Post-AsyncOS-Upgrade, "sophos antivirus - Die Anti-Virus-Datenbank auf diesem System ist abgelaufen" Warnmeldung

Inhalt

Einführung

In diesem Dokument wird erläutert, warum ein Administrator der Cisco E-Mail Security Appliance (ESA) nach einem Upgrade, das besagt, dass die Sophos Anti-Virus-Datenbank abgelaufen ist, eine Warnmeldung von einer Appliance erhält.

Unterstützt von Dominic Yip und Stephan Bayer, Cisco TAC Engineers.

Post-AsyncOS-Upgrade, "sophos antivirus - Die Anti-Virus-Datenbank auf diesem System ist abgelaufen" Warnmeldung

Auf einer ESA erhält ein Administrator nach dem Upgrade auf eine neue Version von AsyncOS und dem Abschluss des erforderlichen Neustarts möglicherweise eine Warnmeldung wie die folgende:

```
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
```

Diese Warnmeldung weist darauf hin, dass die zugehörige Datenbank und das Regelpaket des Anti-Virus-Engines für die aktualisierte Version von AsyncOS zum Zeitpunkt des Systemstarts

nicht aktuell sind. Die ESA sucht nach Updates für die Anti-Virus-Engine, nachdem sie online ist, und aktualisiert sie auf die aktuelle Version.

Aktuelle Sophos-Version überprüfen

Um die Engine-Version von Sophos zu überprüfen, geben Sie **antivirusstatus sophos** (oder, **avstatus sophos**) in die CLI ein, um die aktuelle Version des Anti-Virus-Moduls anzuzeigen.

```
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)
```

Vergleichen Sie die Version der zuvor erhaltenen Warnmeldung mit der Ausgabe der Motorversion des Status-Befehls. Nachdem Sie überprüft haben, ob die Appliance abgelaufen und aktualisiert ist, können Sie diese Warnmeldung sicher ignorieren.

Sophos erzwingen

Sie können auch den Befehl **avupdate force** eingeben, um eine sofortige Aktualisierung der Anti-Virus-Engine und -Regeln anzufordern. Nachdem Sie den Befehl force eingegeben haben, geben Sie **tail updater_logs ein**, um die Aktualisierung anzuzeigen. Dies kann ein paar Minuten dauern, um zum Updater zu gelangen, die richtigen Pakete zu erhalten und dann nach Bedarf herunterzuladen und zu installieren. Ein Beispiel hierfür ist:

```
(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
```

Der Schlüssel in den updater_logs, nach dem gesucht werden soll, ist die "Update completed" und "Waiting for new updates" Protokollzeilen. Sobald diese angezeigt werden, können Sie den Befehl **avstatus sophos** erneut eingeben, um zu überprüfen, ob Version und Datum aktualisiert wurden.