systemd-journald, systemd-journald.service, systemd-journald.socket, systemd-journald-dev-log.socket, systemd-journald-audit.socket

Service de journalisation

systemd-journald est un service système qui collecte et stocke des données de log. Il créé et maintient des journaux indexés basés sur les informations de logging qui sont reçus depuis une variété de sources :

- Logs du kernel, via kmsg
- Logs système simple, via syslog(3)
- Logs système structurés via l'api native sd_journal_print(4)
- Sortie est erreur standard des services système
- Enregistrements d'audit, via le sous-système d'audit

Le service collecte implicitement de nombreux champs de métadonnées pour chaque messages de log de manière sécurisé et inaltérable. Les données de log collectées sont principalement du texte, mais peuvent également inclure des données binaire. Tous les objets stockés dans le journal peuvent avoir une taille allant jusqu'à 2^64-1 octets

Par défaut, le journal stocke les données de logs dans /run/log/journal/. Vu que /run est volatile, les données de log sont perdue au redémarrage. Pour que les données soient persistantes, il suffit de créer /var/log/journal/, où systemd-journal va stocker les données :

```
mkdir -p /var/log/journal
systemd-tmpfiles -create -prefix /var/log/journal
```

Signaux

SIGUSR1 Demande au journal de vider /run dans /var. journalctl –flush utilise ce signal.

SIGUSR2 Demande une rotation immédiate des fichiers journaux. journalctl –rotate utilise ce signal.

SIGRTMIN+1 Demande que toutes les données de log non-écrite le soient sur disque. journalctl –sync utilise ce signal.

Kernel Command Line

Quelques paramètre de configuration de journald.conf peuvent être passés sur la ligne de commande du kernel :

systemd.journald.forward_to_syslog=

systemd.journald.forward_to_kmsg=

systemd.journald.forward_to_console=

systemd.journald.forward_to_wall= Active/désactive la collecte des messages dans syslog, kmsg, la console système, ou wall

Contrôle d'accès

Les fichiers journaux sont par défaut possédés et lisible par le groupe systemd-journal mais ne sont pas accessible en écriture. Ajouter un utilisateur à ce groupe lui permet de lire ces fichiers journaux.

Par défaut, chaque utilisateur loggé a sont propre jeu de fichiers journaux dans /var/log/journal. Ces fichiers ne sont pas possédés par l'utilisateur, cependant, pour éviter que l'utilisateur puisse y écrire directement. Au lieu de ça, les ACL sont utilisées pour s'assurer que l'utilisateur a les accès en lecture seule.

Des utilisateurs et groupes additionnels peuvent obtenir l'accès aux fichiers journaux via les ACL. Par exemple, pour donner l'accès aux membres de wheel et adm :

```
setfacl -Rnm g:wheel:rx,d:g:wheel:rx,g:adm:rx,d:g:adm:rx /var/log/journal/
```

Noter que cette commande va mettre à jours les ACL pour les fichiers journaux existants et pour les futures fichiers journaux créés dans /var/log/journal/

Fichiers

/etc/systemd/journald.conf Configure le comportement de systemd-journald

/run/log/journal/machine-id/*.journal

/run/log/journal/machine-id/*.journal~

/var/log/journal/machine-id/*.journal

/var/log/journal/machine-id/*.journal~ systemd-journald écrit les entrées dans les fichiers avec le suffix .journal. Si le service n'est pas stoppé proprement, ou si des fichiers sont corrompus, il sonts renommés en utilisant le suffix .journal~, et systemd-journald écrit un nouveau fichier.

/dev/kmsg

/dev/log

/run/systemd/journal/dev-log

/run/systemd/journal/socket

/run/systemd/journal/stdout Sockets et autres chemins que systemd-journald écoute qui sont visible dans le système de fichier. De plus, journald peut écouter les évènements d'audit en utilisant netlink.