

Waarschuwingsbericht na-AsyncOS-upgrade, "sofos-antivirus - De anti-virusdatabase op dit systeem is verlopen"

Inhoud

[Inleiding](#)

[Waarschuwingsbericht na-AsyncOS-upgrade, "sofos-antivirus - De anti-virusdatabase op dit systeem is verlopen"](#)

[Huidige versie controleren](#)

[Force Update Sfos](#)

Inleiding

Dit document beschrijft waarom een Cisco Email Security Appliance (ESA) beheerder een waarschuwingsbericht van een apparaat ontvangt na een upgrade waarin staat dat de SophoS Anti-Virus database is verlopen.

Bijgedragen door Dominic Yip en Stephan Bayer, Cisco TAC Engineers.

Waarschuwingsbericht na-AsyncOS-upgrade, "sofos-antivirus - De anti-virusdatabase op dit systeem is verlopen"

Op een ESA, nadat u hebt geupgrade naar een nieuwe versie van AsyncOS en de vereiste herstart hebt voltooid, kan een beheerder een gelijkaardig waarschuwingsbericht ontvangen:

The Warning message is:

```
sophos antivirus - The Anti-Virus database on this system is expired. Although the system will continue to scan for existing viruses, new virus updates will no longer be available. Please run avupdate to update to the latest engine immediately. Contact Cisco IronPort Customer Support if you have any questions.
```

Current Sophos Anti-Virus Information:

```
SAV Engine Version 5.33
IDE Serial Unknown
Last Engine Update Tue Mar 7 01:19:08 2017
Last IDE Update Tue Mar 7 01:19:08 2017
```

```
Version: 11.0.0-028
Serial Number: 111A80C64EA901221AAA-1A11EB54A111
Timestamp: 13 Mar 2017 14:57:21 -0400
```

Dit waarschuwingsbericht geeft aan dat de bijbehorende database en het regelingspakket van de anti-virusmotor niet actueel zijn voor de aangepaste versie van AsyncOS bij het opstarten van het apparaat. De ESA zal na haar online verschijnen controleren op bijgewerkte motoren tegen

virussen en zal de huidige versie bijwerken.

Huidige versie controleren

Om de motorversie van Sofos te controleren, moet **antivirusstatus sofos** (of **avstatus sofos**) in het CLI worden opgenomen om de huidige versie van de anti-virusmotor te bekijken.

```
myesa.local> avstatus sophos
```

```
SAV Engine Version 3.2.07.366.3_5.36
IDE Serial 2017032603
Last Engine Update 26 Mar 2017 13:24 (GMT +00:00)
Last IDE Update 26 Mar 2017 13:24 (GMT +00:00)
```

Vergelijk de versie van het eerder ontvangen waarschuwingsbericht met de uitvoer van de motorversie van de statusopdracht. Nadat u hebt verklaard dat het apparaat is verlopen en bijgewerkt, kunt u dit waarschuwingsbericht veilig negeren.

Force Update Sfos

U kunt ook de commando **avupdate force** invoeren om te vragen om een onmiddellijke update van de anti-virusmotor en de regels. Nadat u de force opdracht hebt ingevoerd, voer u **tail update_logs in** om de update in uitvoering te zien. Dit kan een paar minuten duren om de update te bereiken, de juiste pakketten te verkrijgen en dan te downloaden en te installeren zoals nodig. Een voorbeeld hiervan is:

```
(myesa.local)> avupdate force
```

```
Sophos Anti-Virus updates:
Requesting forced update of Sophos Anti-Virus.
McAfee Anti-Virus updates:
Requesting update of virus definitions
(Machine 122.local)> tail updater_logs
```

Press Ctrl-C to stop.

```
Sun Mar 26 09:20:39 2017 Info: Server manifest specified an update for sophos
Sun Mar 26 09:20:39 2017 Info: sophos was signalled to start a new update
Sun Mar 26 09:20:39 2017 Info: sophos processing files from the server manifest
Sun Mar 26 09:20:39 2017 Info: sophos started downloading files
Sun Mar 26 09:20:39 2017 Info: sophos waiting on download lock
Sun Mar 26 09:20:39 2017 Info: sophos acquired download lock
Sun Mar 26 09:20:39 2017 Info: sophos beginning download of remote file
"http://stage-updates.ironport.com/sophos/4.4/ide/default_esa/1490526336"
Sun Mar 26 09:20:41 2017 Info: sophos released download lock
Sun Mar 26 09:20:41 2017 Info: sophos successfully downloaded file
"sophos/4.4/ide/default_esa/1490526336"
Sun Mar 26 09:20:41 2017 Info: sophos waiting on download lock
Sun Mar 26 09:20:41 2017 Info: sophos acquired download lock
Sun Mar 26 09:20:41 2017 Info: sophos beginning download of remote file
"http://stage-updates.ironport.com/sophos/libsavi/1488816512"
Sun Mar 26 09:24:58 2017 Info: sophos released download lock
Sun Mar 26 09:24:58 2017 Info: sophos successfully downloaded file
"sophos/libsavi/1488816512"
Sun Mar 26 09:24:58 2017 Info: sophos started applying files
Sun Mar 26 09:24:58 2017 Info: sophos updating component ide
```

```
Sun Mar 26 09:24:58 2017 Info: sophos updating component libsavi
Sun Mar 26 09:24:58 2017 Info: sophos updated engine,ide links successfully
Sun Mar 26 09:24:58 2017 Info: sophos cleaning up base dir /data/third_party/sophos
Sun Mar 26 09:24:58 2017 Info: sophos sending version details
{'sophos': {'version': '5.36', 'ide': '2017032603'}} to hermes
Sun Mar 26 09:24:58 2017 Info: sophos verifying applied files
Sun Mar 26 09:24:58 2017 Info: sophos updating the client manifest
Sun Mar 26 09:24:58 2017 Info: sophos update completed
Sun Mar 26 09:24:58 2017 Info: sophos waiting for new updates
```

De sleutel in de update_logs om naar te zoeken is de "update voltooid" en "wachtend op nieuwe updates" loglijnen. Zodra deze worden weergegeven, kunt u de opdracht **avstatus sofs** opnieuw invoeren om te controleren of de versie en de datums zijn bijgewerkt.