Отслеживание завершения процессов средствами auditd

Данная статья применима к:

- ОС ОН Орёл 2.12
- ОС СН Смоленск 1.6 (при наличии диска со средствами разработки)
- ОС СН Ленинград 8.1 (при наличии диска со средствами разработки)

Установка пакетов

Для включения системы аудита требуется установить пакеты auditd и audispd-plugins.
Для ОС ОН Орёл эти пакеты доступны в репозитории, для ОС СН Смоленск/Ленинград в дополнение к основному диску необходимо подключить в качестве репозитория диск со средствами разработки.

После подключения нужных источников пакетов установка может быть выполнена с помощью графическог о менеджера пакетов или из командной строки командами

```
sudo apt update
sudo apt -y install auditd audispd-plugins
```

Добавление правил обработки системных вызовов **kill** и **exit_group**

Актуальные правила обработки событий, которые автоматически включаются при запуске службы, хранятся в файле /etc/audit/audit.rules
Этот файл автоматически генерируется при запуске службы при запуске (рестарте) службы auditd из файлов /etc/audit/audit.d/*.rules

С помощью команды **auditctl** (режим отладки)

Добавить правила обработки можно командой auditctl, например:

```
auditctl -a exit,always -F arch=b64 -S kill -k kill_process
auditctl -a exit,always -F arch=b64 -S exit_group -k kill_process
```

Подробнее по параметрам:
-a exit,always определяет событие и порядок регистрации, в данном случае правило попадает в список **exit,** а параметр **always** означает что событие будет записываться всегда (вместо always можно указать never, чтобы события не регистрировались)
Всего существует 5 списков:

- task — события, связанные с созданием новых процессов;
- entry — события, которые имеют место при входе в системный вызов;
- exit — события, которые имеют место при выходе из системного вызова;
- user — события, использующие параметры пользовательского пространства;
- exclude — используется для исключения событий.

-F arch=b64 фильтр, определяющий архитектуру подлежащую аудиту. Применим для переносимости настроек между разными архитектурами;

-S kill определяет имя отслеживаемого системного вызова, в данном случае системный вызов **kill;**

-k kill_process задает условное имя (ключ) для облегчения поиска записей о событии;

Добавленные с помощью команды auditctl правила будут действовать до перезапуска службы, поэтому данный способ можно использовать как режим отладки.

С помощью файла **/etc/audit/audit.d/audit.rules**

Постоянные правила обработки можно задать добавив в файл /etc/audit/audit.d/audit.rules строки, повторяющие ключи и параметры команды **auditctl**, как на примере выше:

```
-a exit,always -F arch=b64 -S kill -k kill_process
-a exit,always -F arch=b64 -S exit_group -k kill_process
```

После внесения изменений перезапустить службу:

sudo systemctl restart auditd

Отслеживание событий аудита

События аудита можно отслеживать командой

```
ausearch -k kill_process
```

Или искать любыми средствами в файле **/var/log/audit/audit.log**