Логи (журнал сервера) в Linux

Логи (журнал сервера, англ. server log) – это записываемые фрагменты данных, описывающие то, что в конкретный момент времени делает сервер, ядро, службы и приложения.

Логи в Linux поступают из разных источников. Ниже перечислены основные.

Подсистема systemd. Большинство дистрибутивов Linux для управления службами имеют в своём составе systemd. Подсистема инициализации и управления ловит выходные данные служб и записывает их в журнал.

Сообщения процессов по стандарту syslog. При отсутствии systemd такие процессы, как SSH, могут записывать данные в UNIX-сокет в формате syslog. Демон syslog, например, rsyslog, выбирает сообщение, анализирует и по умолчанию записывает его в /var/log.

Ядро Linux пишет собственные логи в особый буфер. Подсистемы systemd или syslog могут считывать журналы из этого буфера, а затем записывать их в свои журналы или файлы – обычно /var/log/kern.log.

Audit logs. Особый случай сообщений ядра, предназначенных для аудита событий, таких как доступ к файлам. Обычно для прослушивания таких журналов безопасности, существует специальная служба, например, auditd, записывающая свои сообщения в /var/log/audit/audit.log.

Журнал приложений. Несистемные приложения имеют тенденцию записывать данные в /var/log:

Apache (httpd) обычно пишет в /var/log/httpd или /var/log/apache2. Журналы HTTP-доступа находятся в файле /var/log/httpd/access.log.

Логи MySQL обычно находятся в /var/log/mysql.log или /var/log/mysqld.log.

Старые версии Linux могут записывать свои логи загрузки с помощью bootlogd в /var/log/boot или /var/log/boot.log. В современных ОС об этом заботится systemd: вы можете просматривать связанные с загрузкой журналы

с помощью journalctl -b. Дистрибутивы без systemd снабжены syslog-демоном, считывающим данные из буфера ядра. Таким образом, вы можете найти свои boot/reboot-журналы в /var/log/messages или /var/log/syslog.

Таблица

Вопрос	**Ответ**
Какой файл логов поможет при проверке безопасности при авторизации в систему, в каком файле смотреть логи неудачных попыток авторизации?	Логи авторизации **/var/log/auth.log** или **/var/log/secure** логи неудачных попыток **/var/log/failog**
Что делает команда ls /var/log?	Команда **Is** наиболее используемая в любой UNIX-системе. Её предназначением является вывод информации о файлах и каталогах. При использовании с параметром **Is/var/log**, будет выведена информация о всех файлах логов системы
Какой командой посмотреть логи журнала сообщений от ядра в реальном времени?	**tail –f /var/log/kern.log** или **cat /var/log/kern.log**
Какая команда покажет, кто из пользователей сейчас залогинен в системе и когда он зашел?	**who** или **/var/run/utmp**
Какая команда дает понять, когда пользователь заходил в систему и сколько времени в ней находился?	**last <username>** или **/var/log/wtmp**
Какой самый простой способ посмотреть логи (открыть лог файл) syslog?	**Is /var/log/syslog** или **cat var/log/syslog**