Best Practices für die Migration von Hardware von ESA/SMA auf virtuelle ESA/SMA

Inhalt

Einleitung

In diesem Dokument werden die Best Practices für Bereitstellung, Migration und Konfiguration von der Hardware-ESA/SMA zur virtuellen ESA/SMA beschrieben.

Wesentliche Schritte

Schritt 1: Laden Sie das virtuelle ESA-Image herunter, und stellen Sie das virtuelle System bereit

Es wird empfohlen, vor der Migration der Konfiguration ein virtuelles Secure Email Gateway (ESA)/eine Security Management Appliance (SMA) mit derselben AsyncOS-Version wie die Hardware auszuführen. Sie können die AsyncOS-Version auswählen, die der auf Ihrer Appliance ausgeführten Version am nächsten kommt, und sie anschließend aktualisieren, falls erforderlich, oder die neueste Version von AsyncOS herunterladen.

Bereitstellungen auf diesen Plattformen werden unterstützt: Microsoft Hyper-V, KVM (Keyboard/Video/Mouse) und VMware ESXi. Weitere Informationen finden Sie im Installationshandbuch: https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/Cisco_Content_S

Sie können das virtuelle Image unter folgendem Link herunterladen: https://software.cisco.com/download/home/284900944/type/282975113/release/15.0.0.

Schritt 2: Erwerb von Lizenzen für die virtuelle ESA/SMA

Um ein Upgrade der virtuellen ESA/SMA durchführen zu können, müssen Sie zunächst deren Lizenzen installieren. Sie können die vorhandenen Lizenzen von Ihrer Hardware mit der neuen virtuellen ESA teilen (beide ESAs können zusammen ausgeführt werden).

Bei herkömmlichen Lizenzen öffnen Sie die Datei, die Sie mit NotePad++ oder WordPad erhalten haben, sobald die physische Lizenz für vESA/vSMA erfolgreich freigegeben wurde und Sie Ihre Lizenz erhalten.XML haben. Wählen Sie alle aus, und kopieren/einfügen Sie sie dann mithilfe des loadlicense Befehls über die vESA/vSMA-CLI. Weitere Informationen finden Sie unter https://www.cisco.com/c/en/us/support/docs/security/email-security-virtual-appliance/118301-technote-esa-00.html.

Fügen Sie für Smart-Lizenzen die neue vESA/vSMA dem Smart Account hinzu. Sobald das Token generiert wurde, registrieren Sie die Geräte

gemäß dem im Artikel erwähnten Prozess: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/214614-smart-licensing-overview-and-best-practi.html.

Schritt 3: Aktualisieren Sie die virtuelle ESA/SMA auf die genaue AsyncOS-Version der Hardware ESA/SMA (falls erforderlich).

Die Hardware und die virtuelle Appliance müssen sich vor der Migration auf derselben Version befinden. Sie können die Kompatibilitätsmatrix für die SMA und die ESA auf dem erwähnten Link überprüfen, um die ESA auf die richtige Version zu aktualisieren: https://www.cisco.com/c/dam/en/us/td/docs/security/security_management/sma/sma_all/email-compatibility/index.html.

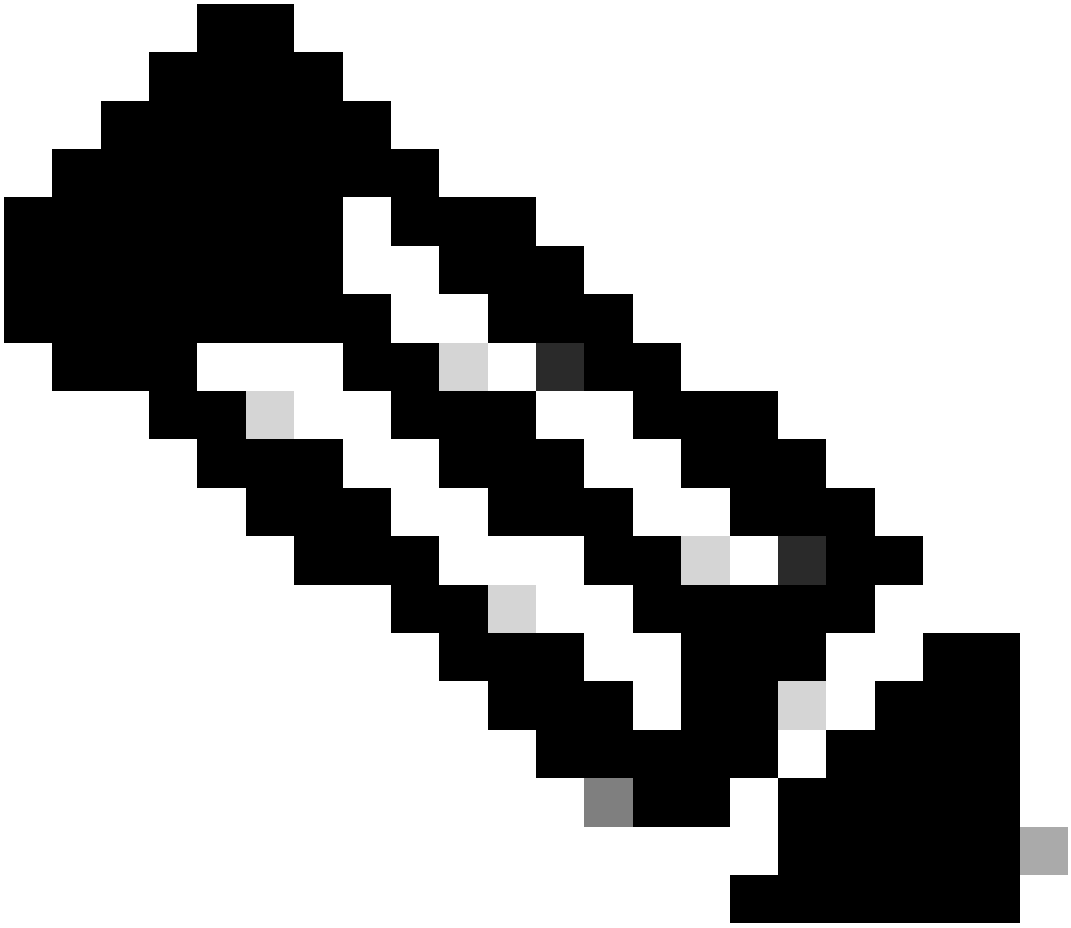
Schritt 4: Migration der vorhandenen Konfiguration von der Hardware-ESA/SMA auf die virtuelle ESA/SMA

Die virtuelle ESA/SMA kann folgendermaßen konfiguriert werden:

- Konfigurieren Sie die Geräte von Grund auf neu, wenn die vorhandene Hardware das End-of-Life (EOL)/End-of-Support (EOS) erreicht oder ein aktualisiertes vESA/SMA-Image installiert ist oder wenn mehrere Geräte konfiguriert werden müssen.

- Wenn sich das Hardwaregerät bereits im Cluster befindet, fügen Sie die neue vESA/vSMA zum Cluster hinzu. Die neuen Geräte erhalten eine Kopie Ihrer vorhandenen Konfiguration vom Cluster.

- Wenn es sich bei dem Hardwaregerät um ein eigenständiges Gerät handelt, aktivieren Sie die Cluster-Konfiguration, und fügen Sie die neue virtuelle ESA/SMA zum Cluster hinzu, um eine Kopie der vorhandenen Konfiguration zu erhalten.



Hinweis: Sobald die virtuelle ESA/SMA die aktuelle Konfiguration erhalten hat, können Sie die Geräte vom Cluster trennen oder sie je nach Anforderung unverändert lassen. Das Hardwaregerät kann aus der Cluster-Konfiguration entfernt und außer Betrieb genommen werden.

Schritt 5: Korrigieren des aktualisierten Servers auf der virtuellen ESA/SMA

Die virtuelle und die Hardware-ESA/SMA verwenden unterschiedliche Upgrade-Server, und nach der Migration der Konfiguration ändert sich der Server. Um Ihr vESA/vSMA weiter zu aktualisieren, können Sie den Server über die vESA/vSMA-CLI mit den folgenden Schritten korrigieren:

- Führen Sie den Befehl updateconfig und dann den Unterbefehl dynamichostaus.

- Server ändern in update-manifests.sco.cisco.com:443.
- Bestätigen Sie die Änderungen.

Weitere häufig gestellte Fragen zur Migration finden Sie unter folgendem Link: https://www.cisco.com/c/en/us/support/docs/security/email-security-virtual-appliance/215466-esa-sma-virtual-deployment-faq.pdf.

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.