How to Apply the Workaround for Cisco vESA/vSMA Failing Upgrade Due to Small Partition Size

Contents

Introduction

This document describes the process to replace the virtual Email Security Appliance (vESA) and virtual Security Management Appliance (vSMA) when an upgrade is failing due to a small Nextroot partition.

Related defects for ESA: CSCvy69068 and SMA: CSCvy69076

Background

Initially, virtual ESA and virtual SMA images were built with a Nextroot partition size of less than 500M. Over the years, and with newer AsyncOS releases that include additional features, upgrades have had to use more and more of this partition throughout the upgrade process. We're now starting to see upgrades fail because of this partition size and we wanted to provide details surrounding the solution, which is to deploy a new virtual image that has a larger Nextroot partition size of 4GB.

Symptoms

An older image vESA or vSMA with a Nextroot partition size of less than 500M may fail to upgrade

with the below errors being seen.

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

To ensure your virtual ESA/SMA can be upgraded, you would need to first check if the next root partition size is 4GB with the CLI command **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 ----->
```

If the next root partition is less than 4GB, follow the next steps to migrate your current VM template to a newer updated image.

Step 1.

Deploy Your New vESA/vSMA

From the pre-requisites, download the virtual ESA/SMA image and deploy per the Cisco Content Security Virtual Appliance Installation Guide.

> **Note**: The installation guide provides information regarding DHCP (**interfaceconfig**) and set the default gateway (**setgateway**) on your virtual host, and also loading the virtual appliance license file. Ensure that you have read and deployed as instructed.

Step 2.

Licensing the New vESA/vSMA

Once the new virtual ESA or SMA has been deployed then it is time to load the license file. For virtuals, the license will be contained within an XML file and must be loaded using the CLI. From the CLI, you will use the **loadlicense** command and then follow the prompts to complete the license import.

If you require further details on loading the license file or obtaining one, then you can review the following article: Best Practices for Virtual ESA, Virtual WSA, or Virtual SMA Licenses.

Step 3.

Ensure the new vESA/vSMA has the same version as the original one, if that is not the case you need to upgrade the vESA/vSMA with the older version to get both devices on the same version. Use the command **upgrade** and follow the prompts until getting the desired version.

Step 4. [Only for vESA, skip for vSMA]

> **Note**: In this step, it is assumed you do not have an existing cluster, in the case, there is already an existent cluster in the current configuration, you just add the new vESA to the cluster to copy the current configuration and then you remove that new machine to start the upgrade process.

Create a New Cluster

In the original vESA run the command **clusterconfig** to create a new 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)>
```

Step 5. [Only for vESA, skip for vSMA]

Join your New vESA to your Original ESA Cluster

From the CLI on the New vESA, run the command **clusterconfig > Join an existing...** to add your New vESA into your new cluster configured on your Original vESA.

```
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)>
```

Once connected and synced, your new vESA now would have the same configuration as your existing vESA.

Run the command **clustercheck** to validate sync and verify if there are any inconsistencies between the upgraded machines.

Step 6. [Only for vSMA, skip for vESA]

Review pre-requisites for SMA data backup listed here.

Use CLI command **backupconfig** on the device that has to be replaced to schedule a backup to the newly deployed vSMA.

To start an immediate backup

1. Log in to the original SMA CLI as admin.
2. Enter**backupconfig**.
3. Choose**Schedule**.
4. Enter the IP address of the new machine to transfer the data to.
5. The "source" SMA verifies the existence of the "target" SMA and makes sure the target SMA has enough space to accept the data.
6. Choose**3 (Start a Single Backup Now)**.
7. Enter **view**or**status** to verify that the backup was successfully scheduled.

   Note: The duration taken for the data backup to complete would vary based on the size of data, network bandwidth, etc.

Once the backup completes, the new vSMA would have received all data from the previous SMA.

To configure the new machine as the primary device, refer to the steps outlined here.

Step 7.

In case you need to deploy more than one ESA/SMA, follow steps 1-6.

Related Information

Cisco Content Security Virtual Appliance Installation Guide

ESA Cluster Requirements and Setup

SMA End User Guides