Fichiers de log

RSYSLOG

Pour isoler les logs d'un service dans un fichier plutôt que dans /var/log/messages créer un fichier /etc/rsyslog.d/<service>.conf

Syntaxe

```
:propriété, [!]Opérations de comparaison basées sur la propriété, "valeur"
```

Propriétés

- **msg** : la partie MSG du message.
- **hostname** : nom d'hôte du message
- **source** : alias pour HOSTNAME
- **timegenerated** : horodatage de la réception du message. Toujours en haute résolution
- **fromhost** : nom d'hôte du système duquel le message a été reçu.
- **fromhost-ip** : Identique à fromhost, mais toujours sous forme d'adresse IP.
- **syslogtag** : TAG du message
- **programname** : la partie «statique» de la balise, telle que définie par BSD syslogd. Par exemple, lorsque TAG est «nommé [12345]», le nom du programme est «nommé».

Opérations

- **contains** : Vérifie si la chaîne fournie dans valeur est contenue dans la propriété. Il doit y avoir une correspondance exacte, les caractères génériques ne sont pas pris en charge. Une option insensible à la casse est contains_i.
- **isequal** : Compare la chaîne «valeur» fournie et le contenu de la propriété. Ces deux valeurs doivent être exactement égales pour correspondre. isequal est le plus utile pour les champs comme syslogtag ou FROMHOST, où vous connaissez probablement le contenu exact.
- **startswith** : Vérifie si la valeur se trouve exactement au début de la valeur de la propriété. Par exemple, si vous recherchez "val" avec: msg, commence par, "val", ce sera une correspondance si msg contient "les valeurs sont dans ce message" mais il ne correspondra pas si le msg contient "Il y a des valeurs dans ce message message". Pour effectuer des comparaisons insensibles à la casse, utilisez startswith_i.
- **regex** : Compare la propriété à l'expression régulière POSIX BRE fournie.
- **ereregex** : Compare la propriété à l'expression régulière POSIX ERE fournie.
- **isempty** : Vérifie si la propriété est vide.

La négation se fait avec !

Exemples

contenu

Rediriger tous les journaux avec [IPTABLES vers /var/log/firewall.log

```
:msg,contains, "[IPTABLES" -/var/log/firewall.log
```

hostname

Sélectionner les messages syslog reçus du nom d'hôte toto.com

```
:hostname, isequal, "toto.com"
```

syslogtag

Rediriger tous les messages dont le TAG contient Node-Red vers vers /var/log/nodered/nodered.log

```
:syslogtag, contains, "Node-RED" -/var/log/nodered/nodered.log
& stop
```

LOGROTATE

Pour provoquer la rotation des fichiers de log créer un fichier /etc/logrotate.d/<service>.conf

Exemple

```
/var/log/nginx/*.log {
        daily
        missingok
        rotate 14
        compress
        delaycompress
        notifempty
        create 0640 www-data adm
        sharedscripts
        prerotate
                if [ -d /etc/logrotate.d/httpd-prerotate ]; then \
                        run-parts /etc/logrotate.d/httpd-prerotate; \
                fi \
        endscript
        postrotate
```

```
                invoke-rc.d nginx rotate >/dev/null 2>&1
        endscript
}
```

Syntaxe

- **daily, weekly, monthly** : pour une rotation sur un jour, une semaine ou un mois.
- **missingok** : permet au processus de ne pas s'arrêter à chaque erreur et de poursuivre avec le fichier de log suivant.
- **rotate** : indique le nombre de fichiers conservés, ici on conserve 14 mois de journalisation.
- **compress** ou **delaycompress** : pour compresser les fichiers au format gzip. 'delaycompress' retarde le processus de compression jusqu'à la prochaine rotation.
- **notifempty** : empêche la rotation de s'effectuer si le fichier de log est vide.
- **create** <mode> <owner> <group> : cré un fichier vide avec les propriétés spécifiées, après la rotation des logs.
- **sharedscripts** : les scripts ne sont exécutés qu'une seule fois, quel que soit le nombre de journaux correspondant au modèle générique, et le modèle entier leur est transmis. Cependant, si aucun des journaux du modèle ne nécessite une rotation, les scripts ne seront pas exécutés du tout. Si les scripts se terminent avec une erreur, les actions restantes ne seront exécutées pour aucun journal. Cette option remplace l'option nosharedscripts et implique l'option de création.
- **prerotate** et **postrotate** : permet de spécifier des actions à effectuer avant et après la rotation de log.
- **copytruncate** : le fichier est copié avant d'être vidé au lieu d'être déplacé. A utiliser avec certaines applications qui ne peuvent être alertée pour fermer le fichier et qui poursuivent l'écriture dans le fichier.

Forcer la rotation

Pour forcer la rotation exécuter la commande :

```
sudo logrotate -f /etc/logrotate.conf
```

Haut de page