

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

Руководство администратора. Часть 1

Оперативное обновление 1.7.1

Бюллетень № 2021-1126SE17

Листов 9

АННОТАЦИЯ

В настоящем руководстве приводятся изменения в документ РУСБ.10015-01 95 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1» из комплектности изделия РУСБ.10015-01 «Операционная система специального назначения «Astra Linux Special Edition» (далее по тексту — ОС), которые необходимо учитывать при настройке и эксплуатации ОС с установленным оперативным обновлением согласно бюллетеню № 2021-1126SE17.

Руководство предназначено для администраторов ОС и сети.

СОДЕРЖАНИЕ

1. Общие сведения	4
2. Перечень изменений	5
2.1. Пункт «2.3.1. Уровень защищенности «Базовый»»	5
2.2. Пункт «2.3.2. Уровень защищенности «Усиленный»»	5
2.3. Пункт «2.3.3. Уровень защищенности «Максимальный»»	5
2.4. Пункт «8.3.12. Сквозная аутентификация в СУБД»	5
2.5. Раздел «11. Защищенная графическая подсистема»	7
2.6. Раздел «15. Средства централизованного протоколирования и аудита»	8
2.7. Подраздел «17.3. Разграничение доступа к устройствам на основе генерации правил udev»	9

1. ОБЩИЕ СВЕДЕНИЯ

В настоящем руководстве приведены изменения в документ РУСБ.10015-01 95 01-1: измененные разделы, подразделы и пункты документа, а также добавленные разделы, подразделы и пункты.

При администрировании ОС с установленным оперативным обновлением согласно бюллетеню № 2021-1126SE17 рекомендуется руководствоваться документом РУСБ.10015-01 95 01-1 совместно с настоящим руководством.

2. ПЕРЕЧЕНЬ ИЗМЕНЕНИЙ

2.1. Пункт «2.3.1. Уровень защищенности «Базовый»»

Заголовок пункта 2.3.1 изложить в редакции:

2.3.1. Уровень защищенности «Базовый» («Орел»)

2.2. Пункт «2.3.2. Уровень защищенности «Усиленный»»

Заголовок пункта 2.3.2 изложить в редакции:

2.3.2. Уровень защищенности «Усиленный» («Воронеж»)

2.3. Пункт «2.3.3. Уровень защищенности «Максимальный»»

Заголовок пункта 2.3.3 изложить в редакции:

2.3.3. Уровень защищенности «Максимальный» («Смоленск»)

2.4. Пункт «8.3.12. Сквозная аутентификация в СУБД»

Пункт 8.3.12 изложить в редакции:

8.3.12. Сквозная аутентификация в СУБД

Для работы СУБД PostgreSQL с FreeIPA необходимо выполнение следующих условий:

- 1) наличие в системах, на которых функционируют сервер и клиенты СУБД PostgreSQL, установленного пакета клиентской части FreeIPA `freeipa-client`;
- 2) разрешение имен должно быть настроено таким образом, чтобы имя системы разрешалось, в первую очередь, как полное имя (например, `postgres.example.ru`);
- 3) клиентская часть FreeIPA должна быть настроена на используемый FreeIPA домен (8.3.6).

Подробное описание работы с защищенной СУБД PostgreSQL приведено в документе РУСБ.10015-01 95 01-2.

Для обеспечения совместной работы сервера СУБД PostgreSQL с FreeIPA необходимо, чтобы сервер СУБД PostgreSQL функционировал как служба Kerberos. Выполнение данного условия требует наличия в БД Kerberos принцепала для сервера СУБД PostgreSQL, имя которого задается в формате:

```
servicename/hostname@realm
```

где `servicename` — имя учетной записи пользователя, от которой осуществляется функционирование сервера СУБД PostgreSQL (по умолчанию `postgres`) и которое указывается в конфигурационном файле сервера PostgreSQL как значение параметра `krb_srvname`;

`hostname` — полное доменное имя системы, на которой функционирует сервер СУБД PostgreSQL;

`realm` — имя домена FreeIPA.

Для обеспечения совместной работы сервера СУБД PostgreSQL с FreeIPA необходимо:

- 1) создать в БД FreeIPA с помощью утилиты администрирования FreeIPA принcipала, соответствующего устанавливаемому серверу PostgreSQL. Принципал создается с автоматически сгенерированным случайным ключом;

Пример

```
ipa service-add postgres/postgres.example.ru
```

- 2) создать файл ключа Kerberos для сервера СУБД PostgreSQL с помощью утилиты администрирования FreeIPA `ipa service-add`.

Пример

Создание файла ключа Kerberos на контроллере домена

```
ipa-getkeytab -s domain.example.ru -k /etc/apache2/keytab
-p HTTP/apache2.example.ru
```

Полученный файл должен быть доступен серверу СУБД PostgreSQL по пути, указанному в конфигурационном параметре `krb_server_keyfile` (для приведенного примера путь `/etc/apache2/keytab`). Пользователю, от имени которого работает сервер СУБД PostgreSQL (по умолчанию `postgres`), должны быть предоставлены права на чтение данного файла;

- 3) назначить владельцем файла `krb5.keytab` пользователя `postgres`, выполнив команду:

```
chown postgres /etc/postgresql/x.x/main/krb5.keytab
```

- 4) задать в конфигурационном файле сервера СУБД PostgreSQL `/etc/postgresql/x.x/main/postgresql.conf` следующие значения для параметров:

```
krb_server_keyfile = '/etc/postgresql/x.x/main/krb5.keytab'
krb_srvname = 'postgres'
```

5) указать для внешних соединений в конфигурационном файле сервера СУБД PostgreSQL `/etc/postgresql/x.x/main/pg_hba.conf` метод аутентификации `gss`.

Пример

```
host all all 192.168.32.0/24 gss
```

2.5. Раздел «11. Защищенная графическая подсистема»

Ввести новый подраздел после 11.6, а также изменить нумерацию подраздела «Мандатное управление доступом» с 11.7 на 11.8 в связи с добавлением нового подраздела:

11.7. Блокировка экрана при бездействии

Блокировка экрана при неактивности задается в конфигурационных файлах типов сессий `*themerc*`, расположенных в каталоге пользователя `/home/<имя_пользователя>/.fly/theme/`, следующими параметрами:

```
ScreenSaverDelay=0/<время_неактивности_в_секундах>
```

```
LockerOnSleep=true/false
```

```
LockerOnDPMS=true/false
```

```
LockerOnLid=true/false
```

```
LockerOnSwitch=true/false
```

При этом имена актуальных для сессии пользователя конфигурационных файлов начинаются с `current`, а файлы, имена которых начинаются с `default`, используются для создания и восстановления файлов `current`.

При создании учетной записи пользователя и его первом входе конфигурационные файлы `default.themerc*` копируются из каталога `/usr/share/fly-wm/theme/` в каталог пользователя `/home/<имя_пользователя>/.fly/theme/`.

Пользователю доступно управление блокировкой экрана своей сессии при неактивности из графической утилиты `fly-admin-theme` (см. электронную справку).

Администратору для управления блокировкой экрана пользователей, в т.ч. централизованного, доступен конфигурационный файл `/usr/share/fly-wm/theme.master/themerc`. В файле указываются строки:

```
[Variables]
```

```
ScreenSaverDelay=0/<время_неактивности_в_секундах>
```

```
LockerOnSleep=true/false
```

```
LockerOnDPMS=true/false
```

```
LockerOnLid=true/false
```

```
LockerOnSwitch=true/false
```

При входе пользователя в сессию после считывания параметров из конфигурационных файлов пользователя проверяется наличие файла `/usr/share/fly-wm/theme.master/themerc` с секцией `[Variables]`. При наличии файла из него считываются параметры, и считанные параметры переопределяют аналогичные параметры, считанные ранее из конфигурационных файлов пользователя.

В ОС выполняется мониторинг каталога `/usr/share/fly-wm/theme.master/` и файла `/usr/share/fly-wm/theme.master/themerc`. При создании/изменении файла `/usr/share/fly-wm/theme.master/themerc` срабатывает механизм мониторинга и параметры из файла считываются и применяются к текущим сессиям всех пользователей.

Каталог `/usr/share/fly-wm/theme.master/` может являться разделяемым ресурсом.

Пользователю не доступна возможность переопределить параметры, заданные в `/usr/share/fly-wm/theme.master/themerc`.

11.8. Мандатное управление доступом

2.6. Раздел «15. Средства централизованного протоколирования и аудита»

Ввести новый подраздел после 15.1, а также изменить нумерацию подраздела «Средства централизованного протоколирования» с 15.2 на 15.3 в связи с добавлением нового подраздела:

15.2. Подсистема регистрации событий

Подсистема регистрации событий включает следующие инструменты:

- 1) менеджер и маршрутизатор событий `syslog-ng` — принимает события из различных источников (события от `auditd`, файлы, прикладное ПО), проводит их обработку и, в зависимости от конфигурации, сохраняет в файл, отправляет по сети и т.д.;
- 2) модуль `syslog-ng-mod-astra` — модуль для `syslog-ng`, выполняющий дополнительную обработку и фильтрацию событий;
- 3) `astra-event-watcher` — демон уведомления пользователя о событиях, обработанных менеджером `syslog-ng`;
- 4) журнал событий `kssystemlog` — просмотр и анализ событий.

Установка выполняется командой:

```
sudo apt install syslog-ng syslog-ng-mod-python syslog-ng-mod-astra
astra-event-watcher
```

Работа модуля `syslog-ng-mod-astra` настраивается в конфигурационных файлах:

- 1) `/etc/astra-syslog.conf` — список регистрируемых событий;
- 2) `/var/cache/astra-syslog/` — каталог с файлами настроек по умолчанию для каждого события.

Модуль `syslog-ng-mod-astra` информацию о событиях регистрирует в файлах:

- 1) `/var/log/astra/events` — лог-файл в формате `json` регистрируемых событий (попытки запуска неподписанных файлов, успешная и неуспешная авторизация, данные о пользовательских сессиях и др.). Доступен для чтения только администратору;
- 2) `/var/log/astra/prevlogin<username>` — лог-файл формате `json` сводной статистики предыдущих входов в систему пользователя `<username>`. Включает данные о последней завершенной сессии пользователя, а также количество успешных и неуспешных входов пользователя со времени начала ведения статистики. Доступен для чтения только пользователю `<username>`.

Настройка отображения уведомлений демона `astra-event-watcher` выполняется в файле `/usr/share/knotifications5/astra-event-watcher.notifyrc`.

15.3. Средства централизованного протоколирования

2.7. Подраздел «17.3. Разграничение доступа к устройствам на основе генерации правил `udev`»

Первый абзац подраздела 17.3 изложить в редакции:

17.3. Разграничение доступа к устройствам на основе генерации правил `udev`

Разграничение доступа к устройству осуществляется на основе генерации правил для менеджера устройств `udev`, которые хранятся в соответствующих файлах в каталогах `/etc/udev/rules.d` и `/run/udev/rules.d`. Генерация правил осуществляется автоматически для символьных и блочных устройств с использованием базы учета устройств, ведущейся в локальной системе (файл `/etc/parsec/PDAC/devices.cfg`) или в ALD/FreelPA (см. раздел 8).