# Comprendere le best practice per la migrazione di hardware ESA/SMA a Virtual ESA/SMA

## Sommario

## Introduzione

In questo documento vengono descritte le best practice relative all'installazione, alla migrazione e alla configurazione dall'hardware ESA/SMA a Virtual ESA/SMA.

## Fasi essenziali

### Passaggio 1. Scaricare l'immagine ESA virtuale e installare la VM

Prima di poter migrare la configurazione, si consiglia di eseguire un gateway di posta elettronica sicuro (ESA)/appliance di gestione della sicurezza (SMA) virtuale sulla stessa versione AsyncOS dell'hardware. È possibile scegliere la versione di AsyncOS più vicina alla versione in esecuzione sull'accessorio e aggiornarla successivamente, se necessario, oppure scaricare la versione più recente di AsyncOS.

Sono supportate le distribuzioni su queste piattaforme: Microsoft Hyper-V, Keyboard/Video/Mouse (KVM) e VMWare ESXi. Per ulteriori informazioni, consultare la guida all'installazione: https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/Cisco_Content_S

È possibile scaricare l'immagine virtuale dal seguente collegamento: https://software.cisco.com/download/home/284900944/type/282975113/release/15.0.0.

### Passaggio 2. Ottenere le licenze per l'ESA/SMA virtuale

Per poter aggiornare l'ESA/SMA virtuale, è necessario innanzitutto installare le relative licenze. È possibile condividere le licenze esistenti dall'hardware con la nuova ESA virtuale (entrambe le ESA possono funzionare insieme).

Per le licenze Traditional, una volta che la licenza fisica è stata condivisa per vESA/vSMA e si è ricevuta la licenza, aprire il file ricevuto con NotePad++ o WordPad,.XML. Selezionare all, quindi copiare/incollare tramite la CLI vESA/vSMA utilizzando il loadlicense comando. Fare riferimento al collegamento per ulteriori dettagli: https://www.cisco.com/c/en/us/support/docs/security/email-security-virtual-appliance/118301-technote-esa-00.html.

Per le licenze Smart, aggiungere il nuovo vESA/vSMA nello smart account, una volta generato il token, registrare i dispositivi secondo il processo indicato nell'articolo: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/214614-smart-licensing-overview-and-best-practi.html.

Passaggio 3. Aggiornare l'ESA/SMA virtuale alla versione AsyncOS esatta dell'ESA/SMA hardware (se necessario)

L'hardware e l'appliance virtuale devono trovarsi nella stessa versione prima della migrazione. Per aggiornare l'ESA alla versione corretta, è possibile controllare la matrice di compatibilità per l'SMA e l'ESA sul link indicato: https://www.cisco.com/c/dam/en/us/td/docs/security/security_management/sma/sma_all/email-compatibility/index.html.

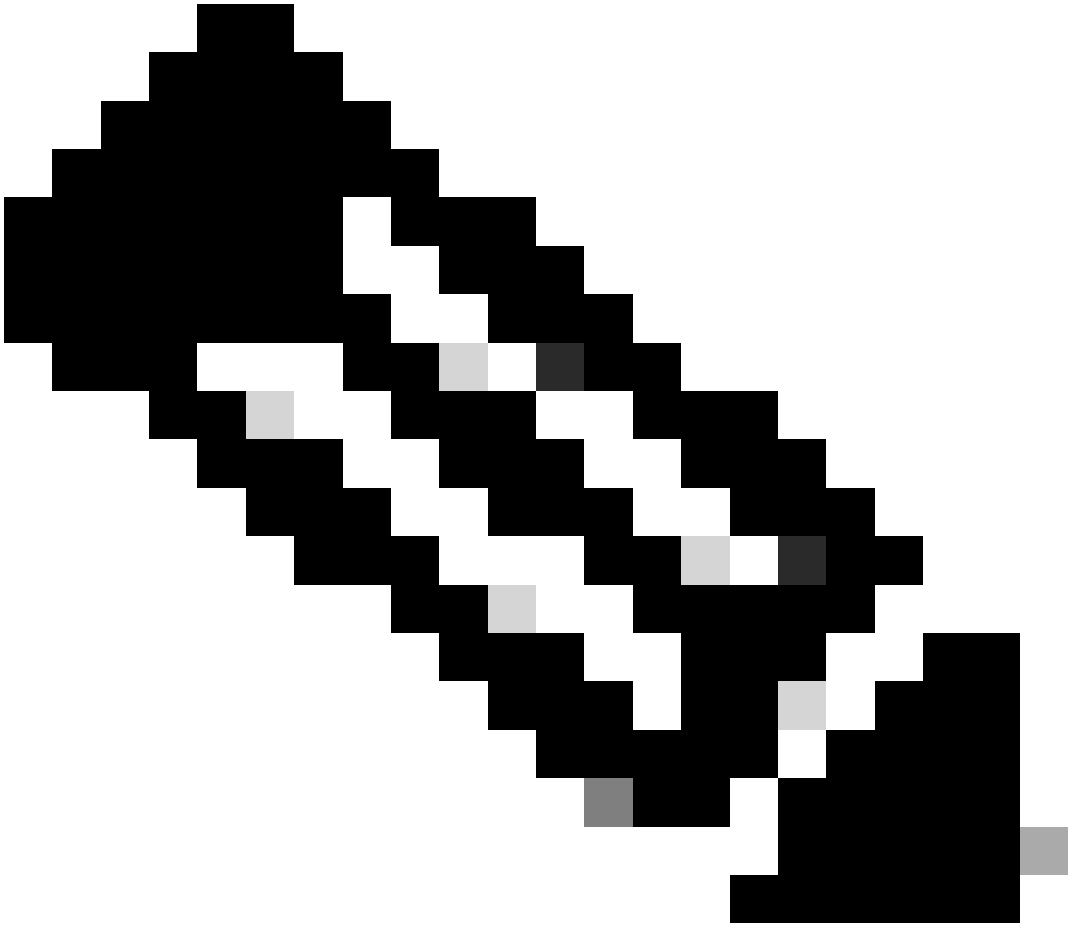
Passaggio 4. Migrazione della configurazione esistente dall'ESA/SMA hardware all'ESA/SMA virtuale

L'ESA/SMA virtuale può essere configurato nei modi seguenti:

- Configurare i dispositivi da zero se l'hardware esistente sta per raggiungere la fine del ciclo di vita (EOL)/fine del supporto (EOS) o se è installata l'immagine vESA/SMA aggiornata o se è necessario configurare più dispositivi.

- Se il dispositivo hardware è già presente nel cluster, aggiungere il nuovo vESA/vSMA al cluster. I nuovi dispositivi ottengono una copia della configurazione esistente dal cluster.

- Se il dispositivo hardware è un dispositivo standalone, abilitare la configurazione del cluster e aggiungere il nuovo ESA/SMA virtuale al cluster per ottenere una copia della configurazione esistente.



**Nota**: dopo che l'ESA/SMA virtuale ha ottenuto la configurazione corrente, è possibile scegliere di disconnettere i dispositivi dal cluster o di mantenerli così come sono in base ai requisiti. È possibile rimuovere il dispositivo hardware dalla configurazione del cluster e rimuovere le autorizzazioni.

---

Passaggio 5. Correggere il server aggiornato sull'ESA/SMA virtuale

L'ESA/SMA virtuale e hardware utilizzano server di aggiornamento diversi e, dopo la migrazione della configurazione, il server cambia. Per poter aggiornare ulteriormente vESA/vSMA, è possibile correggere il server tramite la CLI di vESA/vSMA procedendo come segue:

- Eseguire il comando updateconfig, quindi il sottocomando dynamichost.

    - Cambiare il server in update-manifests.sco.cisco.com:443.
- Eseguire il commit delle modifiche.

Per ulteriori domande frequenti sulla migrazione, fare riferimento al collegamento: https://www.cisco.com/c/en/us/support/docs/security/email-security-virtual-appliance/215466-esa-sma-virtual-deployment-faq.pdf.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).