|  |  |
| --- | --- |
| Best 20 NuGet syslog Packages - NuGet Must Haves Package | **Interrogation des journaux**  **La journalisation avec systemd** |

# Introduction

La commande *journalctl* est une commande permettant d'**afficher les journaux collectés par *systemd***.   
Le **service systemd-journald** est responsable de la **collecte des journaux de systemd** et **récupère les messages du noyau, des services *systemd* et d’autres sources**.

Ces journaux sont **regroupés dans un emplacement central**, ce qui facilite leur consultation.   
Les enregistrements de journal dans le journal sont **structurés et indexés**.   
Ainsi, journIIalctl est en mesure de présenter les informations de ses journaux dans **divers formats utiles**.

## Installation de rsyslog (au besoin)

rsyslog est le syslogd par défaut sur les systèmes Debian et est généralement installé par défaut.  
On peut le vérifier en vérifiant la version de rsyslog installé …  
**>> apt list -a rsyslog  
En train de lister... Fait  
rsyslog/stable,now 8.2102.0-2 amd64 [installé]**

Si, pour une raison quelconque, cela ne serait pas le cas, on doit exécute la commande pour l'installer …  
**>> sudo apt update && sudo apt upgrade -y  
>> sudo apt install rsyslog -y**

Une fois l'installation terminée, démarrez et activez le service rsyslog.  
**>> sudo systemctl enable --now rsyslog**

## Syntaxe de la commande

De manière générale, le format de la commande se présente sous la forme suivante …  
**>> sudo journalctl [Otions ...] [Motfs ...]**

### Format de journal par défaut

journalctl affiche les journaux dans un **format similaire au format *syslog* traditionnel**.   
Chaque ligne commence par la …

* **date** (à l’heure locale du serveur),  
  suivie du
* **nom d’hôte du serveur** ;
* **nom du processus**   
  et
* **message du journal**.

Chaque ligne se présente de cette forme …  
**mai 11 01:05:38 SUSE sshd[24091]: Failed password for root from 218.92.0.163 port 30135 ssh2**

Les journaux seront **affichés du plus ancien au plus récent**.   
Pour **inverser cet ordre** et afficher les messages les plus récents en haut, on utilise l'option -r …  
>> **sudo** **journalctl -r**  
>> **sudo** **journalctl –reverse**

### Recherche dans les journaux

journalctl **dirige sa sortie vers la commande less**, qui affiche les journaux page par page dans le terminal.   
Si une ligne de journal dépasse la largeur horizontale de la fenêtre du terminal, on peut utiliser les touches fléchées gauche et droite pour faire défiler horizontalement et voir le reste de la ligne.

Pour envoyer les journaux vers la **sortie standard et éviter de les paginer**, on utilise l'**option --no-pager** …  
**>> sudo** **journalctl --no-pager**

Il est déconseillé de le faire sans d'abord filtrer le nombre de journaux indiqué.

# Surveillance des journaux

## Surveillance des nouveaux messages de journal

L’exécution de la commande *journalctl* avec l'**option -f va afficher les nouveaux messages au fur et à mesure de leur collecte**…  
**>> sudo** **journalctl -f**ou **>> sudo** **journalctl --follow**

**Remarques** …  
Les **commandes à partir de less ne sont pas disponible**s dans ce mode.   
Les touches **CTRL+C ou CTRL+Z va arrêter l’affichage en direct** et revenir à l'invite de commande.

### Filtrage de la sortie de journalctl

En plus de rechercher dans les journaux avec différentes commandes, il est possible d’appeler journalctl avec des **options permettant de filtrer les messages de journal** avant leur affichage.

Ces filtres peuvent être **utilisés avec l'affichage paginé normal** (*less*) et avec les **options --no-pager et -f**.   
Des filtres de différents types **peuvent également être combinés** pour affiner davantage la sortie.

### Filtre selon l’horodatage

L’**option --since** permet d’afficher les journaux **après une date et une heure spécifiée** …  
**>> sudo** **journalctl --since "2019-05-01 0:0:0"  
-- Logs begin at Sat 2019-05-11 01:05:18 EDT, end at Sat 2019-05-11 10:56:42 EDT. --**  
**mai 11 01:05:18 SUSE sshd[24086]: Failed password for root from 218.92.0.163 port 59971 ssh2**  
**mai 11 01:05:20 SUSE sshd[24084]: Failed password for root from 218.92.0.147 port 3566 ssh2**  
**mai 11 01:05:21 SUSE sshd[24086]: Failed password for root from 218.92.0.163 port 59971 ssh2**  
**mai 11 01:05:23 SUSE sshd[24084]: Failed password for root from 218.92.0.147 port 3566 ssh2**  
**mai 11 01:05:23 SUSE sshd[24086]: Failed password for root from 218.92.0.163 port 59971 ssh2**  
**mai 11 01:05:26 SUSE sshd[24084]: Failed password for root from 218.92.0.147 port 3566 ssh2**  
**…**

L’utilisation de l'**option --until** permet d’**afficher les journaux jusqu'à une date et une heure spécifiée** …  
**>> sudo** **journalctl --until "2019-05-01 0:0:0"**

Il est aussi possible de combiner les deux options afin d’**afficher les journaux entre deux moments** …  
**>> sudo** **journalctl --since "2019-04-04 0:0:0" --until "2019-05-01 0:0:0"**

Les dates et heures doivent être spécifiées au **format** **AAAA-MM-JJ HH:MM:SS.**   
Si l’heure est omise (c’est-à-dire que seule la date AAAA-MM-JJ est spécifiée), l’heure est supposée être 00:00:00.

La commande journalctl peut également **accepter d'autres termes** lors de la spécification des dates …

* Les **termes yesterday, today et tomorrow** sont reconnus.  
  **journalctl --since yesterday**En les utilisant, l'heure est supposée être 00:00:00 ;
* Les **termes comme 1 day ago ou 3 hours ago**sont aussi reconnus …  
  **journalctl --since "1 day ago"**  
  **journalctl --since "3 hours ago" ;**
* Les **symboles - et + peuvent être utilisés** pour spécifier des dates relatives ...   
  **-1h15min** indique il y a 1 heure 15 minutes  
  et  
  **+3h30min** indique 3 heures 30 minutes dans le futur.

Filtre selon les services  
Il est possible de spécifier le nom d’une unité systemd avec **l’option -u pour afficher les journaux d’un service particulier** …  
**>> sudo** **journalctl --unit ssh.service**

Filtre selon les messages du noyau  
L'**option -k permet de limiter l’affichage uniquement des messages du noyau …**  
**>> sudo** **journalctl --dmesg**

### Limite de la sortie à objet spécifique

Si on souhaite **limiter la sortie de *dmesg* à un objet spécifique comme un démon**, on utilise l’**option --facility=daemon** de la commande *dmesg* …  
**>> sudo dmesg --facility=daemon**

Voici les **objets de journalisation pris en charge** dans la commande *dmesg*.

* kern ;
* user ;
* mail ;
* daemon ;
* auth ;
* syslog ;
* lpr ;
* news.

### –Modification du format de sortie du journal p*ermalink*

Les enregistrements de journal des journaux de *systemd* étant structurés, *journalctl* peut afficher vos journaux dans différents formats.   
Voici quelques-uns des formats disponibles …

|  |  |
| --- | --- |
| Nom du format | Description |
| short | Affiche les journaux au **format *syslog* traditionnel** – Option par défaut |
| verbose | Affiche toutes les **informations dans la structure d'enregistrement du journal** |
| json | Affiche les journaux au **format JSON**, avec un **événement par ligne** |
| json-pretty | Affiche les journaux au **format JSON sur plusieurs lignes pour une meilleure lisibilité** |
| cat | Affiche uniquement le **message de chaque journal sans aucune autre métadonnée** |

On désigne le nom du format avec **l'option -o pour afficher les journaux dans ce format**.   
**>> sudo journalctl --output json-pretty  
>> sudo** **journalctl /usr/bin/dbus-daemon**

**Liste tous les pilotes chargés dans le noyau**

L’utilisation des **outils de manipulation de texte** (head, tail, less ou grep) sont utiles avec la commande *dmesg*.   
Comme la sortie du journal *dmesg* ne tient pas sur une seule page, l’utilisation de la **commande *dmesg* dans un pipeline (*pipe* |) avec *less* affichera les journaux sur une seule page**.  
**>> sudo dmesg | less  
>> sudo dmesg | head  
>> sudo dmesg | tail -n 20  
…**  
**[94216.776191] blk\_update\_request: I/O error, dev fd0, sector 0**  
**[94216.776194] floppy: error -5 while reading block 0**  
**[94216.948011] blk\_update\_request: I/O error, dev fd0, sector 0**  
**[94216.948013] floppy: error -5 while reading block 0**  
**…**  
**[216117.180977] eth0: Promiscuous mode enabled.**

# Journalisation du noyau (dmesg)

### Filtre selon les démarrages

**Chaque** **démarrage est répertorié par journalctl**.

La sortie de la commande **journalctl --list-boots** inclut un **ID de démarrage 32 bits** …  
**>> sudo** **journalctl --list-boots  
0 bb66a6318d484c6fa66efb744a3bfe69 Sat 2019-05-11 01:05:18 EDT—Sat 2019-05-11 11:28:38 EDT**

Il est aussi possible de **fournir un ID de démarrage avec l'option -b** …  
**>> sudo** **journalctl --boot bb66a6318d484c6fa66efb744a3bfe69**

**Remarque** …  
Si **aucun démarrage précédent n'est répertorié**, il est possible que sa **configuration journal ne soit pas configurée** pour conserver le stockage des journaux.

Pour afficher tous les **journaux du noyau du démarrage précédent** …  
**>> sudo** **journalctl --dmesg --boot -1**

## Effacement des journaux de mémoire tampon

Il est possible effacer les journaux *dmesg* si nécessaire.   
L’ajout de l’**option -c à la commande dmesg** effacera les journaux des messages de la mémoire tampon en anneau (*buffer ring*).

**Remarques** …  
On peut toujours voir les **journaux emmagasinés dans les fichiers /var/log/dmesg**.   
Tout appareil qui est connecté générera une sortie *dmesg*.

## Recherche d’un périphérique détecté ou une chaîne particulière

Il est difficile de rechercher une chaîne particulière en raison de la longueur de la sortie de dmesg.   
Ainsi, il sera utile de **filtrer les lignes avec des chaînes telles que usb, dma, tty, memory**, ...  
**>> sudo dmesg | grep -i usb  
>> sudo dmesg | grep -i dma  
>> sudo dmesg | grep -i tty  
>> sudo dmesg | grep -i memory**

Pour **découvrir quels disques durs ont été détectés par le noyau**, on peut rechercher le mot clé *sda* ainsi que *grep* …  
**>> sudo dmesg | grep sda  
[ 1.816143] sd 0:0:0:0: [sda] 41943040 512-byte logical blocks: (21.5 GB/20.0 GiB)**  
**[ 1.816325] sd 0:0:0:0: [sda] Write Protect is off**  
**[ 1.816418] sd 0:0:0:0: [sda] Mode Sense: 61 00 00 00**  
**[ 1.816535] sd 0:0:0:0: [sda] Cache data unavailable**  
**[ 1.816627] sd 0:0:0:0: [sda] Assuming drive cache: write through**  
**[ 1.819478] sda: sda1**  
**[ 1.819940] sd 0:0:0:0: [sda] Attached SCSI disk**

## Surveillance des journaux *dmesg* en temps réel

Il est possible, à l’aide de la **commande *watch* de surveiller ce qui se passe au niveau du noyau**…  
**>> sudo watch "dmesg | tail -20"**

Il est aussi possible de **surveiller les journaux dmesg en temps réel à l’aide de l’option --follow** …  
**>> sudo dmesg --follow**

Si on souhaite **activer les horodatages lors de la surveillance en temps réel** de dmesg …  
**>> sudo dmesg -Tx --follow**

**Remarque** …  
Certaines distributions permettent également la commande **tail -f /var/log/dmesg** pour la surveillance en temps réel.

### Horodatages en sortie

Parfois, on souhaiterait peut-être associer un horodatage aux messages produits par *dmesg*.   
Cela peut être fait à l'aide de l'option de ligne de commande ***-T***, qui produit des horodatages facilement lisibles.  
**>> sudo dmesg -t  
…  
[Fri May 10 06:28:42 2019] eth0: Promiscuous mode enabled.  
[Fri May 10 06:28:42 2019] eth0: Promiscuous mode enabled.  
[Fri May 10 18:29:04 2019] eth0: Promiscuous mode enabled.**

### Limite de la sortie aux erreurs et avertissements

En exécutant *dmesg* sur un système, on peut constater qu'il génère une pléthore d'informations.   
Selon ce que l’on recherche, on peut **filtrer ou limiter la sortie**.   
Pour sa part, **dmesg offre cette possibilité grâce à des niveaux**.

Voici la liste complète des niveaux …

* **Urgence** (*emerg*)  
  Le système est inutilisable ;
* **Alerte** (*alert*)  
  Des mesures doivent être prises immédiatement ;
* **Critique** (crit)  
  Conditions critiques ;
* **Erreur** (*err*)  
  Conditions d'erreur ;
* **Avertissement** (*warn*)  
  Conditions d'avertissement ;
* **Notification** (*notice*)  
  État normal mais peut être significatif ;
* **Info** (*info*)  
  Informatif ;
* **Débogage** (*debug*)  
  Messages de niveau débogage.

Ainsi, par exemple, si on souhaite limiter la sortie aux erreurs et aux avertissements …  
**>> sudo dmesg --level=err,warn**

### journalctl et les messages du noyau

La commande journalctl, permet d’obtenir facilement les messa**ges du noyau des précédents démarrage ou redémarrage** (par suite de l’exécution de la commande shutdown ou d’un crash – au format dmesg -T).

|  |  |
| --- | --- |
| Option | Description |
| -k | Journal *dmesg* |
| -b <numéro amorce> | Nombre de redémarrages (0, -1, -2, …) |
| o short-precise | ***dmesg -T*** |
| -p priority | Filtre par sortie prioritaire (4 pour filtrer les avis et les informations) |

**Remarque** …  
Il existe également les **options -o short et -o short-iso qui donnent respectivement la date et la date/heure au format iso**.

Exemple de commandes …

* Démarrage en cours …  
  **>> sudo journalctl -o short-precise -k**
* Dernier démarrage …  
  **>> sudo journalctl -o short-precise -k -b -1**
* Deux redémarrages (il y a …) …  
  **>> sudo journalctl -o short-precise -k -b -2**

# Option de la commande journalctl

|  |  |
| --- | --- |
| Option | Description |
| -C ou --clear | Vider le tampon circulaire du noyau |
| -c ou --read-clear | Vider le tampon circulaire du noyau après avoir affiché son contenu |
| -E ou --console-on | Activer l'affichage des messages sur la console |
| -D ou --console-off | Désactiver l'affichage des messages sur la console |
| -d ou --show-delta | Afficher l'horodatage et la différence de temps passé entre les messages Si *--notime* est utilisé en même temps, seule la différence de temps passé, sans l'horodatage, est affichée |
| -e ou –reltime | Afficher la date locale et la différence en format lisible |
| -F ou --file FICHIER | Lire les messages à partir du fichier donné |
| -f ou --facility LISTE | Restreindre l'affichage à la liste de services (séparés par des virgules) indiquée Par exemple … dmesg --facility=daemon n'affichera que les messages des démons du système |
| -H ou --human | Activer la sortie lisible |
| -k ou –kernel | Afficher les messages du noyau |
| -L ou --color[=Quand] | Colorer la sortie L’argument facultatif quand peut être *auto*, *never* ou *always* *En absence d’argument quand, auto* est la valeur par défaut Les couleurs peuvent être désactivées |
| -l ou --level LISTE | Restreindre l'affichage à la liste de niveaux (séparés par des virgules) indiquée Par exemple … dmesg --level=err,warn n'affichera que les messages d'erreur et d'avertissement |
| -n ou --console-level NIVEAU | Définir le niveau d'affichage des messages en console le niveau est un numéro ou une abréviation du nom de niveau Par exemple, ***-n 1*** ou ***-n alert*** suppriment l'affichage de tous les messages, sauf les messages d'urgence (graves) Tous les niveaux d'affichage des messages sont enregistrés dans */proc/kmsg*, ainsi *syslogd* peut toujours être utilisé pour contrôler exactement où les messages du noyau apparaissent Quand l'option ***-n*** est utilisée, *dmesg* n'affichera pas et n'effacera pas le tampon circulaire du noyau |
| -P ou --nopager | Ne pas renvoyer la sortie dans un visualiseur Un visualiseur est activé par défaut pour la sortie --human |
| -T ou -ctime | Afficher l’horodatage au format lisible |
| -t ou --notime | Ne pas afficher l’horodatage du noyau |
| -u ou --userspace | Afficher les messages en espace utilisateur |
| -w ou --follow | Attendre de nouveaux messages Cette fonctionnalité n’est prise en charge que sur les systèmes avec un */dev/kmsg* lisible (depuis le noyau 3.5.0) |
| -x ou --decode | Décoder les numéros de service et de niveau (priorité) en préfixes lisibles |
| -V ou --version | Afficher les informations sur la version et quitter |
| -h ou --help | Afficher un texte d'aide puis quitter |