridad, el nuevo vSMA habría recibido todos los datos del SMA anterior.

Para configurar la nueva máquina como el dispositivo principal, consulte los pasos descritos aquí.

### Paso 7.

En caso de que necesite implementar más de un ESA/SMA, siga los pasos 1-6.

## Información Relacionada

Guía de instalación de Cisco Content Security Virtual Appliance

Requisitos y configuración del clúster ESA

Guías de usuario final de SMA