**108.2 Журналы событий системы**

Студент должен уметь настраивать классический демон syslog. Это включает в себя настройку отправки событий на центральный сервер логов, и настройку приема этих событий на центральном сервере. Также необходимо знать о возможностях systemd, rsyslog и syslog-ng.

**Изучаем**:

* настройку демона syslog;
* стандартные источники событий, приоритеты и действия;
* настройку ротации логов;
* возможности systemd, rsyslog и syslog-ng.

**Syslog** – классическая система ведения логов. Стандартная конфигурация содержит записи вида ***источник.приоритет назначение****.*

**Источниками** могут быть система аутентификации, демоны, ядро, планировщик и т.д.

**Приоритет** может принимать следующие значения (debug – минимальный приоритет, emergency - максимальный):

* debug
* info
* notice
* warning
* error
* critical
* alert
* emergency

**Назначением** могут быть вывод в консоль, группа пользователей, удаленная система и т.д.

Файл конфигурации syslog - **/etc/syslog.conf**

Примеры:

* ***kern.\* /dev/console*** (все события ядра выводить в консоль);
* ***\*.info /var/log/messages*** (события из любых источников с приоритетом info и выше отправлять в файл /var/log/messages);
* ***mail,news.=crit \**** (критические события систем почты и новостей отправлять всем пользователям);

Для отправки событий на настроенный сервер приема логов в качестве назначения указывается его ip-адрес, например:

* ***user.\* @192.168.0.99*** (все события пользователей отправлять на машину 192.168.0.99)

Для включения возможности приема сообщений на удаленной машине необходимо изменить файл конфигурации syslog: /***etc/sysconfig/syslog*** , а именно дописать к опции ***SYSLOG\_D\_OPTIONS*** ключ «**-r**».

Управлять модулем журнала syslog можно при помощи утилиты logger, например:

* ***logger –p user.warn Please Help!*** (создать событие от источника user с приоритетом warning, содержащее текст “Please Help!”).

Для регистрации событий ядра в syslog используется ***klogd***, который по умолчанию передает события в стандартный syslogd, но может и перенаправлять их в указанный файл.

\_\_

Для облегчения управления лог-файлами используется приложение **logrotate**, автоматизирующее ротацию логов (архивация, удаление, пересылка и т.д.). Приложение запускается по умолчанию планировщиком cron, т.е. в ***/etc/cron.daily/logrotate*** указан сам исполняемый файл и файл конфигурации ***/etc/logrotate.conf***.

Важные опции в файле конфигурации:

* **weekly** (ротация осуществляется раз в неделю, но можно выполнять ее по достижению лог файлом определенного размера);
* **rotate 4** (количество хранимых файлов, так как ротация настроена предыдущим параметром раз в неделю, то в данном случае будут храниться четыре недели событий).
* **прочие параметры** дают возможность настройки пустых новых журналов, сжатия архивируемых логов, права доступа к логам, скрипты после обработки и т.д.

В папке ***/etc/logrotate.d*** могут храниться отдельные настройки для отдельных лог-файлов.

По умолчанию логи (в том числе и обработанные logrotate) хранятся в папке ***/var/log***

\_\_

Система инициализации systemd, облегчает работу с логами, собирая их в одном месте. Для этого используется отдельный демон **journald** (возможно его совместное параллельное использование с классическим **syslogd**), настройки которого хранятся в файле ***/etc/systemd/journald.conf***.

Основные опции файла конфигурации:

* ***storage*** (место хранения логов);
* ***compress*** (сжатие);
* ***seal*** (шифрование);
* ***splitmode*** (опции разбиения лога);
* ***system*** (установка ограничений на размер, и количество журналов);
* ***forward*** (опции пересылки логов).

Хранит события в каталогах:

***/run/log/journal*** (буфер последних сообщений);

***/var/log/journal*** (хранение всех сообщений, если такой каталог создан).

Управляется при помощи утилиты ***journalctl.***

Например (опции можно комбинировать):

* ***journalctl –b*** (показать события с последней загрузки);
* ***journalctl --since 13:00 –until 13:05*** (показать события с 13:00 до 13:05);
* ***journalctl --since yesterday --until now*** (показать события со вчера до сейчас);
* ***journalctl -u networking.service*** (показать события службы сети);
* ***journalctl -p err*** (показать все ошибки);
* ***journalctl -n 20*** (показать последние 20 событий);
* ***journalctl –f*** (показывать события в режиме реального времени);
* ***journalctl --disk-usage*** (показать место на диске, занятое журналами событий);
* ***sjournalctl --vacuum-size=1G*** (установить максимальный размер всех логов в 1 Гб).

Для организации центрального хранилища логов в сети используется демон **systemd-journal-gatewayd**

Для отправки сообщений на удаленный сервер (some.host) используется команда вида ***systemd-journal-upload --url https://some.host:19531/***

Для приема сообщений сервером от удаленной машины (some.host) используется команда вида ***systemd-journal-remote*** ***−−url https://some.host:19531/***

\_\_

**Rsyslog** – расширенный инструмент управления событиями, отличающийся расширенными возможностями фильтрации и использованием протокола tcp (syslogd использует udp).

Основной конфигурационный файл ***/etc/rsyslog.conf***, разбит на секции:

* ***Modules*** (тут включаются и настраиваются модули для работы с разными источниками, анализаторы, фильтры и т.д.);
* ***Configuration Directives*** (общие параметры демона – формат временных отметок, права доступа, размещение файлов и т.д.);
* ***Templates*** (указание формата вывода и возможности динамических имен файлов);
* ***Rule Line*** (правила обработки логов в стандартном формате «*источник.приоритет действие*»).

\_\_

**Syslog-ng** – система управления событиями, содержащая гибкие возможности фильтрации. Оптимизирована для сбора событий в локальной сети (до 700 000 событий в секунду из нескольких тысяч источников).

Файл конфигурации ***/etc/syslog-ng/syslog-ng.conf*** разбит на части:

* ***sources*** (откуда принимать события);
* ***destination*** (куда отправлять события);
* ***filters*** (какие события куда направлять);
* ***log paths*** (правила, по которым сообщения из источников после фильтрации отправляются в назначения).