

E300 - Administrators Guide

FVST/SSI– Logs

Thyge Skoedt Steffensen (Delegate), 23-01-2017

E300 - Administrators Guide

Table of Contents

[Document History 2](#_Toc135321567)

[1 About This Document 2](#_Toc135321568)

[2 Logging – hvem, hvad, hvordan 2](#_Toc135321569)

[3 Eksempler 2](#_Toc135321570)

[4 Fastholdelse 2](#_Toc135321571)

# Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Changed By | Change |
| 1 | 18 May 2023 | Thyge Skødt Steffensen ([tst@delegate.dk](mailto:tst@delegate.dk)) | Initial document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# About This Document

This document is a technical manual for the administrator of the solution. It documents how the application logs, what is logged, where the records are located, logs retention and log cleanup.

# Logging – hvem, hvad, hvordan

## Hvordan bliver der logget

Rammeværktøjet der blandt andet er brugt til at bygge REST API’et i Python er Flask. Flask bruger standard Python logning og hvis ikke det er konfigureret skriver den til stdout og stderr som Linux’ standard error stream.

SOFI kører direkte på maskinerne/VMs der hoster løsnings og SOFI kører som en systemd process. systemd er et værktøj til Linux til at strømline konfiguration af system komponenter, her services. systemd håndtere blandt andet logs fra komponenter gennem systemd-journald og disse kan tilgås via journalctl værktøjet.

systemd processen er konfigureret til at køre SOFI fra docker compose filen, hvor SOFI er bruger standard log konfigurationen som skriver til stdout og stderr. Systemd fortolker bruger disse streams til at samle logs.

I Python implementering kan man lave logs ved f.eks. at kalde app.logger.info(”<log-besked>”) se blandt andet i GdprController.py (’ web/src/SAP/src/controllers/GdprController.py’).

## Hvordan tilgår man loggene

Loggene kan tilgås fra serveren der hoster den instans man gerne vil se logs fra. Brugeren man benytter, skal have lov at tilgå loggene, hvis ikke brugeren har adgang kan en bruger med sudo privilegere give adgang ved: sudo usermod -a -G systemd-journal <username>.

Kommandoen journalctl --unit=sofi.service --no-pager kan bruges til at se loggene fra SOFI. Man kan tilføje flaget -f for at følge logs live og --since (--since=yyyy-mm-dd).

Yderligere kan man benytte grep til at sortere outputtet til kun at vise bestemte log rækker. F.eks. hvis man kun vil se GDPR audit loggene kan man bruge grep "GDPR Audit".

## Fastholdelse

Ifølge <https://www.freedesktop.org/software/systemd/man/journald.conf.html#SystemMaxUse=> bliver /var/log/journal brugt til at persisteret loggene, hvis ikke den eksisterer eller er skriv bar bliver /run/log/journal brugt, som er en volatile in-memory filsystem.

* foodweb.opr.computerome.dk har IKKE /var/log/journal
* foodwebdev.opr.computerome.dk har /var/log/journal

Den kan som standard gemme 15% af disk kapaciteten og maks 4 GB, før at logs vil blive slettet – uagtet af deres alder.

Kigger man i cat /etc/systemd/journald.conf kan man se dev er konfigureret til persistent, hvor prod ikke er konfigureret.

* Dev: -bash-4.2$ journalctl -u sofi.service

-- Logs begin at Sat 2022-04-30 12:09:58 CEST, end at Fri 2023-05-19 11:28:26 CEST. –

* Prod: (base) [root@foodweb thyste]# journalctl -u sofi.service

-- Logs begin at Mon 2023-05-15 12:39:45 CEST, end at Fri 2023-05-19 11:33:01 CEST. –

Så vi er ikke compliant…

Jeg genstartede servicen den 11. maj, måske der ikke var aktivitet før den 15.?

Journal filer can be rotated, then compressed and move to a new location. In this location they can be for x amounts of days. Now we can ensure we fill up the drive, because journald is now longer or supervisor.

We can inspect the files with journalctl and using the –file option.

Det virker ikke til der er nogen god måde at rotate logs, det er en black box med guide fra vendors som vil sælge et produkt.

Man kan også spytte logs ud til sys-logs, til fil og flytte den. Det bliver kompleks og jeg kan ikke garantere det virker i det lange løb, hvad hvis storage bliver fyldt op?

Paywall artikel: <https://access.redhat.com/solutions/2263121>

Journald håndterer logs fra alle services…

Jeg har prøvet at lave en config på dev for at se hvad der sker. Der skal roterer hver dag.

Fra systemd version 236 og frem kan man specifere filer i systemd service filen. Vi kører 219 på CentOS 7. EOL er 30. juni 2024 – derefter skal de nok overveje at bruge Rocky i stedet.

# Eksempler