Mise à jour de POST-AsyncOS, « antivirus de sophos - La base de données d'antivirus sur ce système est » message d'avertissement expiré

Contenu

Introduction

Ce document décrit pourquoi un administrateur des appareils de sécurité du courrier électronique de Cisco (ESA) reçoit un message d'avertissement d'une appliance après une mise à jour cette déclare que la base de données d'antivirus de Sophos est expirée.

Contribué par Dominique Yip et Stephan Bayer, des ingénieurs TAC Cisco.

Mise à jour de POST-AsyncOS, « antivirus de sophos - La base de données d'antivirus sur ce système est » message d'avertissement expiré

Sur un ESA, après que vous amélioriez à une nouvelle version d'AsyncOS et vous terminiez la réinitialisation priée, un administrateur pourrait recevoir un message d'avertissement semblable à ceci :

```
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
```

Ce message d'avertissement indique que la base de données de l'engine d'antivirus et le module associés de règles ne sont pas en cours pour la version mise à jour d'AsyncOS au moment du startup d'appareils. L'ESA vérifiera des mises à jour d'engine d'antivirus après qu'il soit livré en ligne et les mettra à jour à la version en cours.

Vérifiez la version en cours de Sophos

Afin de vérifier la version d'engine de Sophos, entrez dans les **sophos d'antivirusstatus** (ou, des **sophos d'avstatus**) dans le CLI afin de visualiser la version en cours d'engine d'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)
```

Comparez la version du message d'avertissement reçu plus tôt à la sortie de version d'engine de la commande d'état. Après que vous validiez que l'appliance a atteint et mis à jour, vous pouvez sans risque ignorer ce message d'avertissement.

Mise à jour Sophos de force

Vous pouvez également écrire la **force d'avupdate de** commande afin de demander une mise à jour immédiate à l'engine et aux règles d'antivirus. Après que vous sélectionniez la commande de force, écrivez les **updater_logs de queue** afin de visualiser la mise à jour en cours. Ceci pourrait prendre quelques minutes pour atteindre à l'updater, pour obtenir les modules appropriés, et puis pour les télécharger et les installer comme nécessaires. Un exemple de ceci est :

```
(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 clé dans les updater_logs à rechercher est « mise à jour terminée » et les lignes de log « attendante nouvelles mises à jour ». Une fois que ceux sont affichés, vous pouvez entrer dans les **sophos d'avstatus** commandez de nouveau afin de vérifier que la version et les dates sont mises à jour.