Entender as práticas recomendadas para migrar o ESA/SMA de hardware para o ESA/SMA virtual

Contents

Introdução

Este documento descreve as práticas recomendadas com relação à implantação, migração e configuração de ESA/SMA de hardware para ESA/SMA virtual.

Etapas essenciais

Etapa 1. Faça download da imagem do ESA virtual e implante a VM

É recomendável ter um Secure Email Gateway (ESA)/Security Management Appliance (SMA) virtual em execução na mesma versão do AsyncOS que o hardware antes de poder migrar a configuração. Você pode escolher a versão do AsyncOS mais próxima da versão em execução no seu equipamento e atualizá-la depois disso, se necessário, ou baixar a versão mais recente do AsyncOS.

As implantações nessas plataformas são suportadas: Microsoft Hyper-V, teclado/vídeo/mouse (KVM) e VMWare ESXi. Consulte o guia de instalação para obter mais detalhes: https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/Cisco_Content_S

Você pode fazer o download da imagem virtual no link: https://software.cisco.com/download/home/284900944/type/282975113/release/15.0.0.

Etapa 2. Obter licenças para o ESA/SMA virtual

Para poder atualizar o ESA/SMA virtual, primeiro você deve instalar suas licenças - você pode compartilhar as licenças existentes do seu hardware com o novo ESA virtual (ambos os ESAs podem ser executados juntos).

Para licenças Tradicionais, depois que a licença física tiver sido compartilhada com êxito para o vESA/vSMA e você tiver recebido sua licença, abra o .XML arquivo recebido com o NotePad++ ou WordPad. Selecione all e depois copie/cole via CLI vESA/vSMA usando o comandoloadlicense . Consulte o link para obter mais detalhes: https://www.cisco.com/c/en/us/support/docs/security/email-security-virtual-appliance/118301-technote-esa-00.html.

Para licenças Smart, adicione o novo vESA/vSMA na Smart Account, depois que o token for gerado, registre os dispositivos de acordo com o processo mencionado no artigo: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/214614-smart-licensing-

overview-and-best-practi.html.

Etapa 3. Atualize o ESA/SMA virtual para a versão AsyncOS exata do ESA/SMA de hardware (se necessário)

O hardware e o dispositivo virtual devem estar na mesma versão antes da migração. Você pode verificar a matriz de compatibilidade para o SMA e o ESA no link mencionado para atualizar o ESA para a versão apropriada: https://www.cisco.com/c/dam/en/us/td/docs/security/security_management/sma/sma_all/email-compatibility/index.html.

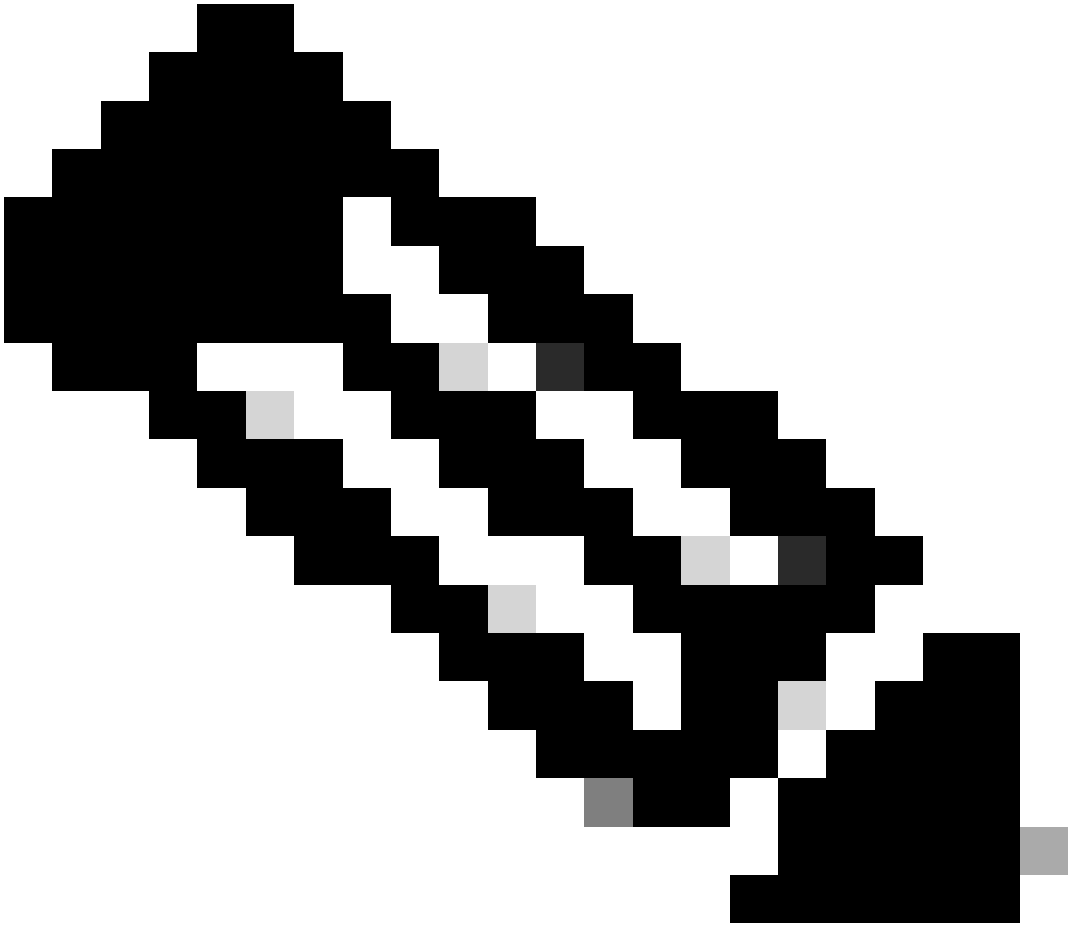
Etapa 4. Migrar a configuração existente do ESA/SMA de hardware para o ESA/SMA virtual

O ESA/SMA virtual pode ser configurado das seguintes maneiras:

- Configure os dispositivos desde o início se o hardware existente estiver chegando ao fim da vida útil (EOL)/fim do suporte (EOS) ou se a imagem vESA/SMA atualizada estiver instalada ou se for necessário configurar vários dispositivos.

- Se o dispositivo de hardware já estiver no cluster, adicione o novo vESA/vSMA ao cluster. Os novos dispositivos obtêm uma cópia da configuração existente do cluster.

- Se o dispositivo de hardware for um dispositivo autônomo, habilite a configuração do cluster e adicione o novo ESA/SMA virtual ao cluster para obter uma cópia da configuração existente.



Observação: depois que o ESA/SMA virtual obtém a configuração atual, você pode optar por desconectar os dispositivos do cluster ou mantê-los como estão com base no requisito. O dispositivo de hardware pode ser removido da configuração do cluster e descomissionado.

Etapa 5. Corrija o servidor atualizado no ESA/SMA virtual

O ESA/SMA virtual e de hardware usam servidores de atualização diferentes e, após a migração da configuração, o servidor é alterado. Para poder atualizar ainda mais seu vESA/vSMA, você pode corrigir o servidor através da CLI do vESA/vSMA com estas etapas:

- Execute o comando updateconfig e, em seguida, o subcomandodynamichost.

    - Alterar servidor para update-manifests.sco.cisco.com:443.

- Confirme as alterações.

Para obter mais perguntas frequentes sobre migração, consulte o link: https://www.cisco.com/c/en/us/support/docs/security/email-security-virtual-appliance/215466-esa-sma-virtual-deployment-faq.pdf.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.