Aggiornamento dopo AsyncOS, messaggio di avviso "sofos antivirus - Il database antivirus sul sistema è scaduto"

Sommario

Introduzione

In questo documento viene illustrato il motivo per cui un amministratore di Cisco Email Security Appliance (ESA) riceve un messaggio di avviso da un accessorio dopo un aggiornamento in cui viene indicato che il database antivirus Sophos è scaduto.

Contributo di Dominic Yip e Stephan Bayer, Cisco TAC Engineers.

Aggiornamento dopo AsyncOS, messaggio di avviso "sofos antivirus - Il database antivirus sul sistema è scaduto"

Su un'ESA, dopo l'aggiornamento a una nuova versione di AsyncOS e il completamento del riavvio richiesto, un amministratore potrebbe ricevere un messaggio di avviso simile al seguente:

```
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
```

Questo messaggio di avviso indica che il database associato al motore antivirus e il pacchetto di regole non sono aggiornati per la versione aggiornata di AsyncOS al momento dell'avvio dell'accessorio. L'ESA verificherà la disponibilità di aggiornamenti del motore antivirus dopo la

connessione e si aggiornerà alla versione corrente.

Verifica versione Sophos corrente

Per verificare la versione del motore di Sophos, immettere **antivirusstatus sophos** (o **avstatus sophos**) nella CLI per visualizzare la versione corrente del motore antivirus.

```
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)
```

Confrontare la versione del messaggio di avviso ricevuto in precedenza con l'output della versione del motore del comando status. Dopo aver verificato che l'accessorio è stato raggiunto e aggiornato, è possibile ignorare questo messaggio di avviso.

Forza aggiornamento Sophos

Èinoltre possibile immettere il comando **avupdate force** per richiedere un aggiornamento immediato del motore antivirus e delle regole. Dopo aver immesso il comando force, immettere **tail updater_logs** per visualizzare l'aggiornamento in corso. L'operazione potrebbe richiedere alcuni minuti per raggiungere il programma di aggiornamento, ottenere i pacchetti appropriati, quindi scaricare e installare in base alle esigenze. Un esempio è:

```
(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 chiave nelle righe di log updater_logs da cercare è "aggiornamento completato" e "in attesa di nuovi aggiornamenti". Una volta visualizzate, è possibile immettere di nuovo il comando **avstatus sophos** per verificare che la versione e le date siano state aggiornate.