Evtsys

Перенаправление Windows (Event Log) на Syslog сервер Linux

http://code.google.com/p/eventlog-to-syslog/

Версия 4.4.0, (последняя под MS Windows 2000)

Установка

```
copy evtsys.* %systemroot%\system32
%systemroot%\system32\evtsys.exe -h syslog -s 240 -i
net start evtsys
```

Параметры evtsys.exe

`-i`	Установить сервис
`-u`	Удалить сервис
`-d`	Режим отладки. Запуститься как консольная программа
`-h syslog`	Имя хоста куда отправлять логи
`-b syslog2`	Имя второго хоста кому дублировать логи
`-f 3`	Facility
`-l 0`	Минимальный уровень отсылаемых сообщений: 0=Всё, 1=Критические, 2=Ошибки, 3=Предупреждение, 4=Информация
`-n`	Отправлять только события включенные в `evtsys.cfg`
`-p 514`	Номер порта syslog
`-q 0`	Опросить DHCP чтобы получить имя хоста syslog и порт. 0=Включить, 1=Выключить
`-s 60`	Интервал между сообщениями о статусе (в минутах). 0=Отключить

Facility

По умолчанию `system daemons` на `local1`

```
0 kernel messages
1 user-level messages
2 mail system
3 system daemons
4 security/authorization messages
5 messages generated internally by syslogd
6 line printer subsystem
7 network news subsystem
8 UUCP subsystem
9 clock daemon
10 security/authorization messages
11 FTP daemon
12 NTP subsystem
13 log audit
14 log alert
15 clock daemon
16 local use 0 (local0)
```

```
17 local use 1 (local1)
18 local use 2 (local2)
19 local use 3 (local3)
20 local use 4 (local4)
21 local use 5 (local5)
22 local use 6 (local6)
23 local use 7 (local7)
```

Ссылки

Перенаправление событий Windows (Event Log) на сервер syslog Linux / Хабр

http://sysadminmosaic.ru/evtsys/evtsys

2020-11-16 10:56