

Logs

Introducción

Linux registra todos los eventos o mensajes que generan las aplicaciones que se están ejecutando a través de unos archivos en formato texto llamados logs.

Los ficheros logs pueden ser de gran ayuda en el momento de detectar una intrusión o un mal funcionamiento del sistema. La mayoría de logs son tratados a través del servicio *syslog* para registrarse en formato fichero y es la aplicación *logrotate* la que gestiona la rotación.

Logrotate es una simple aplicación (52Kb) que copia o trunca los logs indicados con la finalidad de organizar tales ficheros, esta aplicación es ejecutada a través de el servicio *crond* y se ejecuta a lo sumo diariamente.

Actuaciones

Se modifica la configuración del servicios de recogida y rotación de logs para recoger mayor información del sistema.

Modificaciones en el fichero `/etc/syslog.conf`

Modificamos las directrices del fichero de configuración del sistema para registrar más información del sistema

```
# Monitor authentication attempts
auth.*;authpriv.* /var/log/authlog

# Monitor all kernel messages
kern.* /var/log/kernlog

# Monitor all warning and error messages
*.warn;*.err /var/log/syslog
```

Otra buena medida de seguridad es reportar los registros a otro equipo

```
# Send a copy to remote loghost. Configure syslogd init
# script to run with -r -s domain.com options on log
# server. Ensure a high level of security on the log
# server!
*.info @loghost
auth.*;authpriv.* @loghost
```

Modificaciones de permisos

Limitamos el acceso al directorio de logs del sistema para usuarios sin privilegios, mediante los comandos:

```
chmod 751 /var/log /etc/logrotate.d
chmod 640 /etc/syslog.conf /etc/logrotate.conf
chmod 640 /var/log/*log
```

Configuración general de rotación de logs

El archivo `/etc/logrotate.conf` contiene la configuración general del servicio `logrotate`.

Configuración logrotate para httpd

La mayoría de logs que registrará el sistema son los referentes al servicio `httpd`, que es el principal servicio del equipo por lo que cambiamos la configuración para almacenar coherentemente esta información.

Se aplican los siguientes cambios en la configuración para los logs referentes al *virtual host* de `favshare.com` que situamos en el archivo de configuración `/etc/logrotate.d/httpd-sites.conf`

Ciclo de vida igual a 60 rotaciones con una frecuencia diaria.

```
daily
rotate 60
```

Cambiamos el tamaño máximo de logs a 100 Megas, esta medida impide que los archivos de log sean demasiado grandes y requieran de demasiados recursos para el acceso al fichero.

```
# Maximum size of logs
size=100M
```

Comprimimos el log un vez rotado para evitar un exceso de ocupación en el disco.

```
compress
```

Añadimos la marca de tiempo tipo `YYYYMMDD` en lugar de añadir un simple número.

```
dateext
```

Para mantener coherencia con este formato, además evitamos que no se roten los logs aunque estos estén vacíos

```
# Rotate if empty
ifempty
```

Referencias

Para ampliar información consulta las siguientes referencias:

<http://www.topology.org/linux/logrotate.html>

<http://www.debian-administration.org/users/lee/weblog/8>

<http://llestes.bulma.net/pipermail/bulmailing/Week-of-Mon-20060522/076867.html>

¿Que es iddover.net?

Iddover Hosting es una iniciativa española en el sector de servidores dedicados. Nace en contraposición de los servicios actuales de hosting . Pretende ofrecer un hosting de alta calidad gestionable a través de un potente panel propio que se adecua a los requisitos de seguridad y que proporciona al cliente potentes herramientas al alcance de un solo click

Desde 69€ dispondrás de un servidor dedicado administrado auditado con todas las medidas de seguridad ya aplicadas.

<http://www.iddover.net>