

Actualización del poste-AsyncOS, “antivirus de los sophos - La base de datos del contra virus en este sistema es” mensaje de advertencia expirado

Contenido

[Introducción](#)

[Actualización del poste-AsyncOS, “antivirus de los sophos - La base de datos del contra virus en este sistema es” mensaje de advertencia expirado](#)

[Verifique la versión actual de Sophos](#)

[Fuerce la actualización Sophos](#)

Introducción

Este documento describe porqué un administrador del dispositivo de seguridad del correo electrónico de Cisco (ESA) recibe un mensaje de advertencia de un dispositivo después de una actualización que estado que está expirada la base de datos del contra virus de Sophos.

Contribuido por Dominic Yip y Stephan Bayer, los ingenieros de Cisco TAC.

Actualización del poste-AsyncOS, “antivirus de los sophos - La base de datos del contra virus en este sistema es” mensaje de advertencia expirado

En un ESA, después de que usted actualice a una nueva versión de AsyncOS y complete la reinicialización requerida, un administrador pudo recibir un mensaje de advertencia similar a esto:

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
```

Este mensaje de advertencia indica que la base de datos del motor antivirus y el paquete asociados de las reglas no son actuales para la versión actualizada de AsyncOS a la hora del lanzamiento del dispositivo. El ESA marcará para saber si hay actualizaciones del motor antivirus después de que venga en línea y se pondrá al día a la versión actual.

Verifique la versión actual de Sophos

Para verificar la versión del motor de Sophos, ingrese los **sophos del antivirusstatus** (o, los **sophos del avstatus**) en el CLI para ver la versión actual del motor del contra virus.

```
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)
```

Compare la versión del mensaje de advertencia recibido anterior al motor version output del comando status. Después de que usted valide que el dispositivo ha alcanzado hacia fuera y puesto al día, usted puede ignorar con seguridad este mensaje de advertencia.

Actualización Sophos de la fuerza

Usted puede también ingresar la **fuerza del avupdate del** comando para pedir una actualización inmediata al motor y a las reglas del contra virus. Después de que usted ingrese el comando de la fuerza, ingrese los **updater_logs de la cola** para ver la actualización en curso. Esto pudo tardar algunos minutos para alcanzar hacia fuera al updater, para conseguir los paquetes apropiados, y entonces para descargarlos y para instalarlos según las necesidades. Un ejemplo de esto es:

```
(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
```

La clave en los updater_logs a buscar es las líneas del registro para nuevas de las actualizaciones completadas” y “que esperan” de la “actualización. Una vez que se visualizan éstos, usted puede ingresar los **sophos del avstatus** ordena otra vez para verificar que la versión y las fechas sean actualizadas.