AsyncOS 업그레이드 후, "sophos antivirus - 이 시스템의 안티바이러스 데이터베이스가 만료되었습니다." 경고 메시지

목차

소개

이 문서에서는 Cisco ESA(Email Security Appliance) 관리자가 Sophos Anti-Virus 데이터베이스가 만료되었음을 나타내는 업그레이드 후 어플라이언스에서 경고 메시지를 수신하는 이유에 대해 설명합니다.

기고자: Dominic Yip 및 Stephan Bayer, Cisco TAC 엔지니어

AsyncOS 업그레이드 후, "sophos antivirus - 이 시스템의 안티바이러스 데이터베이스가 만료되었습니다." 경고 메시지

ESA에서 새 버전의 AsyncOS로 업그레이드하고 필요한 재부팅을 완료하면 다음과 같은 경고 메시지가 관리자에게 표시될 수 있습니다.

```
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
```

이 경고 메시지는 어플라이언스 시작 시 업그레이드된 AsyncOS 버전에 대해 안티바이러스 엔진의 관련 데이터베이스 및 규칙 패키지가 최신 상태가 아님을 나타냅니다.ESA는 안티바이러스 엔진 업데이트가 온라인 상태가 된 후 업데이트를 확인하고 현재 버전으로 업데이트합니다.

현재 Sophos 버전 확인

Sophos 엔진 버전을 확인하려면 현재 Anti-Virusstatus **sophos**(또는 **avstatus** sophos)를 CLI에 입력하여 현재 Anti-Virus 엔진 버전을 확인합니다.

```
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)
```

앞에서 받은 경고 메시지의 버전을 status 명령의 엔진 버전 출력과 비교합니다. 어플라이언스가 도달 및 업데이트되었는지 확인한 후 이 경고 메시지를 무시해도 됩니다.

Sophos 강제 업데이트

안티바이러스 엔진 및 규칙에 대한 즉각적인 업데이트를 요청하기 위해 **avupdate force** 명령을 입력할 수도 있습니다.force 명령을 입력한 후 진행 중인 업데이트를 보려면 **tail updater_logs**를 입력합니다.업데이터에 연결하고 적절한 패키지를 가져온 다음 필요에 따라 다운로드하여 설치하는 데 몇 분 정도 걸릴 수 있습니다.예를 들면 다음과 같습니다.

```
(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
```

updater_logs에서 찾을 키는 "update completed" 및 "waiting for new updates" 로그 라인입니다.이러한 항목이 표시되면 **avstatus sophos** 명령을 다시 입력하여 버전 및 날짜가 업데이트되었는지 확인할 수 있습니다.