ОПЕРАЦИОННАЯ СИСТЕМА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ «ASTRA LINUX SPECIAL EDITION» РУСБ.10015-01

Руководство по КСЗ. Часть 2

Оперативное обновление 1.7.1

Бюллетень № 2021-1126SE17

Листов 7

2021

АННОТАЦИЯ

В настоящем руководстве приводятся изменения в документ РУСБ.10015-01 97 01-2 «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 2» из комплектности изделия РУСБ.10015-01 «Операционная система специального назначения «Astra Linux Special Edition» (далее по тексту — ОС), которые необходимо учитывать при проверке и тестировании комплекса средств защиты из состава ОС с установленным оперативным обновлением согласно бюллетеню № 2021-1126SE17.

Руководство предназначено для администраторов безопасности.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

В настоящем руководстве приведены изменения в документ РУСБ.10015-01 97 01-2: измененные разделы, подразделы и пункты документа.

При проверке и тестировании комплекса средств защиты ОС с установленным оперативным обновлением согласно бюллетеню № 2021-1126SE17 рекомендуется руководствоваться документом РУСБ.10015-01 97 01-2 совместно с настоящим руководством.

2. ПЕРЕЧЕНЬ ИЗМЕНЕНИЙ

2.1. Раздел «8. Проверка контроля подключения съемных машинных носителей информации и сопоставления пользователя с устройством»

В разделе 8 пункт 6) перечисления изложить в редакции:

6) добавить строку, предоставляющую пользователям право монтировать ФС подключенного USB-носителя:

```
/dev/sdc /mnt auto rw,user,noauto 0 0
```

Пункт 13) перечисления изложить в редакции:

13) смонтировать USB-носитель командой:

```
mount /mnt
```

2.2. Подраздел «9.2. Регистрация событий при работе с БД»

Подраздел 9.2 изложить в редакции:

9.2. Регистрация событий при работе с БД

Тестирование системы регистрации событий (аудита) СУБД PostgreSQL проводится в полуавтоматическом режиме. Тестированию подвергается требование к регистрации событий и фиксируемой в сообщениях аудита информации, а также к наличию средств выборочного ознакомления с информацией.

При выполнении тестирования (см. 2.2) генерируются следующие виды событий:

- использование механизма идентификации и аутентификации;
- попытки доступа;
- действия выделенных пользователей;
- запрос на доступ к защищаемому ресурсу;
- создание и удаление объекта;
- действия по изменению ПРД.

Для просмотра сообщений аудита СУБД необходимо:

1) войти в систему от имени администратора;
2) запустить окно терминала;
3) выполнить команду:

```
sudo ausearch -x postgres -i | more
```

Пример

Сообщение аудита, выданное СУБД PostgreSQL

```
type=PROCTITLE msg=audit(07.12.2021 11:49:01.438:13375) : proctitle=postgres:
     11/setest: postgres template1 [local] startup
type=SYSCALL msg=audit(07.12.2021 11:49:01.438:13375) : arch=x86_64
     syscall=write success=yes exit=94 a0=0x1f a1=0x1dd1410 a2=0x5e a3=0x0
```

```
      items=0 ppid=10726 pid=10760 auid=unset uid=postgres gid=postgres
      euid=postgres suid=postgres fsuid=postgres egid=postgres sgid=postgres
      fsgid=postgres tty=(none) ses=unset comm=postgres
      exe=/usr/lib/postgresql/11/bin/postgres subj=0:63:0:0 key=(null)
----
 type=USER_AVC msg=audit(07.12.2021 11:49:01.438:13376) : user_parsec=success
      eid=257 msg0="SUBJECT" msg1="[local]" msg2="template1" msg3="postgres"
      msg4=" " msg5="postgres" msg6=" " msg7=":SQL:DROP USER u_0_01;"
      ppid=10726 pid=10760 auid=unset uid=postgres gid=postgres euid=postgres
      suid=postgres fsuid=postgres egid=postgres sgid=postgres fsgid=postgres
      tty=(none) ses=unset comm=postgres
      exe=/usr/lib/postgresql/11/bin/postgres subj=0:63:0:0
```

Из записи можно получить следующую информацию:

- успешность осуществления события (`success=yes` или `success=no`);
- тип события (`CONNECT`, `DISCONNECT`, `SUBJECT`, `RIGHTS` и т. д.);
- хост, с которого отправлен клиентский запрос (в приведенном примере `[local]`, что соответствует `localhost`);
- имя кластера, с которым работают (`setest`);
- имя БД, с которой работают (`template1`);
- имя авторизованного пользователя (`postgres`).

Описание остальных полей в записи:

- `type` — тип записи;
- `msg=audit` — запись времени события и его уникальный идентификационный номер
- `arch` — запись об архитектуре процессора;
- `syscall` — тип систем вызова;
- `success` — результат обработки вызова (успешно или нет);
- `exit` — значение выполнения, возвращенное системным вызовом;
- `a0`, `a1`, `a2`, `a3` — четыре аргумента, закодированные в шестнадцатеричный формат, зависят от системного вызова;
- `ppid` — идентификационный номер родительского процесса;
- `pid` — идентификационный номер процесса;
- `auid` — идентификационный номер пользователя аудита;
- `uid` — имя пользователя, который вызвал процесс;
- `gid` — группа пользователя, который вызвал процесс;
- `euid` — имя действующего пользователя, который вызвал процесс;

- suid — имя пользователя, установленного во время выполнения;
- fsuid — имя пользователя файловой системы;
- egid — имя действующей группы пользователя, который вызвал процесс;
- sgid — имя группы пользователя, установленного во время выполнения;
- fsgid — имя группы пользователя файловой системы;
- tty — номер терминала, с которого вызван анализируемый процесс;
- ses — идентификационный номер сессии, в которой вызван анализируемый процесс;
- comm — название команды, из которой был вызван процесс;
- exe — путь до исполняемого файла, который вызвал анализируемый процесс;
- subj — контекст безопасности анализируемого процесса.

При проведении тестирования возможно настроить генерацию сообщений аудита PostgreSQL в интерактивном режиме, для этого в терминале от имени администратора выполнить команду:

```
watch -n 1  'ausearch -x postgres -i | tail'
```

При дальнейшей передаче SQL-команд в СУБД все сообщения аудита от СУБД PostgreSQL будут выводиться в терминал с интервалом равным одной секунде.

2.3. Раздел «11. Проверка работы механизма контроля целостности»

В разделе 11 пункт 6) перечисления изложить в редакции:

6) произвести намеренные изменения в ФС:

```
sudo -s
echo asdf >> /sbin/blkid
chmod 700 /sbin/sysctl
```