Logwatch – отчет на почту

```
# yum install logwatch
```

Logwatch входит в Базовые репозитории CentOS и не требует подключения дополнительных репозиториев. Все зависимости будут автоматом устранены.

Примечание: Для отправки отчёта по email, я использую Postfix так как даже разработчики RedHat в новой версии RedHAt 7 используют его вместо Sendmail. Соответственно и настройка отправки будут заточены под Postfix.

Редактируем основной конфигурационный файл:

```
# vim /usr/share/logwatch/default.conf/logwatch.conf
```

```
##Указываем кому будет отправляться почта
MailTo = admin@domen.com

## Адрес отправителя отчета
MailFrom = Logwatch@domen.com

##За какой период отправить отчёт: All, Today, Yesterday (переводить не вижу смысла всё и так предельно понятно)
Range = yesterday

##Детализация отчёта, максимальная, средняя либо низкая : High, Med, Low. Практический опыт показал, что оптимальнее всего указать среднюю либо максимальную детализацию.
Detail = Med

##Сервисы подлежащие анализу по умолчанию указаны все
Service = All

##Далее можем исключить сервисы из вывода статистики пример:
Service = "-sendmail"

##По умолчанию Logwatch анализирует логи в директории /var/log, но мы можем задать дополнительные пути, пример:
```

```
LogFile = /home/httpd/access_log
LogFile = /home/httpd/error_log

##Задаём путь и ключ к система обработки почтовых сообщений
mailer = "/bin/mailx -t"
```

На этот настройка конфигурационного файла завершена. Осталось настроить файл для авторизации (ЕСЛИ НУЖНО) на почтовом сервере.

В домашней директории пользователя создаём файл *.mailrc* и задаём нужные параметры:

Если используется защищенное SSL/TLS соединение то нужно расскоментировать строчки ниже:

```
#set smtp-use-ssl/tls
#set ssl-verify=ignore
```

Далее задаем имя домен (либо IP) порт, способ авторизации, email и пароль:

```
set smtp=smtp://mail.server.com:25
set smtp-auth=login
set smtp-auth-user=logwatch@mail.server.com
set smtp-auth-password=qwerty123!
set from="logwatch@mail.server.com(My server)"
```

Для безопасности меняем права на файл:

```
chmod 400 .mailrc
```

Теперь можем проверить работу выполнив команду:

```
# logwatch
```

Если будут ошибки то они будут отображены в терминале.

Для тестирования отправки можно также воспользоваться следующей командой:

```
echo "Test" | mail -v -s "Test message" admin@domain.com
```

В конечном итоге на указанный почтовый адрес нам должен придти

отчёт. Если есть проблемы читаем ниже.

Скрипт формирования отчёта и отправки автоматически создался во время установки пакета и помещается в директорию: /etc/cron.daily/0logwatch но на следующий день Вы не получите отчёта, более того добавление скрипта в crontab также не помогает, а проблема эта из-за переменных окружения, точнее путей, которые при работе через cron нужно указывать либо экспортировать.

Проблема решается редактированием файла

/etc/cron.daily/0logwatch

```
#!/bin/bash
export PATH=$PATH:/usr/sbin
.................................
.................................
then
 logwatch
fi
```

Теперь нам остаётся только по утрам открывать свою почту и просматривать отчёт.

P.S. если лог файл отличается от стандартного, лежит не в /var/log/, а в ином место

$ nano /usr/share/logwatch/default.conf/logfiles/

```
 LogFile = apache/*access.log
 LogFile = /www/site1/logs/access*.log
 LogFile = /www/site2/logs/access*.log
 #LogFile = apache/*access.log.1
 #LogFile = apache2/*access.log.1
 LogFile = apache/error_log
 LogFile = /www/site1/logs/error*.log
 LogFile = /www/site2/logs/error*.log
 #LogFile = httpd/site1/_log
 #LogFile = httpd/site2/error_log...........
```

Пример для OpenVPN:

```
/etc/logwatch/scripts/openvpn      - Logwatch perl module
/etc/logwatch/conf/openvpn.conf    - Configuration file
```

```
# cp /usr/share/logwatch/default.conf/services/openvpn.conf /etc/logwatch/conf/logfiles/
```

```
# cp /usr/share/logwatch/scripts/services/openvpn /etc/logwatch/scripts/services/
```

Проверяем

```
# logwatch --detail low --range today --service openvpn --debug 5
# logwatch --service openvpn --output stdout --debug 10
```

https://forum.sys-adm.in/index.php?topic=3808.0
http://www.itword.net/page/logwatch-linux
http://bflinux.blogspot.com/2011/07/logwatch-linux.html