Conozca las prácticas recomendadas para migrar el hardware ESA/SMA a ESA/SMA virtual

Contenido

Introducción

Este documento describe las prácticas recomendadas con respecto a la implementación, migración y configuración de ESA/SMA de hardware a ESA/SMA virtual.

Pasos esenciales

Paso 1. Descargue la imagen ESA virtual e implemente la máquina virtual

Se recomienda tener un Secure Email Gateway (ESA)/Security Management Appliance (SMA) virtual ejecutándose en la misma versión de AsyncOS que el hardware antes de poder migrar la configuración. Puede elegir la versión de AsyncOS más cercana a la versión que se ejecuta en el dispositivo y actualizarla después, si es necesario, o descargar la última versión de AsyncOS.

Las implementaciones en estas plataformas son compatibles: Microsoft Hyper-V, teclado, vídeo y ratón (KVM) y VMWare ESXi. Consulte la guía de instalación para obtener más información: https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/Cisco_Content_S

Puede descargar la imagen virtual desde el enlace: https://software.cisco.com/download/home/284900944/type/282975113/release/15.0.0.

Paso 2. Obtener licencias para el ESA/SMA virtual

Para poder actualizar el ESA/SMA virtual, primero debe instalar sus licencias; puede compartir las licencias existentes de su hardware con el nuevo ESA virtual (ambos ESA se pueden ejecutar juntos).

En el caso de las licencias tradicionales, una vez que la licencia física se haya compartido correctamente para vESA/vSMA y haya recibido la licencia, abra el .XML archivo que recibió con NotePad++ o WordPad. Seleccione todos y, a continuación, copie y pegue mediante la CLI de vESA/vSMA mediante el loadlicense comando. Consulte el enlace para obtener más información: https://www.cisco.com/c/en/us/support/docs/security/email-security-virtual-appliance/118301-technote-esa-00.html.

Para las licencias Smart, agregue el nuevo vESA/vSMA en la cuenta Smart. Una vez generado el token, registre los dispositivos según el proceso mencionado en el artículo: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/214614-smart-licensing-overview-and-best-practi.html.

Paso 3. Actualice el ESA/SMA virtual a la versión AsyncOS exacta del ESA/SMA de hardware (si es necesario)

El hardware y el dispositivo virtual deben estar en la misma versión antes de la migración. Puede verificar la matriz de compatibilidad para el SMA y el ESA en el link mencionado para actualizar el ESA a la versión adecuada: https://www.cisco.com/c/dam/en/us/td/docs/security/security_management/sma/sma_all/email-compatibility/index.html.

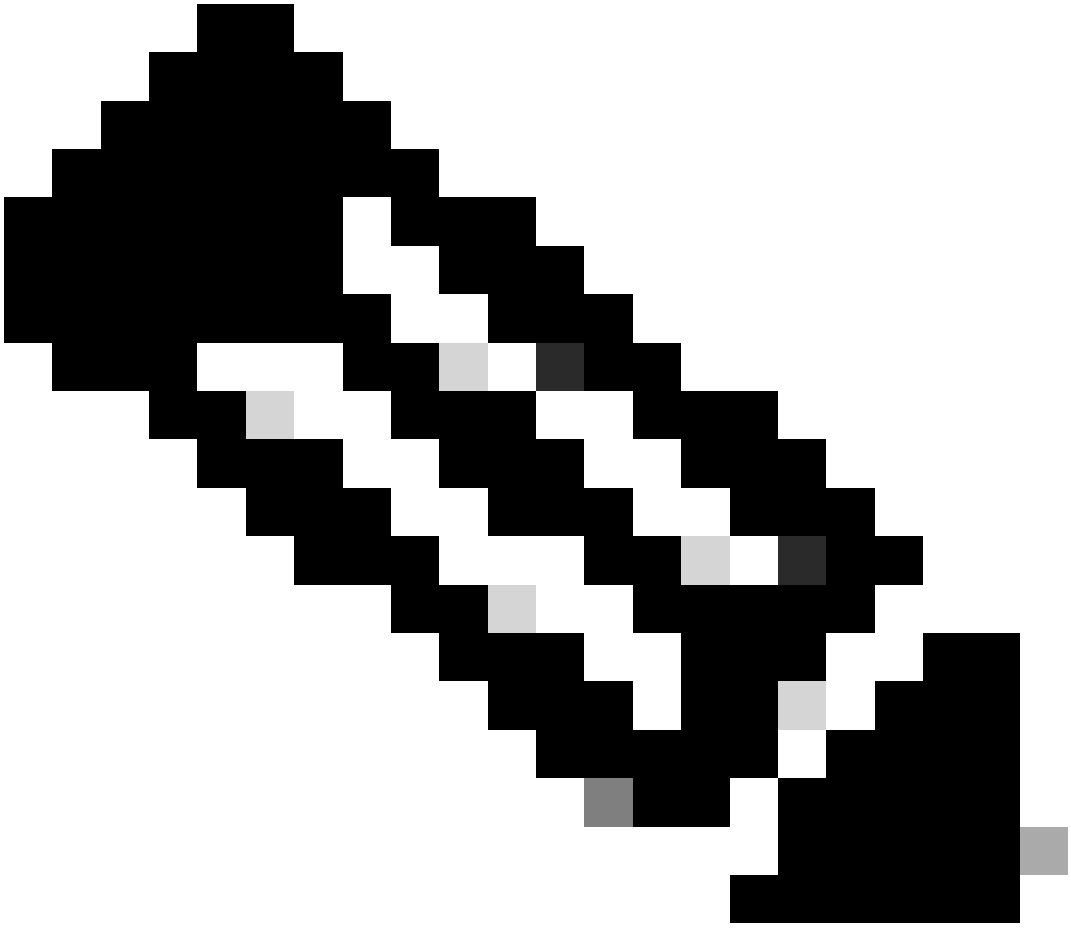
Paso 4. Migrar la configuración existente del ESA/SMA de hardware al ESA/SMA virtual

El ESA/SMA virtual se puede configurar de las siguientes maneras:

- Configure los dispositivos desde el principio si el hardware existente está llegando al fin de su vida útil (EOL)/fin de soporte (EOS) o si se ha instalado una imagen vESA/SMA actualizada o si se deben configurar varios dispositivos.

- Si el dispositivo de hardware ya está en el clúster, agregue el nuevo vESA/vSMA al clúster. Los nuevos dispositivos obtienen una copia de la configuración existente del clúster.

- Si el dispositivo de hardware es un dispositivo independiente, habilite la configuración del clúster y agregue el nuevo ESA/SMA virtual al clúster para obtener una copia de la configuración existente.



Nota: Una vez que el ESA/SMA virtual obtiene la configuración actual, puede elegir desconectar los dispositivos del clúster o mantenerlos tal cual según los requisitos. El dispositivo de hardware puede eliminarse de la configuración del clúster y retirarse.

Paso 5. Corrija el servidor actualizado en el ESA/SMA virtual

El ESA/SMA virtual y de hardware utilizan diferentes servidores de actualización y, después de migrar la configuración, el servidor cambia. Para poder seguir actualizando su vESA/vSMA, puede corregir el servidor a través de la CLI de vESA/vSMA con estos pasos:

- Ejecute el comando updateconfig y, a continuación, el subcomando dynamichost.
- Cambie el servidor a update-manifests.sco.cisco.com:443.

- Realice los cambios.

Para obtener más preguntas frecuentes sobre la migración, consulte el enlace: https://www.cisco.com/c/en/us/support/docs/security/email-security-virtual-appliance/215466-esa-sma-virtual-deployment-faq.pdf.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).