ESA und SMA auf ursprüngliche Konfiguration zurücksetzen

Inhalt

Einleitung

Lösung

Hardware-Appliances (ESA/SMA)

Virtuelle Appliances (ESA/SMA)

- VMware ESXi
- Microsoft Hyper-V
- KVM
- Nutanix

Public Cloud-Bereitstellung

- Azure
- AWS
- GCP

Einleitung

In diesem Dokument wird das Verfahren zum Zurücksetzen und erneuten Bereitstellen einer E-Mail Security Appliance (ESA) oder Security Management Appliance (SMA) beschrieben.

Lösung

Hardware-Appliances (ESA/SMA)

Schritte zum Reinigen und Zurücksetzen einer physischen Appliance.

1. SSH für die Appliance ausführen und Version ausführen und die aktive Version notieren, die auf der Appliance ausgeführt wird.

2. Führen Sie Zurücksetzen aus, wählen Sie eine ältere Codeversion als Von 1 aus, und geben Sie Y ein.

```
sma.example.com> revert

This command will revert the appliance to a previous version of AsyncOS.

WARNING: Reverting the appliance is extremely destructive.
The following data will be destroyed in the process:
- all configuration settings (including listeners)
- all log files
```

```
- all databases (including messages in Virus Outbreak and Policy quarantines)
- all reporting data (including saved scheduled reports)
- all message tracking data
- all Cisco IronPort Spam Quarantine messages
  and end-user safelist/blocklist data

Only the network settings (except the 'allow_arp_multicast' configuration variable)
will be retained. If you need to establish connectivity to a Microsoft Network Load Balancer,
you must configure the 'allow_arp_multicast' configuration variable after the revert process
is complete.

Before running this command, be sure you have:
- saved the configuration file of this appliance (with passwords unmasked)
- exported the Cisco IronPort Spam Quarantine safelist/blocklist database
  to another machine (if applicable)
- waited for the mail queue to empty

Reverting the device causes an immediate reboot to take place.
After rebooting, the appliance reinitializes itself and reboots
again to the desired version.

    Available versions
    ==================
 1. 16.0.1-010
 2. 16.0.2-088
 3. 16.0.3-016
Please select an AsyncOS version [2]: 1
Do you want to continue? [N]> y
Are you sure you want to continue? [N]> y
```

Warnung: Mit diesem Verfahren werden Konfiguration, Daten und Verlauf der Upgrades auf der Appliance gelöscht.

---

4. Warten Sie, bis der Computer vollständig wiederhergestellt ist. Es wird erwartet, dass der Vorgang ca. 30 Minuten in Anspruch nimmt.

3. Sobald das Zurücksetzen abgeschlossen und die Appliance aktiv ist, greifen Sie erneut auf die Befehlszeile zu und führen Sie Reload via Diagnostic aus.

```
esa.example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- RELOAD_STATUS - Display status of last reload run
- SERVICES - Service Utilities.
[]> reload

This command will remove all user settings and reset the entire device.
```

```
If this is a Virtual Appliance, all feature keys will be removed, and the license must be reapplied. Th
Are you sure you want to continue? [N]> y
Are you *really* sure you want to continue? [N]> y
Do you want to wipe also? Warning: This action is recommended if the device is being sanitized before s
Sometimes, it may take several minutes to complete the process because it follows the NIST Purge standa
Reverting to "virtualimage" preconfigure install mode.
```

Virtuelle Appliances (ESA/SMA)

Informationen zu den Hardwareanforderungen und der unterstützten Hypervisor-Plattform finden Sie unter https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/Cisco_Content_S

VMware ESXi

1. Laden Sie das virtuelle Appliance-Image und den MD5-Hash von Cisco herunter.
2. Entpacken Sie die ZIP-Datei für die virtuelle Appliance in einem eigenen Verzeichnis. z. B. C:\vESA\C100V.
3. Öffnen Sie VMware vSphere Client auf Ihrem lokalen System.
4. Wählen Sie den ESXi-Host oder -Cluster aus, auf dem Sie die virtuelle Appliance bereitstellen möchten.
5. Wählen Sie Datei > OVF-Vorlage bereitstellen aus.
6. Geben Sie den Pfad zur OVF-Datei in das von Ihnen erstellte Verzeichnis ein, und klicken Sie auf Weiter. Schließen Sie den Assistenten ab.
7. Wenn DHCP deaktiviert ist, richten Sie die Appliance in Ihrem Netzwerk ein. Installieren Sie die Lizenzdatei.
8. Melden Sie sich bei der Webbenutzeroberfläche Ihrer Appliance an, und konfigurieren Sie die Appliance-Software.

Microsoft Hyper-V

1. Laden Sie das Image der virtuellen Appliance und den MD5-Hash von Cisco herunter.

2. Öffnen Sie Hyper-V Manager, verwenden Sie den "Assistenten für neue virtuelle Systeme", um ein neues virtuelles System zu erstellen.

3. Weisen Sie die empfohlenen Hardware-Ressourcen zu. (siehe virtuelle Installationsanleitung)

4. Fügen Sie das heruntergeladene Image der virtuellen Appliance als virtuelle Festplatte an. Schließen Sie den Assistenten ab, und starten Sie das virtuelle System.

5. Wenn DHCP deaktiviert ist, richten Sie die Appliance in Ihrem Netzwerk ein. Installieren Sie die Lizenzdatei.

6. Melden Sie sich bei der Webbenutzeroberfläche Ihrer Appliance an, und konfigurieren Sie die Appliance-Software.

KVM

Bereitstellung virtueller Systeme mit Virtual Machine Manager Laden Sie das virtuelle Appliance-Image und den MD5-Hash von Cisco herunter.

1. Starten Sie die Anwendung virt-manager. Wählen Sie Neu aus.

2. Geben Sie einen eindeutigen Namen für die virtuelle Appliance ein. Wählen Sie Vorhandenes Bild importieren aus.

3. Wählen Sie Weiterleiten, geben Sie Optionen OS Typ: UNIX, Version: FreeBSD 13.

4. Suchen Sie das heruntergeladene virtuelle Appliance-Image, und wählen Sie Weiterleiten aus.

5. Geben Sie RAM- und CPU-Werte für das bereitzustellende virtuelle Appliance-Modell ein. (siehe virtuelle Installationsanleitung)

6. Wählen Sie Weiterleiten, aktivieren Sie das Kontrollkästchen Anpassen, und wählen Sie Beenden.

7. Konfigurieren Sie das Laufwerk. Wählen Sie im linken Bereich das Laufwerk und unter Erweiterte Optionen, Datenträgerbus: Virtualisierung, Speicherformat: qcow2 aus, und wählen Sie Anwenden aus.

8. Konfigurieren Sie das Netzwerkgerät für die Verwaltungsschnittstelle. Wählen Sie im linken Bereich eine Netzwerkkarte aus, und wählen Sie die Optionen Quellgerät: Ihr Management-VLAN, Gerätemodell: virtIO, Quellmodus: VEPA, wählen Sie Anwenden.

9. Konfigurieren Sie Netzwerkgeräte für zusätzliche Schnittstellen, wiederholen Sie Schritt 8 für jede Schnittstelle, die der virtuellen Maschine hinzugefügt wird.

10. Wählen Sie Installation beginnen.

Nutanix

1. Laden Sie das Image der virtuellen Appliance und den MD5-Hash von Cisco herunter.

2. Rufen Sie Nutanix Prism auf, entfernen Sie das virtuelle qcow2-Image, und laden Sie es in Ihren Speicherpool hoch.

3. Klicken Sie auf das Hamburger-Symbol in der oberen linken Ecke des Nutanix Prism-Dashboards, und wählen Sie Compute and Storage > VM aus dem linken Navigationsbereich aus.

4. Klicken Sie auf die Schaltfläche Create VM (VM erstellen), geben Sie die Details für die Konfiguration der VM ein, und klicken Sie auf Next (Weiter).

5. Konfigurieren Sie die Hardwareressourcen basierend auf dem Modell (siehe virtuelle Installationsanleitung)

6. Klicken Sie auf die Schaltfläche Festplatte anhängen unter Festplatten und wählen Sie in der

Dropdown-Liste Operation die Option Aus Image klonen und qcow2 Image aus der Dropdown-Liste Image hochgeladen aus.

7. Klicken Sie unter Netzwerke auf die Schaltfläche An Subnetz anhängen, und konfigurieren Sie die Einstellungen für die Netzwerkschnittstelle.

8. Schließen Sie den Assistenten ab, um die virtuelle Appliance auf Nutanix Prism bereitzustellen.

Public Cloud-Bereitstellung

Informationen und Verfahren zur Bereitstellung von ESA und SMA in einer Public Cloud finden Sie unter https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/ESA_SMA_Virtua

Azure

1. Erstellen Sie die Anforderungskomponenten.

2. Rufen Sie das VM-Image ab.

3. Zugriffskontrolle konfigurieren - Identitäts- und Zugriffsmanagement (IAM)

4. Melden Sie sich an, und erstellen Sie die VM.

Auf den Seiten 4 bis 18 des Bereitstellungsleitfadens für Public Clouds finden Sie detaillierte Anweisungen zur Bereitstellung des virtuellen Systems auf Azure.

AWS

1. Wenden Sie sich an das Cisco TAC, um die AMI-ID zu erhalten.

2. Öffnen Sie die Amazon EC2 Konsole.

3. Wählen Sie im Navigationsbereich AMIs aus.

4. Wählen Sie im ersten Filter Öffentliche Bilder.

5. Geben Sie in der Suchleiste die "Build-Nummer" und das "Modell" entsprechend dem erforderlichen virtuellen Appliance-Modell ein.

Auf den Seiten 19 bis 29 des Bereitstellungsleitfadens für Public Clouds finden Sie detaillierte Anweisungen zur Bereitstellung des virtuellen Systems auf AWS.

GCP

1. Vorbereitung der Umgebung und Konfiguration des virtuellen Systems

2. Wählen Sie Betriebssystem und Speicher.

3. Konfigurieren Sie das Netzwerk, die Firewall und die Netzwerkschnittstelle.

4. Konfigurieren des virtuellen Systems

Auf den Seiten 30 bis 34 des Bereitstellungsleitfadens für Public Clouds finden Sie detaillierte Anweisungen zur Bereitstellung des virtuellen Systems auf GCP.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.