Anleitung zur Anwendung der Problemumgehung bei einem Upgrade von Cisco vESA/vSMA wegen kleiner Partitionsgröße

Inhalt

Einführung

In diesem Dokument werden die Schritte beschrieben, um die auf Cisco vESA/vSMA bereitgestellte Problemumgehung anzuwenden, wenn das Upgrade aufgrund der kleinen Partitionsgröße fehlschlägt.

Verwandte Fehler für ESA: CSCvy69068 und SMA: CSCvy69076

Problem

Alte virtuelle Systeme stellen während des Upgrades auf die Version 14.x oder neuer ein Problem dar. Jede virtuelle E-Mail-Security-Appliance (vESA) oder virtuelle Security Management Appliance (vSMA) mit einer nächsten Root-Partitionsgröße von weniger als 4 GB weist während des Upgrade-Prozesses die folgenden Fehler auf:

```
For vESA

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

For vSMA

Finding partitions... done.
Setting next boot partition to current partition as a precaution... done.
Erasing new boot partition... done.
Erasing new boot partition... done.
Extracting scanerroot done.
Extracting splunkroot done.
Extracting distroot
/nextroot: write failed, filesystem is full
./usr/bin/objdump: Write failed
./usr/bin/raid: Write to restore size failed
./usr/bin/disk_seek: Write to restore size failed
```

Lösung

Um sicherzustellen, dass Ihr virtuelles ESA/SMA aktualisiert werden kann, müssen Sie zuerst überprüfen, ob die nächste Root-Partitionsgröße 4 GB ist. Dazu verwenden Sie den CLI-Befehl **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 ----->
```

Wenn die nächste Root-Partition weniger als 4 GB beträgt, befolgen Sie die nächsten Schritte, um Ihre aktuelle VM-Vorlage auf ein neueres aktualisiertes Image zu migrieren.

Schritt 1:

Bereitstellung Ihrer neuen vESA/vSMA

Laden Sie das virtuelle ESA/SMA-Image unter den Voraussetzungen herunter, und stellen Sie es gemäß dem Installationsleitfaden für die Cisco Content Security Virtual Appliance bereit.

> **Hinweis:** Die Installationsanleitung enthält Informationen zu DHCP (**Interfaceconfig**), zum Festlegen des Standard-Gateways (**setgateway**) auf Ihrem virtuellen Host sowie zum Laden der Lizenzdatei der virtuellen Appliance. Stellen Sie sicher, dass Sie die Anweisungen

gelesen und bereitgestellt haben.

Schritt 2:

Lizenzierung der neuen vESA/vSMA

Demolizenz erstellen

1. Rufen Sie das Cisco License Registration Portal (LRP) auf: cisco.com/go/license
2. Melden Sie sich mit Ihrer Cisco Konto-ID an.
3. Lizenzen auswählen
4. Wählen Sie im Dropdown-Menü **"Lizenzen** abrufen" die Option **Demo und Evaluation aus..**
5. Wählen Sie im Popup-Fenster die Produktfamilie: **Sicherheitsprodukte** und Produkt: **Cisco Email/Web/Content Security Virtual Demo-Lizenz**
6. Wählen Sie das Produkt für eine der folgenden Optionen aus:

- ESA Virtual Appliance Demo-Lizenz, 45 Tage
- Demo-Lizenz für WSA Virtual Appliance 45 Tage
- SMA Virtual Appliance 45-Tage-Demo-Lizenz

7. **Weiter** auswählen
8. Für SN/Virtual Device Identifier (SN/Virtual Device Identifier) können Sie die Seriennummer Ihrer vorhandenen, vollständig lizenzierten Appliance eingeben oder eine leere Zeichenfolge lassen und **Weiter** auswählen.
9. Überprüfen Sie abschließend die Felder **Senden an**, **Endbenutzer**. Klicken Sie auf **..** um zusätzliche Empfänger hinzuzufügen
10. Wählen Sie **Senden**, um die Demo-Lizenzanfrage abzuschließen.
11. Überprüfen Sie die E-Mail-Adresse, wie in früheren Schritten eingegeben, da die Demolizenz an diese E-Mail-Adresse gesendet wird.

Hinweis: Ihre virtuelle Lizenzdatei wird innerhalb von drei Stunden im XML-Format an die von Ihnen angegebene E-Mail-Adresse gesendet.

Freigeben einer vorhandenen Lizenz

1. Rufen Sie das Cisco License Registration Portal (LRP) auf: cisco.com/go/license
2. Melden Sie sich mit Ihrer Cisco Konto-ID an.
3. Lizenzen auswählen
4. Wählen Sie im Dropdown-Menü **Lizenzen verschieben** die Option **Lizenz teilen aus..**
5. Wählen Sie die Option **Aktivierungscodes abrufen aus.**
6. Ein Popup-Fenster wird angezeigt. Wählen Sie **IronPort-Produkt - SW-Pakete** (wenn Sie ein vorhandenes Softwarepaket besitzen) oder **IronPort-Produkt - TC** (wenn Sie individuelle Produkte haben) aus.
7. Geben Sie im Feld Source Serial Number/Virtual Device Identifier (Seriennummer/Virtuelle Geräte-ID) eine vorhandene ESA-/WSA-/SMA-Seriennummer ein. Wenn Sie über mehrere ESAs, WSAs oder SMAs verfügen, wählen Sie eine Appliance mit den gleichen Lizenzen aus, die Sie für Ihre virtuelle Appliance aktivieren möchten.

8. Wählen Sie für die Option **Zielappliance-Typ auswählen** die Schaltfläche **Virtuell** aus.
9. Lassen Sie das Feld "Seriennummer/ID des virtuellen Geräts" leer.
10. Geben Sie im Feld **Senden an** die E-Mail-Adresse ein, an die der Aktivierungscode gesendet werden soll.
11. Wenn Sie die Lizenzanfrage bereits bearbeitet haben, können Sie vorhandene VLNs erhalten. Wählen Sie diese Option aus.
12. **Anforderungscode** auswählen
13. Wiederholen Sie nach Erhalt des Aktivierungscodes die Schritte 3 und 4 (oben aufgeführt). Wenn Sie Schritt 5 erreicht haben, wählen Sie die Option **Use Activation Codes (Aktivierungscodes verwenden) aus.**
14. Fügen Sie den bereitgestellten Aktivierungscode ein, und klicken Sie auf Weiter.
15. Wählen Sie die Cisco ESA/WSA-Software-SKUs aus, die in die virtuelle ESA/virtuelle WSA/virtuelle SMA-Lizenz von Cisco eingebettet werden sollen. Klicken Sie auf **Weiter**
16. Geben Sie die E-Mail-Adresse ein, an die die Lizenz gesendet werden soll.
17. Klicken Sie abschließend auf **Lizenz abrufen.**

Hinweis: Ihre virtuelle Lizenzdatei wird innerhalb von drei Stunden im XML-Format an die von Ihnen angegebene E-Mail-Adresse gesendet.

Schritt 3:

Stellen Sie sicher, dass die neue vESA/vSMA die gleiche Version wie die ursprüngliche hat, wenn dies nicht der Fall ist, müssen Sie die vESA/vSMA mit der älteren Version aktualisieren, um beide Geräte auf derselben Version abzurufen. Verwenden Sie den Befehl **upgrade** und folgen Sie den Anweisungen, bis die gewünschte Version angezeigt wird.

Schritt 4: [Nur für vESA, für vSMA überspringen]

Hinweis: In diesem Schritt wird davon ausgegangen, dass Sie kein vorhandenes Cluster haben. Falls es in der aktuellen Konfiguration bereits ein vorhandenes Cluster gibt, fügen Sie einfach die neue vESA zum Cluster hinzu, um die aktuelle Konfiguration zu kopieren, und entfernen Sie dann dieses neue System, um den Upgrade-Prozess zu starten.

Erstellen eines neuen Clusters

Führen Sie in der ursprünglichen vESA den Befehl **clusterconfig** aus, um einen neuen Cluster zu erstellen.

```
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)>
```

Schritt 5: [Nur für vESA, für vSMA überspringen]

Verbinden Sie Ihre neue vESA mit Ihrem ursprünglichen ESA-Cluster.

Führen Sie in der CLI der neuen vESA den Befehl **clusterconfig > An vorhandener Konfiguration beitreten aus..** , um Ihre neue vESA zu Ihrem neuen Cluster hinzuzufügen, der auf Ihrer ursprünglichen vESA konfiguriert wurde.

```
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)>
```

Nach der Verbindung und Synchronisierung verfügt Ihre neue vESA jetzt über die gleiche Konfiguration wie Ihre vorhandene vESA.

Führen Sie den Befehl **clustercheck aus**, um die Synchronisierung zu überprüfen und zu überprüfen, ob die aktualisierten Computer Inkonsistenzen aufweisen.

Schritt 6: [Nur für vSMA, für vESA überspringen]

Lesen Sie die hier aufgelisteten Voraussetzungen für SMA-Daten-Backups.

Verwenden Sie den CLI-Befehl **backupconfig** auf dem Gerät, das ersetzt werden muss, um eine Sicherung für die neu bereitgestellte vSMA zu planen.

So starten Sie eine sofortige Sicherung

1. Melden Sie sich als admin bei der ursprünglichen SMA-CLI an.
2. **Enterbackupconfig**.
3. **Wählen SieZeitplan aus**.

4. Geben Sie die IP-Adresse des neuen Geräts ein, an das die Daten übertragen werden sollen.
5. Die "Quell"-SMA überprüft das Vorhandensein der "Ziel"-SMA und stellt sicher, dass die Ziel-SMA genügend Platz hat, um die Daten zu akzeptieren.
6. Wählen Sie **3 aus (eine einzelne Sicherung jetzt starten)**.
7. Geben Sie den **Anzeigestatus ein**, um zu überprüfen, ob die Sicherung erfolgreich geplant wurde.

   Hinweis: Die Dauer der Datensicherung hängt von der Datengröße, der Netzwerkbandbreite usw. ab.

Nach Abschluss der Sicherung hätte die neue vSMA alle Daten der vorherigen SMA erhalten.

Um das neue System als primäres Gerät zu konfigurieren, beachten Sie die hier beschriebenen Schritte.

Schritt 7:

Wenn Sie mehrere ESAs/SMAs bereitstellen müssen, gehen Sie wie folgt vor: 1-6.

Zugehörige Informationen

Installationsanleitung für die Cisco Content Security Virtual Appliance

ESA-Cluster-Anforderungen und Einrichtung

SMA-Benutzerhandbücher