Порядок ротации журналов безопасности подсистемы регистрации событий

В операционной системе Astra Linux для ротации журналов используется утилита logrotate.

logrotate разработан для облегчения администрирования систем, которые порождают большое количество файлов журналов происходящих в системе событий. Утилита предоставляет автоматическое обращение, сжатие, удаление и отправление по электронной почте журналов системы. Каждый файл журнала сообщений может обрабатываться ежедневно, еженедельно, ежемесячно, либо когда увеличится в размерах выше указанного предела.

Информация

Справку по утилите logrotate можно получить по команде:

man logrotate

Создадим конфигурационный файл в котором будут прописаны настройки ротации:

/etc/logrotate.d/kernlog

```
/var/log/parsec/kernel.mlog {
    daily
    missingok
    rotate 7
    compress
    notifempty
    postrotate
        /etc/init.d/parlogd restart > /dev/null
    endscript
}
```

Разберем директивы, указанные в конф. файле:

`daily`

Ежедневная ротация файлов журналов. Можно настроить ротацию по достижению файла журнала определенного размера. См. `size`

`missingok`

Если файл журнала отсутствует, перейти к следующему без создания сообщения об ошибке.

`rotate 7`

Файлы журнала ротируются 7 раз перед тем, как будут удалены или отправлены на адрес, указанный в директиве mail.

`compress`

Сжать старые файлы журналов. Несмотря на то что файлы журналов представлены в бинарном виде, сжимаются они на ура.

`notifempty`

Не ротировать журнал если он пуст.

`postrotate/endscript`

Строки между postrotate и endscript (каждая из которых должна располагаться в отдельной строке) выполняются после ротации файла журнала при помощи /bin/sh. В данном случае перезапускается демон parlogd, для пересоздания файлов журналов.

`size`

Ротация будет происходить раз в день, (запуск logrotate по cron'у осуществляется раз в день) но будут ротированы только те файлы журналов, размер которых больше указанного размера в байтах. Если использована буква k, то размер указан в килобайтах. Если размер указан с буквой M, подразумевается размер в мегабайтах. Если используется буква G, то размер указан в гигабайтах.

Так же возможен запуск утилиты logrotate командой:

```
sudo logrotate /etc/logrotate.d/kernlog
```

Такое может понадобится в случае быстрого роста файла журнала, когда ротация раз в день не помогает.

Для этого в конф.файле нужно указать размер, при котором следует ротировать файл:

/etc/logrotate.d/kernlog

```
/var/log/parsec/kernel.mlog {
    size 100M
    missingok
    rotate 7
    compress
    notifempty
    postrotate
        /etc/init.d/parlogd restart > /dev/null
    endscript
}
```

И, например, запускать logrotate /etc/logrotate.d/kernlog по cron'у раз в час, разместив скрипт выполнения в /etc/cron.hourly/ или прописав в crontab'е:

```
sudo crontab -e
```

crontab -e

```
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command

0 * * * *       /usr/sbin/logrotate /etc/logrotate.d/kernlog
```

Параметры ротации журнала user.mlog можно добавить в этот же файл, либо создать по аналогии новый. (обычно user.mlog не так раздувает)