Администрирование Linux
Лекция 5
Лог-файлы и мониторинг

Иртегов Д.В.

Новосибирский гос. Университет

2014

Лог-файлы

- dmesg
  - Сообщения ядра на всех этапах функционирования.
  - Выдаются на консоль
  - Дублируются во внутреннем буфере (могут быть получены командой dmesg)
  - Складываются в файл /var/log/dmesg
- syslog (в RHeL/CentOS 6 rsyslogd)
  - Через этот сервис идет выдача сообщений практически всех системных сервисов
  - В RHS туда также дублируется dmesg
  - /var/log/messages
    в некоторых системах /var/log/syslog
  - Можно настроить передачу логов на другую машину
  - Можно настроить селективную выдачу отдельных типов сообщений в разные места: на консоль, в отдельные файлы, в базу данных
  - Можно настроить запуск программы на появление некоторых сообщений (например, отправка почты/SMS)

Демонстрация

- dmesg
- /var/log/messages
- /var/rsyslog.conf

Траблшутинг ядра

- lscpu и /proc/cpuinfo – информация о процессорах
- lspci – список PCI устройств по данным автоконфигурации PCI lsusb – список устройств USB
- lsscsi – список устройств SCSI и SATA
- lsmod – список модулей ядра
- modprobe – загрузить модуль
- /etc/modprobe.d – файлы, управляющие загрузкой модулей при старте

Еще один интересный лог

- /var/log/wtmp
- В него записаны все логины – с консоли, по ssh, через другие сервисы, если они есть
- Бинарный, содержимое выдается командой last

Ротация логов

- Скрипт logrotate запускается каждую ночь
- Конфигурация - /etc/logrotate.conf

Полезные программки для мониторинга

- ps – список процессов
  - ps -f, -l – различные длинные форматы вывода (параметры команд, состояние процесса, объем памяти, время…)
  - ps -o опции – форматированный вывод
  - ps -u user – все процессы данного пользователя
  - ps -a – все процессы, кроме демонов (лидеров сессий без терминала)
  - ps -e | -A | -ex – все процессы
- top, htop, System Monitor (GUI) – список процессов в динамике, как Win32 taskmanager
- sar, iostat, vmstat – утилиты для сбора статистики
- netstat – список сетевых соединений и Unix Domain Sockets
  - netstat –a – выводить также слушающие сокеты
  - netstat –p – выводить, какой процесс держит соединение (root only)