

ESA en SMA terugzetten naar oorspronkelijke configuratie

Inhoud

[Inleiding](#)

[Oplossing](#)

[Hardwareapparaten \(ESA/SMA\)](#)

[Virtuele apparaten \(ESA / SMA\)](#)

[ESXi van VMware](#)

[Microsoft Hyper-V](#)

[KVM](#)

[Nutanix](#)

[Publieke cloudimplementatie](#)

[Azure](#)

[AWS](#)

[GCP](#)

Inleiding

In dit document wordt de procedure beschreven voor het terugzetten en opnieuw implementeren van een e-mailbeveiligingsapparaat (ESA) of beveiligingsbeheerapparaat (SMA).

Oplossing

Hardwareapparaten (ESA/SMA)

Stappen om een fysiek apparaat te reinigen en terug te zetten.

1. SSH naar het toestel en voer de versie uit en noteer de actieve versie die op het toestel draait.
2. Voer Omkeren uit, selecteer een versie van de code die ouder is dan Van #1 en typ 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



Waarschuwing: met deze procedure worden de configuratie, gegevens en geschiedenis van upgrades op het toestel gewist

4. Laat de machine volledig omkeren en het duurt naar verwachting ongeveer 30 minuten om te voltooien.

3. Zodra het terugzetten is voltooid en het toestel is ingeschakeld, opent u de opdrachtregel opnieuw en voert u het opnieuw laden uit 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.

## Virtuele apparaten (ESA / SMA)

Voor informatie over hardwarevereisten en het ondersteunde hypervisorplatform verwijzen wij u naar

[https://www.cisco.com/c/dam/en/us/td/docs/security/content\\_security/virtual\\_appliances/Cisco\\_Content\\_S](https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/Cisco_Content_S)

### ESXi van VMware

1. Download het image van het virtuele apparaat en de MD5-hash van Cisco.
2. Pak het .zip-bestand voor het virtuele toestel uit in zijn eigen directory, bijvoorbeeld C:\vESA\C100V.
3. Open de VMware vSphere-client op uw lokale computer.
4. Selecteer de ESXi-host of het ESXi-cluster waarop u het virtuele toestel wilt implementeren.
5. Kies Bestand > OVF-sjabloon implementeren.
6. Voer het pad naar het OVF-bestand in in de map die u hebt gemaakt en klik op Volgende. Voltooi de wizard.
7. Als DHCP is uitgeschakeld, stelt u het toestel in op uw netwerk. Het licentiebestand installeren.
8. Meld u aan bij de web-gebruikersinterface van uw toestel en configureer de toestelsoftware.

### Microsoft Hyper-V

1. Download het image van het virtuele toestel en de MD5-hash van Cisco.
2. Open Hyper-V Manager en gebruik de wizard Nieuwe virtuele machine om een nieuwe virtuele machine te maken.
3. Wijs de aanbevolen hardwarebronnen toe. (Raadpleeg de virtuele installatiehandleiding)
4. Koppel het gedownloade image van het virtuele toestel aan de virtuele harde schijf. Voltooi de wizard en start de virtuele machine.
5. Als DHCP is uitgeschakeld, stelt u het toestel in op uw netwerk. Het licentiebestand installeren.
6. Meld u aan bij de web-gebruikersinterface van uw toestel en configureer de toestelsoftware.

### KVM

Virtuele machine implementeren met Virtual Machine Manager. Download het image van het virtuele apparaat en de MD5-hash van Cisco,

1. Start de virt-manager-toepassing. Selecteer Nieuw.

2. Voer een unieke naam in voor uw virtuele toestel. Selecteer Bestaande image importeren.
3. Selecteer Doorsturen, voer opties in Type besturingssysteem: UNIX, versie: FreeBSD 13.
4. Blader en selecteer het gedownload image van het virtuele toestel en selecteer Doorsturen.
5. Voer RAM- en CPU-waarden in voor het virtuele toestelmodel dat moet worden geïmplementeerd. (Raadpleeg de virtuele installatiehandleiding)
6. Selecteer Doorsturen, selecteer het selectievakje Aanpassen en selecteer Voltooien.
7. Configureer het schijfstation. Selecteer in het linkerdeelvenster het station en selecteer onder Geavanceerde opties, Schijfbus: Virtio, Opslagformaat: qcow2 en selecteer Toepassen.
8. Configureer het netwerkkapparaat voor de beheerinterface. Selecteer in het linkerdeelvenster een netwerkinterfacekaart en selectieopties Bron: uw beheer-VLAN, Apparaatmodel: virtIO, Bronmodus: VEPA, selecteer Toepassen.
9. Configureer netwerkkapparaten voor extra interfaces en herhaal stap 8 voor elke interface die aan de virtuele machine is toegevoegd.
10. Selecteer Installatie starten.

## Nutanix

1. Download het image van het virtuele toestel en de MD5-hash van Cisco.
2. Toegang tot Nutanix Prism, untar het virtuele toestel qcow2 beeld en upload het naar uw opslagpool.
3. Klik op het pictogram Hamburger in de linkerbovenhoek van het Nutanix Prism-dashboard en selecteer Compute and Storage > VM in het linkernavigatiedeelvenster.
4. Klik op de knop VM maken, voer de gegevens in om de VM te configureren en klik op Volgende.
5. Configureer hardwarebronnen op basis van het model (raadpleeg de virtuele installatiehandleiding)
6. Klik op de knop Schijf koppelen onder Schijven en selecteer Klonen van afbeelding in de vervolgkeuzelijst Bewerking en qcow2-afbeelding uploaden uit de vervolgkeuzelijst Afbeelding .
7. Klik op de knop Bijvoegen aan subnet onder Netwerken en configureer de instellingen voor de netwerkinterface.
8. Vul de wizard in om het virtuele apparaat te implementeren op Nutanix Prism.

## Publieke cloudimplementatie

Voor informatie en procedures voor de implementatie van ESA & SMA in de publieke cloud verwijzen wij u naar

[https://www.cisco.com/c/dam/en/us/td/docs/security/content\\_security/virtual\\_appliances/ESA\\_SMA\\_Virtua](https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/ESA_SMA_Virtua)

## Azure

1. Maak de vereiste componenten.
2. Zorg voor het VM-image.
3. Toegangscontrole configureren - Identiteits- en toegangsbeheer (IAM)
4. Log in en maak de VM.

Zie pagina 4 tot en met 18 van de implementatiegids voor openbare clouds voor gedetailleerde procedures voor het implementeren van de virtuele machine op Azure.

## AWS

1. Neem contact op met Cisco TAC om de AMI ID te verkrijgen.
2. Open de Amazon EC2-console.
3. Kies AMI's in het navigatiedeelvenster.
4. Kies Openbare afbeeldingen in het eerste filter.
5. Voer in de zoekbalk het "buildnummer" en het "model" in volgens het vereiste virtuele toestelmodel.

Zie pagina 19 tot en met 29 van de implementatiegids voor openbare clouds voor gedetailleerde procedures voor het implementeren van de virtuele machine op AWS.

## GCP

1. De omgeving voorbereiden en de virtuele machine configureren.
2. Kies besturingssysteem en opslag.
3. Configureer de netwerk-, firewall- en netwerkinterface.
4. Virtuele machine configureren.

Zie pagina 30 tot en met 34 van de implementatiegids voor openbare clouds voor gedetailleerde procedures voor de implementatie van de virtuele machine op GCP.

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.