Sophos Anti-Virus for Linux - Hidden On-Access Scan debug option

Date: 2021-05-12
modified: 2021-05-12
Author: Dominik Wombacher

I had to learn that it can be quite challenging to troubleshoot performance issues related Sophos Anti-Virus for Linux or to identify paths with high I/O load that might require an adjusted Policy or even Exclude.

In a Situation were SAV processes generate 100% load on one or more CPU Cores, there is definitely something wrong that need a closer look.

Sophos does provide a lot of config settings but just very limited debug capabilities, at least when you trust the official manual and knowledge base.

But there is a hidden and not public documented config setting to log all On-Access Scan activities. For sure that might generate a huge amount of data and therefore should only activated a limited time during an ongoing troubleshooting session.

Activate:

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

systemctl restart sav-protect
```

Log files will be written to **/opt/sophos-av/tmp/**, you should stop *sav-protect* and copy the logs to another location before deativating the debug mode.

Deactivate:

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

systemctl restart sav-protect
```

It would actually be way easier if Sophos would cover such topics in their own documentation.