Reverter ESA e SMA para a configuração original

Contents

Introdução

Este documento descreve o procedimento para reverter e reimplantar um Email Security Appliance (ESA) ou Security Management Appliance (SMA).

Solução

Dispositivos de hardware (ESA/SMA)

Etapas para limpar e reverter um dispositivo físico.

1. SSH para o equipamento e executar a versão e anotar a versão ativa em execução no equipamento.

2. Execute Reverter, selecione uma versão do código que seja mais antiga que De #1 e digite 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
```

aviso: Este procedimento apagará a configuração, os dados e o histórico de atualizações no dispositivo

---

4. Deixe que a máquina conclua a reversão e espera-se que ela demore aproximadamente 30 minutos para ser concluída.

3. Quando a reversão for concluída e o equipamento estiver ativado, acesse a linha de comando novamente e execute Recarregar via Diagnóstico.

```
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.
```

Dispositivos virtuais (ESA / SMA)

Para obter informações sobre requisitos de hardware, consulte a plataforma de hipervisor suportada em https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/Cisco_Content_S

VMware ESXi

1. Faça download da imagem do dispositivo virtual e do hash MD5 da Cisco.
2. Descompacte o arquivo .zip do equipamento virtual em seu próprio diretório; Por exemplo, C:\vESA\C100V.
3. Abra o VMware vSphere Client no computador local.
4. Selecione o host ou cluster ESXi no qual deseja implantar o dispositivo virtual.
5. Escolha File > Deploy OVF template.
6. Insira o caminho para o arquivo OVF no diretório criado e clique em Avançar. Conclua o assistente.
7. Se o DHCP estiver desabilitado, configure o equipamento na rede. Instale o arquivo de licença.
8. Faça login na interface do usuário da Web do seu equipamento e configure o software do equipamento.

Microsoft Hyper-V

1. Faça download da imagem do dispositivo virtual e do hash MD5 da Cisco.

2. Abra o Hyper-V Manager, use o "Assistente de Nova Máquina Virtual" para criar uma nova máquina virtual.

3. Atribua os recursos de hardware recomendados. (consulte o guia de instalação virtual)

4. Anexe a imagem do dispositivo virtual baixado como o disco rígido virtual. Conclua o assistente e inicie a máquina virtual.

5. Se o DHCP estiver desativado, configure o equipamento na rede. Instale o arquivo de licença.

6. Faça login na interface do usuário da Web do seu equipamento e configure o software do equipamento.

KVM

Implante a máquina virtual usando o Virtual Machine Manager. Faça download da imagem do

dispositivo virtual e do hash MD5 da Cisco,

1. Inicie o aplicativo virtual manager. Selecione New.

2. Insira um nome exclusivo para o dispositivo virtual. Selecione Importar imagem existente.

3. Selecione Forward, insira as opções OS Type: UNIX, version: FreeBSD 13.

4. Procure e selecione a imagem do equipamento virtual que foi baixada e selecione Forward.

5. Insira os valores de RAM e CPU para o modelo de dispositivo virtual que precisa ser implantado. (consulte o guia de instalação virtual)

6. Selecione Encaminhar, marque a caixa de seleção Personalizar e selecione Finalizar.

7. Configure a unidade de disco. No painel esquerdo, selecione a unidade e, em Advanced Options, Disk bus: Virtio, Storage format: qcow2 e selecione Apply.

8. Configure o dispositivo de rede para a interface de gerenciamento. No painel esquerdo, selecione uma placa de rede e as opções de seleção Dispositivo de origem: Sua VLAN de gerenciamento, Modelo do dispositivo: virtIO, modo Origem: VEPA, selecione Apply.

9. Configure dispositivos de rede para interfaces adicionais, repita a etapa 8 para cada interface adicionada à máquina virtual.

10. Selecione Iniciar Instalação.

Nutanix

1. Faça download da imagem do dispositivo virtual e do hash MD5 da Cisco.

2. Acesse o Nutanix Prism, descompacte a imagem qcow2 do dispositivo virtual e carregue-a no pool de armazenamento.

3. Clique no ícone Hamburger no canto superior esquerdo do painel Nutanix Prism e selecione Compute and Storage > VM no painel de navegação esquerdo.

4. Clique no botão Criar VM, insira os detalhes para configurar a VM e clique em Avançar.

5. Configurar recursos de hardware com base no modelo (consulte o guia de instalação virtual)

6. Clique no botão Anexar Disco em Discos e selecione, Clonar da Imagem na lista drop-down Operação e faça upload da imagem da lista drop-down Imagem .

7. Clique no botão Attach to Subnet em Networks e configure a interface de rede.

8. Conclua o assistente para implantar o Dispositivo virtual no Nutanix Prism.

Implantação de nuvem pública

Para obter informações e o procedimento para implantar ESA e SMA na nuvem pública, consulte https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/ESA_SMA_Virtua

Azure

1. Crie os componentes da necessidade.

2. Obtenha a imagem da VM.

3. Configurar Controle de Acesso - Gerenciamento de Identidade e Acesso (IAM)

4. Faça login e crie a VM.

Consulte as páginas 4 a 18 do guia de implantação para nuvens públicas para obter o procedimento detalhado para implantar a máquina virtual no Azure.

AWS

1. Entre em contato com o TAC da Cisco para obter a ID do AMI.

2. Abra o console Amazon EC2.

3. Escolha AMIs no painel de navegação.

4. Escolha Imagens Públicas no primeiro filtro.

5. Na barra de pesquisa, insira o "número da compilação" e o "modelo" de acordo com o modelo de dispositivo virtual necessário.

Consulte as páginas 19 a 29 do guia de implantação para nuvens públicas para obter procedimentos detalhados para implantar a máquina virtual no AWS.

GCP

1. Prepare o ambiente e configure a máquina virtual.

2. Escolha SO e Armazenamento.

3. Configure a rede, o firewall e a interface de rede.

4. Configure a Máquina Virtual.

Consulte as páginas 30 a 34 do guia de implantação para nuvens públicas para obter procedimentos detalhados para implantar a máquina virtual no GCP.

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.