**Глава 11. Мониторинг. Работа с файлами журналов.**

Запись в журнале – текстовая запись сиситемного события.

Журналы:

* syslogd (/var/log/syslog + /var/log/..) - Текстовая запись
* journalctl – Бинарная запись

**1) Управление файлами журналов:**

1.1. Журналирования с помощью journald

* Посмотреть журнал: -journalctl
* Последние 20 записей: -journal -n 20
* Критические записи: journalctl -p emerg
* Оталдка (выведет 10 тек. И 10 последующих записей): journalctl -f
* ПО времени: journalctl –since 15:50:00 –until 15:52:00

1.2. Журналирования с помощью syslogd

Настройки распределения записей: /etc/rsyslog.d/50-default.conf

Приложения записывают данные как в стандартные журналы (auth.log, kern.log), так и в свои файлы журналов (var/log/mysql/). У каждой записи есть уровни приоритета (от debug-полезно для отладки, до emerg-систему нельзя использовать).

Пример: принесли комп, который не прогрузился и последнее, что он выводил на экран было : /dev/sda1: clean, 121212/456456 files, 543646/565436 blocks.

Строка нам говорит о том, что диск жив, GRUB прогрузился и Linux частично загружена. Но это стровка не ошибка – это последнее сообщение, которое вывела система, что может ввести в заблуждение. (Открываем виртуальную консоль Alt+F2,F3…), проверяем сисстемные журналы, там была строка:

* xinit: unable to connect to X server: connetction refused.

Сервер X – система Linux, отвечающая за графический интерфейс. И если пользователь не может подключиться, это дает 2 наводки:

* Система X сервера повреждена
* Проблема аутентификации

В файле auth.log оказалась запись:

* lightdm: pam\_succeed\_if(lightdm:auth): requirement
* “user ingroup nopasswdlogin” not met by user “user\_name”

lightdm – менеджер рабочего стола, pam – модуль аутентификации. Оказалось, что дело с неправильными провами владения на файл .Xauthority из домашнего каталога пользователяю. Т.к. Сервер X не может загружать сеанс с графическим интерфейсом, если этот файл не принадлежит пользователю. В итоге этот файл принадлежал root. (проверка через ls). Поменять пользователя можно через (chown)

* chown user\_name:user\_name .Xauthority

**2) Управление файлами журналов.**

Т.к. в журналы ежеминутно что-то записывается, то они могут легко разрастаться до больших размеров. В связи с этим можно вводить ограничения на размеры файлов журнала.

2.1 Способ journald

В journald (/etc/systemd/journal.conf) есть параметры SystemMaxUse= RuntimeMaxUse=. Но так как по умолчанию journald ведет только временый журнал в /run/log/journal, то для веденя постоянного журнала следует создать каталог /var/log/journal/ и ввести команду для перенапрвления потока в него:

* mkdir -p /var/log/journal/
* systemd-tmpfiles –create –prefix /var/log/journal/

2.2 Способ syslogd

По умолчанию syslogd сам обрабатывает ротацию, сжатия, удаление логов, за это отвечает система logrotate, например в каталоге /var/log/ auth.log представлен в нескольких форматах: auth.log, auth.log.1, auth.log.2.gz… По истечении срока, logrotate автоматически удалит последнйи файл, переименует остальные и создаст новый auth.log.

Цикл этой ротации задан в файле(/etc/logrotate.conf),который настроивает

* Периол ротации (weekly – еженедельно)
* Период храненя (rotate 4 – за 4 недели)
* Создавать новый файлы осле ротации старых: (create)
* Добавлять инф о ротации в ЭТОТ каталог (include /etc/logrotate.d)

В свою очередь каталог /etc/logrotate.d/ содержит свои конфигурации, например, для apt, apache2 и тд.

! Совет: Можно перенаприавлять записи журнала на специальные удаленные серверы журналов, где они могут быть обработаны индивидулаьно. Это освобождает серверы приложений и хранит все в одном месте.

**3) Обработка больших файлов**

Здесь будут рассмотрены инструменты обработкаи текста.

3.1. grep (a.k.a. по совпадениям строк)

Пример: поиск в auth.log неудачных аутентификаций:

* cat /*var*/log/auth.log | grep “Authentication failure”
* cat /*var*/log/auth.log | grep -B 1 -A 1 failure (включение строк до и после совпадения)
* Для генерации в журнал: logger “Authentication failure”

3.2. awk (a.k.a. разбиение строк на поля)

Имеет лучшие утонченные параметры для поиска, умеет, к примеру, отличать столбцы по пробелам.

* Cat error.log | awk ‘$3 ~/[Warning]/’ | wc – поиск по 3 столбцу ($3), слова Warning и подсчет таких значений (программа wc).

3.3 sed (a.k.a. подстановка строк)

Возвращает втроку в соответствии с условием.

* Cat error.log | awk ‘$3 ~/[Warning]/’ | sed -n ‘$=’ (-n -не печатать текст)

Заменть слово в потоке:

* echo “hello world” | sed “s/world/fishtank/”
* echo “hello world” | sed “s/world/fishtank/g” (g - заменть все world, если их больше одного)

Удалить что-то из файла:

* sed “s/^ \*[0-9]\* //g” numbers.txt (удалит цифры из начала строк)
* sed “s/^ \*[0-9]\* //” numbers.txt > new-numbers.txt (+ перенаправить вывод в новый файл)

Печатать подкаталоги, без файлов :

* ls -l | sed -n ‘/^d/ p’

4) Мониторинг с обнаржуением вторжений.

Суть: Имеем исходную картину (профиль, состояние) системы, периодически сканируем ее на изменения, которые и будут указывать на вторжение.

Варианты:

* Сетевая система обнаружения вторжений (NIDS) – опирается на регулярное прослушивание сетевого окружения.
* Система обнаружения вторжений на хосте (HIDS), чтобы постоянно следить за своим сервером.

Вариант HIDS реализует пакет Tripwire.

Принцип: Tripwire сканирует сервер и добавляет атрибуты важных системных файлов (размер и т.д.) в свои БД. Если какой-то из файлов будет отредактирован или удален, атрибуты изменятся и когда мы попосим Trpwire проверить систему, то он обнаружит несоответсвие и сообщит об этом (по почте и в консоль).

Поведение Tripwire основано на 2х ЗАШИФРОВАННЫХ файлах: /etc/tripwire/tw.cnf и tw.pol, которые основаны на информации из twcnf.txt и twpol.txt. (Они **удаляются, после настройки** и создания tw.cnf и tw.pol, чтобы нельзя было прочитать их содержимое), чтобы при изменении конфигурации можно было изменить параметры состояния Tripwire, вызывается команда для внесения изменений:

* twadmin –print-cfgfile > twcfg.txt (основные переменные среды)
* twadmin –print-polfile > twpol.txt (полистики для сканирования)