Rétablir la configuration initiale de ESA et SMA

Table des matières

Introduction

Solution

Appareils matériels (ESA/SMA)

Appliances virtuelles (ESA/SMA)

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

Déploiement de cloud public

- Azure
- AWS
- GCP

Introduction

Ce document décrit la procédure de rétablissement et de redéploiement d'un appareil de sécurité de la messagerie (ESA) ou d'un appareil de gestion de la sécurité (SMA).

Solution

Appareils matériels (ESA/SMA)

Étapes de nettoyage et de rétablissement d'une appliance physique.

1. Établissez une connexion SSH avec l'appliance et exécutez la version et notez la version active en cours d'exécution sur l'appliance.

2. Exécutez Revert, sélectionnez une version du code antérieure à From #1 et tapez Y.

```
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
```



Avertissement : Cette procédure effacera la configuration, les données et l'historique des mises à niveau sur l'appliance

---

4. Laissez la machine terminer le rétablissement et il est prévu qu'il prenne environ 30 minutes pour terminer.

3. Une fois le rétablissement terminé et l'appareil activé, accédez de nouveau à la ligne de commande et exécutez Recharger via Diagnostic.

```
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.
```

Appliances virtuelles (ESA/SMA)

Pour plus d'informations sur la configuration matérielle requise, reportez-vous à la page https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/Cisco_Content_S

VMware ESXi

1. Téléchargez l'image de l'appliance virtuelle et le hachage MD5 depuis Cisco.
2. Décompressez le fichier .zip de l'appliance virtuelle dans son propre répertoire ; Par exemple, C:\vESA\C100V.
3. Ouvrez le client VMware vSphere sur votre machine locale.
4. Sélectionnez l'hôte ou le cluster ESXi vers lequel vous souhaitez déployer l'appliance virtuelle.
5. Choisissez Fichier > Déployer le modèle OVF.
6. Entrez le chemin d'accès au fichier OVF dans le répertoire que vous avez créé et cliquez sur Next. Terminez l'Assistant.
7. Si le protocole DHCP est désactivé, configurez l'appliance sur votre réseau. Installez le fichier de licence.
8. Connectez-vous à l'interface utilisateur Web de votre appliance et configurez le logiciel de l'appliance.

Microsoft Hyper-V

1. Téléchargez l'image de l'appliance virtuelle et le hachage MD5 depuis Cisco.

2. Ouvrez le Gestionnaire Hyper-V et utilisez l'Assistant Nouvel ordinateur virtuel pour créer un nouvel ordinateur virtuel.

3. Affectez les ressources matérielles recommandées. (reportez-vous au guide d'installation virtuelle)

4. Connectez l'image de l'appliance virtuelle téléchargée en tant que disque dur virtuel. Terminez l'Assistant et démarrez l'ordinateur virtuel.

5. Si le protocole DHCP est désactivé, configurez l'appliance sur votre réseau. Installez le fichier de licence.

6. Connectez-vous à l'interface utilisateur Web de votre appliance et configurez le logiciel de l'appliance.

KVM

Déployez la machine virtuelle à l'aide de Virtual Machine Manager. Téléchargez l'image de

l'appliance virtuelle et le hachage MD5 depuis Cisco,

1. Lancez l'application virt-manager. Sélectionnez Nouveau.

2. Entrez un nom unique pour votre appliance virtuelle. Sélectionnez Importer une image existante.

3. Sélectionnez Forward, entrez les options OS Type : UNIX, version : FreeBSD 13.

4. Recherchez et sélectionnez l'image de l'appliance virtuelle qui a été téléchargée, puis sélectionnez Transférer.

5. Entrez les valeurs de mémoire vive et de processeur pour le modèle d'appareil virtuel qui doit être déployé. (reportez-vous au guide d'installation virtuelle)

6. Sélectionnez Forward, activez la case à cocher Customize et sélectionnez Finish.

7. Configurez l'unité de disque. Dans le volet de gauche, sélectionnez le lecteur et sous Options avancées, Disk bus: Virtio, Storage format: qcow2 et sélectionnez Apply.

8. Configurez le périphérique réseau pour l'interface de gestion. Dans le volet de gauche, sélectionnez une carte réseau et les options de sélection Source Device : Votre Vlan De Gestion, Modèle De Périphérique : virtIO, mode source : VEPA, sélectionnez Apply.

9. Configurez les périphériques réseau pour des interfaces supplémentaires. Répétez l'étape 8 pour chaque interface ajoutée à la machine virtuelle.

10. Sélectionnez Commencer l'installation.

Nutanix

1. Téléchargez l'image de l'appliance virtuelle et le hachage MD5 depuis Cisco.

2. Accédez à Nutanix Prism, décompressez l'image qcow2 de l'appliance virtuelle et téléchargez-la dans votre pool de stockage.

3. Cliquez sur l'icône Hamburger dans le coin supérieur gauche du tableau de bord Prism de Nutanix, sélectionnez Compute and Storage > VM dans le volet de navigation de gauche.

4. Cliquez sur le bouton Créer une VM, entrez les détails pour configurer la VM et cliquez sur Suivant.

5. Configurez les ressources matérielles en fonction du modèle (reportez-vous au guide d'installation virtuelle)

6. Cliquez sur le bouton Attach Disk sous Disks et sélectionnez, Clone from Image de la liste déroulante Operation et a téléchargé l'image qcow2 de la liste déroulante Image.

7. Cliquez sur le bouton Attach to Subnet sous Networks et configurez les paramètres de l'interface réseau.

8. Exécutez l'assistant pour déployer l'appliance virtuelle sur Nutanix Prism.

Déploiement de cloud public

Pour obtenir des informations et connaître la procédure de déploiement de l'ESA et du SMA sur le cloud public, consultez le site https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/ESA_SMA_Virtua

Azure

1. Créez les composants du besoin.

2. Obtenez l'image de la VM.

3. Configurer le contrôle d'accès - Gestion des identités et des accès (IAM)

4. Connectez-vous et créez la VM.

Reportez-vous aux pages 4 à 18 du guide de déploiement des clouds publics pour obtenir la procédure détaillée de déploiement de la machine virtuelle sur Azure.

AWS

1. Contactez le TAC Cisco pour obtenir l'ID AMI.

2. Ouvrez la console Amazon EC2.

3. Sélectionnez AMI dans le volet de navigation.

4. Choisissez Public Images dans le premier filtre.

5. Dans la barre de recherche, entrez le « numéro de build » et le « modèle » en fonction du modèle d'appareil virtuel requis.

Reportez-vous aux pages 19 à 29 du guide de déploiement des clouds publics pour obtenir la procédure détaillée de déploiement de la machine virtuelle sur AWS.

GCP

1. Préparez l'environnement et configurez l'ordinateur virtuel.

2. Sélectionnez OS et Storage.

3. Configurez le réseau, le pare-feu et l’interface réseau.

4. Configurez la machine virtuelle.

Reportez-vous aux pages 30 à 34 du guide de déploiement des clouds publics pour connaître la procédure détaillée de déploiement de la machine virtuelle sur GCP.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.