journalctl

Gestion du journal systemd

Permet de requêter le contenu du journal systemd qui est écrit par systemd-journald.service. Sans paramètre, affiche tout le journal, en commençant par les entrées les plus anciennes

Si un ou plusieurs arguments de match sont passés, la sortie est filtrée en accord. Un match est dans le format "FIELD=VALUE" (ex : _SYSTEMD_UNIT=httpd.service), réferant aux composant d'une entrée de journal structuré. Voir systemd.journal-fields pour une liste de champs. Si plusieurs match sont spécifiés et matchant différents champs, les entrées de logs sont filtrés par les 2 (les entrées affichées matchent tous les champs). Si 2 matchs s'appliquent sur le même champs, les entrées affichées matchent une des valeurs du champs. Le caractère final '+' peut apparaître comme séparateur de mot entre les autres termes (OU logique)

OPTIONS

–no-full, –full, -l Réduit la taille des champs s'ils ne rentrent pas dans la largeur de colonne.

-a, –all Affiche tous les champs, même s'ils contiennent des cararctères non-imprimables ou sont très long

-f, –follow Affiche seulement les entrées de journal récent, et affiche les entrées en continue

-e, –pager-end Va immédiatement à la fin du journal dans le pager. Ne fonctionne qu'avec less

-n, –lines= Nombre de lignes à afficher (défaut : 10)

–no-tail Affiche toutes les lignes, même avec -f

-r, –reverse Les nouvelles entrées s'affiche en premier

-o, –output= Contrôle le formatage des entrées du journal. Prend une des options suivantes :

- **short** Est le défaut et génère une sortie la plus identique au formattage classique des fichiers syslogs, une entrée par ligne.
- **short-iso** Similaire, mais affiche les timestamp au format ISO 8601
- **short-precise** Similaire, mais affiche les timestamp avec une précision au microseconde.
- **short-monotonic** Similaire, mais affiche les timestamp monotonique
- **verbose** Affiche les entrée structurées avec tous les champs.
- **export** Sérialise le journal dans un flux binaire pour les sauvegardes et les transferts réseaux
- **json** Formate les entrées en structures de données JSON, une par ligne.
- **json-pretty** Similaire mais les formate sur plusieurs lignes
- **json-sse** Similaire, mais les format pour être utilisable pour Server-Sent Events
- **cat** Génère une sortie sans métadonnées, ni timestamp.

–utc Exprime de temps en UTC

-x, –catalog Ajoute les lignes de log avec les textes explicatifs du catalog de message. Cela va ajouter des textes d'aide aux messages de log dans la sortie si disponible.

-q, –quiet Supprime tous les message d'information (ex : –Logs begin at ...", "–Reboot –"), et tout messages de journaux système inaccessible quand lancé comme utilisateur normal.

-m, –merge Affiche les entrées de tous les journaux disponible, inclant ceux distants

-b [ID] [±offset], –boot=[ID] [±offset] Affiche les message d'un boot spécifique. Cela ajoute un match pour "_BOOT_ID=". L'argument peut être vide, dans ce cas, ajoute un match pour le boot courant.

–list-boots Affiche une liste de nombre de boots, leurs ID et le timestamp du premier et dernier message.

-k, –dmesg Affiche seulement les messages kernel. Implique -b et ajoute le match "_TRANSPORT=kernel"

-t, –identifier=SYSLOG_IDENTIFIER Affiche les messages pour l'identifiant syslog spécifié

-u, –unit=UNIT|PATTERN Affiche les messages pour l'unité spécifiée ou correspondant au motif. Peut être spécifié plusieurs fois

–user-unit= Affiche les messages pour l'unité de session utilisateur spécifié. Peut être spécifié plusieurs fois

-p, –priority= Filtre les messages par priorité ou plage de priorité. ("emerg" (0), "alert" (1), "crit" (2), "err" (3), "warning" (4), "notice" (5), "info" (6), "debug" (7))

-c, –cursor= Affiche le entrées depuis l'emplacement dans le journal spécifié par le curseur spécifié

–after-cursor= Affiche les entrées après l'emplacement spécifié par le curseur.

–show-cursor= Affiche le curseur après la dernière entrée

-S, –since=, -U, –until= Affiche les entrée depuis ou jusqu'à la date spécifiée. Le format devrait être au format "2012-10-30 18 :17 :16", voir systemd.time pour la spécification complète des dates.

-F, –field= Affiche toutes les valeurs possible que le champ spécifié peut prendre dans toutes les entrées du journal.

–system, –user Affiche les message des services système et kernel, ou de l'utilisateur courant. Non spécifié, affiche tous les messages que l'utilisateur peut voir.

-M, –machine= Affiche les messages d'un conteneur local.

-D DIR, –directory=DIR Répertoire où rechercher les journaux

–file=GLOB Opère sur les fichiers journaux spécifiés par le GLOB au lieu des chemins de journaux par défaut. Peut être spécifié plusieurs fois.

–root=ROOT Opère sur les catalogues sous le répertoire spécifié

–new-id128 Au lieu d'afficher le contenu du journal, génère un nouvel ID 128bits pour identifier les messages. C'est prévu pour les développeurs qui ont besoin d'un nouvel identifiant pour un nouveau message.

–header Affiche seulement les informations d'en-tête dus champs de journal accédés.

–disk-usage Affiche l'utilisation disque des fichiers journaux

–vacuum-size=, –vacuum-time=, –vaccum-files= Supprime les fichiers journaux archivés jusqu'à ce que l'espace disque qu'ils utilisent soit inférieur à la taille ou le nombre de journaux, ou postérieur à la date spécifié.

–list-catalog [128-bits ID...] Liste le contenu du catalogue de message.

–dump-catalog [128-bit-ID...] Affiche le contenu du catalogue de message

–update-catalog Met à jours les indexs de catalogue

–setup-keys Au lieu d'afficher le contenu des journaux, génère une nouvelle paire de clé pour FSS. Cela génère une clé de scellement et une clé de vérification. La clé de scellement est stockée dans le répertoire des journaux et devrait rester dans l'hôte. La clé de vérification devrait être stocké ailleurs.

–force Quand –setup-keys est passé et que FSS (Forward Secure Sealing) a déjà été configuré, recréé les clés FSS.

–interval= Spécifie l'interval de changement pour la clé en générant une paire de clé FSS avec –setup-keys. Un interval plus court augmente la consommation CPU mais raccourcis la plage de temps des altération de journaux indétectable. Défaut : 15min

–verify Vérifie le fichier journal pour sa consistance interne. Si le fichier a été généré avec FSS activé et la clé a été spécifiée dans –verify-key, l'authenticité du journal est vérifié.

–verify-key= Spécifie la clé de vérification FSS à utiliser pour l'opération –verify

–sync Demande au service de journalisation d'écrire toutes les données non-écrite dans les fichiers journaux

–flush Demande au service de journalisation de vider les logs stockés dans /run/log/journal dans /var/log/journal, si le stockage persistant est activé.

–rotate Demande au service de journalisation de tourner les fichiers journaux.

–no-pager N'utilise pas de pager.

Variables d'environnement

SYSTEMD_PAGER Pager à utiliser. Vide, ou 'cat' est équivalent à –no-pager

SYSTEMD_LESS Remplace les options par défaut de less ('FRSXMK')

Exemples

Collecter tous les logs
journalctl
Ajouter un match
journalctl _SYSTEMD_UNIT=avahi-daemon.service
Si 2 champs sont matchés, seules les entrées matchant les 2 expressions sont affichées
journalctl _SYSTEMD_UNIT=avahi-daemon.service _PID=28097
Si 2 matchs réfèrent au même champ, toutes les entrées matchant une des expression sont affichés
journalctl _SYSTEMD_UNIT=avahi-daemon.service _SYSTEMD_UNIT=dbus.service
Avec '+', 2 expression peuvent être combinées
journalctl _SYSTEMD_UNIT=avahi-daemon.service _PID=28097 + _SYSTEMD_UNIT=dbus.service
Affiche tous les logs générés par DBus
journalctl /usr/bin/dbus-daemon
Affiche tous les logs kernel du boot précédent
journalctl -k -b -1
Affiche un log du service système apache.service
journalctl -f -u apache