Sophos Anti-Virus fuer Linux - Versteckte On-Access Scanner Debug Option

Date:	2021-05-12
modified:	2021-05-12
tags:	Sophos, Anti-Virus, Linux, Debug
description:	Sophos Versteckte Debug Option "OnAccessRecordAllScans"
category:	Misc
slug:	sophos-anti-virus-fuer-linux-versteckte-on-access-scanner-debug-option
Author:	Dominik Wombacher
lang:	de
transid:	sophos-anti-virus-for-linux-hidden-on-access-scan-debug-option
Status:	published

Ich musste lernen, dass es eine ziemliche Herausforderung sein kann, Performance Probleme im Zusammenhang mit Sophos Anti-Virus fuer Linux zu beheben oder Pfade mit hoher I/O-Last zu identifizieren, die eine angepasste Policy oder Exclusion brauchen koennten.

In einer Situation, in der SAV Prozesse eine 100%ige Last auf einem oder mehreren CPU-Kernen erzeugen, stimmt aber definitiv etwas nicht und muss genauer untersucht werden.

Sophos bietet zwar viele Einstellungen, aber nur sehr begrenzte Debug Moeglichkeiten, zumindest wenn man dem offiziellen Handbuch und der Knowledge Base glaubt.

Es gibt allerdings einen versteckten und nicht oeffentlich dokumentierten Parameter zur Protokollierung aller On-Access Scanner Aktivitaeten. Das kann allerdings eine Menge Daten generieren und sollte daher nur eine begrenzte Zeit waehrend dem Troubleshooting aktiviert werden.

Aktivieren:

```
/opt/sophos-av/bin/savconfig set OnAccessRecordAllScans enable

systemctl restart sav-protect
```

Log Dateien werden nach **/opt/sophos-av/tmp/** geschrieben, du solltest *sav-protect* beenden und die Logs an einen anderen Ort kopieren, bevor du den Debug Modus deaktivierst.

Deaktivieren:

```
/opt/sophos-av/bin/savconfig set OnAccessRecordAllScans disable

systemctl restart sav-protect
```

Es waere um einiges einfacher, wenn Sophos so etwas in der eigenen Dokumentation behandeln wuerde.